

UNIVERZITET  SINGIDUNUM



Milan Milosavljević
Saša Adamović

KRIPTOLOGIJA II

OSNOVE ZA ANALIZU I SINTEZU ŠIFARSKIH SISTEMA



Beograd, 2014.



UNIVERZITET SINGIDUNUM

FAKULTET ZA INFORMATIKU I RAČUNARSTVO

Milan Milosavljević

Saša Adamović

KRIPTOLOGIJA 2

Prvo izdanje

Beograd, 2014.

KRIPTOLOGIJA 2

Autori:

dr Milan Milosavljević
dr Saša Adamović

Recenzenti:

dr Mladen Veinović
dr Branko Kovačević
dr Dejan Živković

Izdavač:

UNIVERZITET SINGIDUNUM
Beograd, Danijelova 32
www.singidunum.ac.rs

Za izdavača:

dr Milovan Stanišić

Tehnička obrada:

Saša Adamović

Dizajn korica:

Aleksandar Mihajlović

Godina izdanja:

2014.

Tiraž:

300 primeraka

Štampa:

Mladost Grup
Loznica

ISBN: 978-86-7912-537-8

Copyright:

© 2014. Univerzitet Singidunum

Izdavač zadržava sva prava.

Reprodukcija pojedinih delova ili celine ove publikacije nije dozvoljeno.

„Mudrost postavlja granice i spoznaji.“

Fridirh Niče





SADRŽAJ

PREDGOVOR	VII
1. UVOD	9
1.1. Kratka istorija politike šifrovanja	10
1.2. Uloga fizike, pretpostavki i poverenja	15
1.3. Ontologija domena zaštite	20
1.4. Praktična bezbednost	27
1.4.1. Ekvivokacija ključa i tačka jedinstvenosti	28
1.4.2. Povećanje tačke jedinstvenosti	31
1.5. Verovatnosni model šifrovanja	33
2. AUTENTIFIKACIJA	43
2.1. Jednostavni protokoli za autentifikaciju na računaru	46
2.2. Jednostavni protokoli za autentifikaciju na mreži	49
2.3. Autentifikacija – informaciono teorijska analiza	55
3. OSNOVE KRIPTOGRAFSKIH PROTOKOLA	58
3.1. Autentifikacija sa simetričnim ključevima	59
3.2. Autentifikacija sa javnim ključevima	64
3.2.1. Sesijski ključ	66
3.2.2. Perfektna tajnost unapred	70

3.2.3. Vremenski pečat.....	75
3.3. Autentifikacija zasnovana na TCP protokolu	80
3.4. Dokazi sa nulnim znanjem – ZKP	84
3.5. Najbolji autentifikacioni protokoli	90
4. SAVREMENI KRIPTOGRAFSKI PROTOKOLI	91
4.1. SSH.....	92
4.2. SSL/TLS	95
4.2.1. Arhitektura SSL protokola.....	97
4.2.2. Bezbednost SSL protokola.....	99
4.2.3. Efikasni metodi u SSL protokolu.....	101
4.3. IPSec.....	103
4.3.1. IKE prva faza: digitalni potpis.....	106
4.3.2. IKE prva faza: simetrični ključ.....	108
4.3.3. IKE prva faza: javni ključ za šifrovanje	110
4.3.4. IKE druga faza	113
4.3.5. IP datagrami u IPSEC protokolu	114
4.3.6. Transport i režimi tunelovanja	115
4.3.7. ESP i AH	118
4.4. Kerberos	120
4.4.1. Kerberos inicijalizacija	122
4.4.2. Kerberos tiketi	123
4.4.3. Bezbednost Kerberos protokola.....	124

4.5. WEP	126
4.5.1. Autentifikacija u WEP protokolu	126
4.5.2. Šifrovanje u WEP protokolu	127
4.5.3. Problem integriteta u WEP protokolu	129
4.5.4. Osnovne za bezbedno korišćenje bežičnih mreža	132
4.5.5. Saveti za bezbedno konfigurisanje bežičnih uređaja	134
4.6. GSM	136
4.6.1. Arhitektura i bezbednost GSM protokola	137
4.6.2. Treća generacija protokola – 3GPP	141
5. BIOMETRIJA	142
5.1. Vrste biometrijskih podataka i njihova podela	143
5.2. Biometrijski servisi za autentifikaciju	149
5.3. Biometrijski sistemi za generisanje ključeva	154
5.3.1. Biometrijska kriptografija	155
5.3.2. Razvoj sistema zasnovanih na biometrijskoj kriptografiji	158
5.3.3. Generisanje ključeva iz biometrije	159
5.3.4. Generisanje ključeva na osnovu biometrije	162
5.4. Jedan algoritam za generisanje kriptoloških ključeva na osnovu biometrije	170
5.4.1. Generička šema algoritma	171
5.4.2. Postavka eksperimentalnog okruženja	174
5.4.3. Informaciona analiza tekstone irisa	175
5.4.5. Izbor adekvatnog zaštitnog koda	180

5.4.6. Motiv za uvođenje zaštitnog koda i interlivera	184
5.4.7. Oblast primene i budući razvoj oblasti	185
6. TAJNA RAZMENA KRIPTOLOŠKOG KLJUČA JAVNIM KANALOM – BEZBEDNOST NA FIZIČKOM SLOJU	190
6.1. Razmena ključa 1: Satelitski scenario.....	193
6.2. Razmena ključa 2: Wayner Wire-Tap kanal.....	201
6.3. Razmena ključa 3: Karte	206
6.4. Jedan algoritam za razmenu ključeva u lokalnoj računarskoj mreži.....	208
LITERATURA	214
DODATAK – HRONOLOŠKI PREGLED OBJAVLJENIH INCIDENATA NA INTERNETU U PERIODU OD 2006. DO 2012. GODINE.....	219
REČNIK POJMOVA	232

Kriptologija 2 – je udžbenik koji je namenjen studentima Fakulteta za informatiku i računarstvo Univerziteta Singidunum za pripremu ispita iz predmeta „Kriptologija 2“, a mogu ga koristiti svi oni kojima je potrebna kriptografska zaštita podataka u savremenim komunikacionim sistemima. Ovaj udžbenik ima više ciljeva, kao što je sticanje novih razmišljanja o ovoj oblasti, znanja i ideja koje ćemo u budućnosti koristiti, a sve to će nas osposobiti da samostalno dizajniramo bezbednosne protokole za potrebe naših budućih poslovnih okruženja, na mestima gde bezbednost podataka bude zahtevana. U prvom, uvodnom delu udžbenika dali smo kratak istorijski pregled politike šifrovanja. Kroz ontologiju domena zaštite prikazali smo osnovnu i glavnu podelu šifarskih sistema na perfektne (apsolutno bezbedne) i neperfektne sisteme (praktično bezbedne). Obzirom na neuporedivo veću zastupljenost neperfektni šifarskih sistema ili sistema koji nude praktičnu bezbednost, diskutovaćemo o kritičnim tačkama ili kriptološkim ključevima, preko tema koje se bave ekvivokacijom ključa, tačke jedinstvenosti i mogućnosti za povećanje tačke jedinstvenosti.

U drugom i trećem poglavlju govorićemo o nekoliko različitih metoda za potvrdu autentičnosti i načinima za uspostavljanje (ili razmenu) sesijskih ključeva preko nebezbedne mreže. Ovakve servise možemo realizovati upotrebom simetričnih ključeva, javnih ključeva ili heš funkcija u kombinaciji sa simetričnim ključevima. Takođe, naučićemo kako da se ostvari perfektna tajnost unapred – *PFS*, razmotrićemo uvođenje vremenskih pečata, kako njegove prednosti tako i nedostatke. Uput, proučićemo nekoliko bezbednosnih zamki koje nisu očigledne i bolje razumeti suptilna pitanja koja se odnose na bezbednost kriptografskih protokola. Sve ovo će biti osnova za razumevanje narednog poglavlja u kome ćemo govoriti o savremenim bezbednosnim protokolima. Videćemo da uprkos obimnom razvoju i uloženom naporu velikog broja stručnjaka, takvi protokoli nisu imuni na neke bezbednosne propuste koje ćemo istaći i razraditi u ovom poglavlju.

U četvrtom poglavlju upoznaćemo se sa nekoliko savremenih bezbednosnih protokola (*SSH, SSL/TLS, IPSec, Kerberos, WEP, GSM*), koji su osnova velikog broja

Internet servisa u savremenom poslovnom svetu. Razumećemo njihov dizajn i način na koji obezbeđuju servise autentifikacije, tajnosti, integriteta i neporecivosti. Drugi cilj je da razumemo do sada sve prepoznate bezbednosne probleme kod ovih protokola, kao i da razumemo modifikacije koje bi bilo potrebno uraditi za prevazilaženje tih problema, a uspešnost modifikacije zavisice od našeg stečenog znanja i iskustva.

U petom poglavlju govorićemo o biometriji i biometrijskim sistemima. Biometrija ili bio-informacija se nameće kao moguće rešenje za obezbeđenje čvrste veze između autentifikatora i sistema za autentifikaciju. Reč „biometrija“ vodi poreklo od grčke imenice „bios“ – život i glagola „metreo“ – meriti. Biometrija je opšti termin za opis i merenje fizičkih karakteristika koje mogu biti korišćene za autentifikaciju. U nastavku govorimo o biometrijskim sistemima za generisanje ključeva i jednoj klasi sistema za generisanje kriptološkog ključa na osnovu biometrije irisa. Naučićemo zašto biometrija rešava mnogo bezbednosnih problema, ali i uvodi neka nova ograničenja.

U šestom poglavlju govorićemo o sistemima za generisanje i distribuciju kriptoloških ključeva preko javnih komunikacionih kanala u savremenim računarskim mrežama, kao i razvoj sopstvenog rešenja na osnovu teorijskih radova. Protokoli koji se danas koriste za razmenu kriptoloških ključeva prepuštaju bezbednost ključeva rešavanju problema faktorizacije. Najčešće korišćeni metodi za distribuciju ključeva su *Diffie-Hellman* protokol i zaštita ključeva u javnim komunikacionim kanalima korišćenjem asimetričnih šifara – *RSA* ili *DSA*. Prikazaćemo osnove protokola koji proizilaze iz kvantne kriptografije, a daju osnovu za dalji razvoj protokola u klasičnoj kriptografiji.

Na kraju je jedan dodatak u kome je hronološki prikazana lista svih uspešnih napada u poslednjih sedam godina, a iz kategorije visokotehnološkog kriminala. Zadatak ovog poglavlja je da zainteresuje čitaoce, stavi do znanja svim onima koji danas rade i radiće u oblasti *IT* bezbednosti i da ukaže na postojanje neprkidne potrebe za kreiranjem novih kriptografskih mehanizama koje će nadjačavati oružje napadača, jer bitka između dobrih i loših momaka se nastavlja...

Beograd, Srbija 2014.

Autori

1. UVOD

Savremene informacione tehnologije i globalizacija dramatično su promenile današnji svet računarskih mreža, koje se odlikuju visokim stepenom integracije različitih elektronskih servisa. Obzirom da je broj Internet servisa i novih korisnika usluga svakodnevno u porastu, povećava se količina i vrednost informacija koje se razmenjuju. Informacije koje se razmenjuju putem mreža i skladište na umreženim memorijskim lokacijama, mogu biti kompromitovane ukoliko nisu adekvatno zaštićene. U svim tipovima mrežne komunikacije poseban izazov predstavljaju mehanizmi za kontrolu pristupa. Njihova uloga je da zaštite podatke i informacije od neovlašćenih pristupa putem dovoljno bezbednih postupaka za proveru identiteta.

Procenjuje se da celokupna oblast zaštite informacija u narednom periodu treba da obezbedi radikalno kvalitativan skok i pomeranje osnovne paradigme računarske sigurnosti ka paradigmi informaciono teorijske sigurnosti. Ovaj pomeraj bi omogućio sintezu čitave klase zaštitnih mehanizama, čija kompromitacija više ne bi zavisila od računarske snage napadača.

Interesantno je zapaziti da preduslov za ovaj poduhvat leži u razvoju novih metoda digitalne obrade signala, koje na fizičkom sloju savremenih računarsko komunikacionih mreža treba da obezbede ekstrakciju dovoljne količine čisto slučajnih nizova pogodnih za primenu u novim protokolima uspostavljanja i razmene kriptoloških ključeva maksimalne dužine i neodređenosti.

U domenu pouzdane i za praksu prihvatljive autentifikacije, biometrija postaje značajan izvor kriptoloških parametara. Digitalna obrada izvornih biometrijskih signala je od presudnog značaja, kako za uspostavljanje tako i za ekstrakciju autentifikacionih kodova maksimalne entropije.

U domenu upravljanja autorskim pravima digitalnih sadržaja, digitalna obrada signala nosioca i utiskivanje digitalnih pečata, vidljivih i nevidljivih, takođe predstavlja nezaobilazan gradivni element. Sve ovo ukazuje na novo mesto ove discipline u okviru opšte teorije i prakse sinteze sistema za zaštitu informacija. U udžbeniku se identifikuje, analizira i razvija klasa podsistema digitalne obrade signala koje ispunjavaju nove zahteve proistekle iz ovih novih trendova u zaštiti informacija u savremenim računarsko komunikacionim sistemima.

1.1. KRATKA ISTORIJA POLITIKE ŠIFROVANJA

Alati koji implementiraju kriptografske mehanizme, omogućiće kompanijama i pojedincima da zaštite svoje lične podatke i privatnost. Sjedinjene Države su nekada kontrolisale izvoz šifarskih mehanizama, sa istim tretmanom kao da se radi o oružju. To je učinjeno zbog zaštite NSA-a. To je bio period kada je šifrovanje bilo ograničeno na mali broj korisnika, uglavnom vlade i banke. Tada je to ograničenje imalo smisla. Takođe, bilo je lakše da se kontroliše šifrovanje kada je to bio samo komad hardvera (kao Enigma), nego danas kada je moguće pokrenuti softver na bilo kom računaru.

Internet je značajno uticao na promenu svega oko nas. Računari su bili bezbedni, jer nisu bili povezani na mrežu. Glavna procedura zaštite podataka je bila zaključavanje vrata od prostorije u kojoj se računar nalazio. Međutim, sa pojavom Interneta sve ove računarske mašine postale su nezaštićene u nebezbednom mrežnom okruženju, tako da zaštita od fizičkog pristup više nije dovoljna. Danas je neuporedivo bitnije zaštititi računar od udaljenog pristupa preko Interneta, koji danas predstavlja glavnu pretnju.

NSA-a koja je trenutno mnogo osporavana u svetu, uvidela je ovaj problem još u ranim 1990-im. NSA je tada imala dve misije. Prva je da se zaštite podaci od američkih državnih i privatnih institucija od strane špijunaže. Druga je, da sačuva sposobnost za prikupljanje obaveštajnih podataka iz stranih zemalja. Američka politika je bila da se pronađe rešenje koje će učiniti Internet mnogo bezbednijim, a sa druge strane da se sačuva operativnost NSA-a. NSA je razvio elegantno i skupo rešenje *Klipper* čip „engl. *Clipper chip*“. *Klipper* je hardversko rešenje. Ideja je da se čip ugrađuje na svakom novom računaru. To bi omogućilo šifrovanje podataka, ali i mogućnost čitanja podataka od strane onih ovlašćenih lica koji su imali ključ za šifrovanje. Jedan od problema sa čipom je dodatno veća cena za stotinak dolara na postojeću cenu svakog računara i mobilnog telefona. Drugi problem se ticao privatnosti sa aspekta sudskih organa, jer NSA bi znala ključ i tako mogla da čita bilo koju šifrovanu poruku.

Međutim, prema mišljenju mnogih stručnjaka iz ove oblasti, ovakva ideja nije imala potencijala da zaživi. Umesto čipa dati su predlozi da se ljudima da pristup

softveru za šifrovanje. Ove predloge je zastupao tadašnji direktor centralne obaveštajne službe, koji je direktno iznosio nove predloge predsedniku *USA*.

Skup proizvod koji vas štiti od svih, ali ne i od *NSA*, što je iznenađujuće, na tržištu je imao mali broj pritužbi. Na kraju, *Kliper* nije dao odgovor na ovaj problem. Nova Klintonova administracija, u želji da kontroliše široko rasprostranjenu Internet mrežu, odlučila je da formira dve grupe u Beloj kući za nadzor Interneta. Prva grupa je imala nadzor nad servisima za elektronsku trgovinu, dok druga grupa ima zadatak da vodi računa o bezbednosti javnih mreža. Zadatak ovih radnih grupa je bio da pronađu način za stvaranje bezbednosne politike na Internetu bez oštećenja ili sprovođenja zakona ili obaveštajnih sposobnosti. Radna grupa je potrošila na ovaj zadatak preko četiri godine i došla do rešenja u kom predlažu široko rasprostranjenu upotrebu softvera za šifrovanje.

Tada je postalo jasno da će se koristiti softversko šifrovanje umesto hardverskog. Komercijalna proizvodnja hardverskih uređaja za šifrovanje nije mogla da zaživi za upotrebu u poslovnim okruženjima, na taj način ne bi postojalo veliko tržište za šifarske proizvode. Grupa za bezbedne javne mreže se usmerila na *PKI* infrastrukturu ili na infrastrukturu sa javnim ključevima. *PKI* obezbeđuje bezbedne načine za razmenu kriptoloških ključeva, tako da samo ovlašćena lica mogu pristupiti podacima, koji se skladište na računarima ili putuju između dva računara. Međutim, kao i svaki drugi sistem koji poseduje interakciju sa spoljnim svetom i *PKI* je imao mnogo problema.

Prvo, *FBI* i *NSA* su hteli da poseduju kopije ključeva, kojima je moguće pristupiti po sudskom nalogu. Tražili su „treću stranu od poverenja“ da raspolaže sa ključevima, ali shvatili su da nijedna kompanija ne želi da dozvoli pristup trećoj strani svojim važnim podacima. Ne postoji takva stvar kao što je „treća strana od poverenja“ za istinski vredne podatke, ovo svi treba da imamo na umu.

Drugo, otkriveno je da kod većine komercijalno dostupnih softvera postoje ozbiljni bezbednosni nedostaci. Godine 1999. *NSA* je pregledala 40 najboljih proizvoda koji su se prodavali za šifrovanje. Nijedan od njih nije bi bez mana. Neke kompanije su tvrdile da koriste ključeve dužine 56 bitova, ali po dizajnu ili greškom programi nisu koristili više od 28 bitova ključa, čije su dužine još u to vreme bile izuzetno kratke. Ključna komponenta šifarskih algoritama su generatori slučajnih brojeva. Neke kompanije koriste neispravne generatore slučajnih bro-

jeva. Drugi su odustali u potpunosti od generatora, koristili su listu predefinisanih brojeva, sa koje bi programi nasumično birali one koje će iskoristiti za šifrovanje. Neadekvatan generator slučajnih brojeva omogućava kriptanalitičaru da sa značajno manje truda probije neki šifarski sistem, ovo svakako ne predstavlja izazov za *NSA*-a i *FBI*-a.

Pisanje programa za šifrovanje predstavlja izuzetno težak posao. Posle tog izveštaja o stanju softvera na tržištu, iz godine u godinu je softver napredovao, ali ne toliko da i danas ne zadrži bezbednosne propuste. Da je *SAD* pokušao da održi softver na nekom nivou izvrsnosti, to bi sigurno ubilo tržište, baš kada je pokušao da održi automobile od 1920 po bezbednosnim standardima koje imamo i danas. Ovo je upravo razlog zašto je kriptologija kao vojna tehnologija dospela u civilnu upotrebu, koja se sve više kao ozbiljna nauka sa ogromnim potencijalom u budućnosti izučava na mnogim svetskim univerzitetima. Zahvaljujući sve većem broju stručnjaka iz ove oblasti, nedostaci koji postoje će nestati, ali ne u skorije vreme.

Problem bezbednosti na Internetu bio je toliko aktuelan da je eskalirao u predstavničkom odboru saveta za nacionalnu bezbednost, gde se zvaničnici u toj administraciji sastaju samo u vezi najvažnijih problema. Šifrovanje i Internet bezbednost traži neminovno teške odluke. Ako *SAD* dozvoli kompanijama da prodaju softver i hardver za šifrovanje, *NSA* će izgubiti velike mogućnosti (ovo se nedavno desilo, zbog promene u tehnologiji). Tačnije, *FBI* bi mogao izgubiti sposobnosti da prisluškuje „kriminalne komunikacije“ (Žestoka pomoć za sprovođenje zakona i zakona o patriotskom aktu, mere za očuvanje sposobnosti za prisluškivanje bez obzira na promene u tehnologiji, (podešavanje konteksta za sprovođenje zakona)). Tehnologija se menja najviše iz komercijalnih razloga, vladine agencije to moraju ispratiti. Teškoća ovoga je preterana rutina, ali inteligentni signali i postojanje prisluškivanja u dinamičnim tehnološkim okruženjima, moraju biti jednako prilagođeni dinamičnim naporima da održi svoje operativne sposobnosti.

Izvor dinamizma u ovoj debati je bio veoma neočekivan, kad su upitanju žalbe na bezbednost računara i Internet-a. Tempo prilagođavanja premašio je očekivanja. Tražnja je bila nezasićena. Nekoliko novih korisnika je znalo ili nije marilo zbog ranjivosti. Postoje oni koji su bili svesni, ali nisu mogli da kupuju američke dovoljno „jake“ proizvode. Mnoge kompanije su napravile grešku, jer su koristile besplatne softver za kriptografsku zaštitu. To je bio slučaj jedne američke avio kompanije

koja je preuzela sa Interneta *PGP* softver sa jednog sajta u Holandiji. Ovo je glavni mamac stranih obaveštajni službi, oni nude besplatno ovakav softver da bi kasnije mogli da pročitaju sve šifrovane poruke. Ovo je jedan jasan pokazatelj na potrebu za razvojem sopstvenog kripto softvera, bez obzira na postojanje suptilnih nedostataka. Sve ovo je stvorilo komercijalne rizike koji su pretili američkim kompanijama uspon na tržištu informacionih tehnologija.

Radna grupa koja je formirana u Beloj kući za nadzor elektronskih Internet servisa imala je velike sukobe sa *FBI* i *NSA*. Ideja da se nad šifrovanjem izgubi kontrola nije bila nikako prihvatljiva za *FBI* i *NSA*. Razlozi su jasni, to bi smanjilo sposobnost prikupljanja obaveštajnih podataka. Međutim, radna grupa je predložila da se ona pobrine o bezbednosnoj Internet politici.

Razlozi za promenu politike bili su jasni. Iako postoji rizik za nemogućnost prikupljanja obaveštajnih podataka, radi zaštite američkih kompanija i potrošača. Veliki komercijalni rizik američkih kompanija je u dinamičnom tržištu u kom *SAD* više neće imati monopol nad šifrovanjem podataka. U budućnosti ćemo videti raširenu upotrebu šifrovanja na Internetu, da li će nam se dopasti ili ne. Bilo je govora o „zadnjim vratima“ u softveru (softver koji je ponudila *NSA*), ali je to odbačeno. Razlog tome su strani protivnici koji žele da iskoriste zadnja vrata. Radna grupa je zadobila poverenje narodnih poslanika, da je moguće prevazići probleme bez ograničenja i zadnjih vrata.

Ovo je iz mnogo razloga idealan ishod. Oni koji su doneli ideju o kontroli šifrovanja, mislili su da su pobedili. Do tada je bilo normalno da država odlučuje o svesmu, odobrava prodaju kompanije ili pribavlja sve što može da joj zatreba. Jedino politika nije uspela u ovom slučaju, kada je reč o zaštiti računarskih mreže.

Klintonova administracija, kreirala je Internet politiku od *ICANN* (engl. *Internet Corporation for Assigned Names and Numbers*) i zakona o elektronskoj trgovini na kritičnoj infrastrukturi - *PDD63*. Nažalost i pored Internet politike, šifrovanje je najmanje uspešan deo Internet politike. Pretpostavka koja je dovela do nekontrolisanog šifrovanja u svetu je, da ako pustimo šifarske mehanizme izvan kontrole, ljudi će ih koristiti i Internet će biti bezbedan. Izgleda da je ova pretpostavka bila pogrešna.

Većina ljudi ne koristi kriptografsku zaštitu od kada je postala javno dostupna. Ovo nije očekivan ishod. Oni su potencijalni rizik. Možda će sadašnja otkrića promeniti stvari. Šifrovanje za obične ljude je „bezveze“, tako reći samo usporava računare i postaje dosadno. Možda će rast procesorske snage rešiti ovaj problem. Šifrovanje je teško sprovesti i implementirati, ali ako to postane deo servisa u oblacima (engl. *cloud*) koji ne zahteva korisničku aktivnost sa aspekta implementacije kriptografskog mehanizma, to ne mora više da bude problem u praksi. Nova istraživanja ukazuju da je jednostavnost korišćenja važnija od procene rizika u određivanju da li će ljudi koristiti šifarske algoritme, ali i promene u načinu upotrebe Interneta danas, daće šifarskim mehanizmima drugu šansu.

I dalje će biti problema. Prirodno je da razvoj hardvera generiše nove probleme na softverskoj strani. Softver će i dalje imati nedostatke, a implementacije će sigurno biti neujednačene. Drugi tip problema koji nastaje, jeste zbog ljudskih grešaka. Ovo stvara mogućnosti za uspešan napad nekog sofisticiranog napadača, koji će to pokušati iskoristiti, ali to će biti sve teže i teže. Prevelika upotreba šifrovanja će verovatno zahtevati mnogo više od poslovnih podela na kojima je zasnovana Internet trgovina. Problem privatnosti na Internetu i dalje ostaje kao dovoljno nerešen problem. Nismo još sigurni šta reč privatnost na Internetu predstavlja. S druge strane, razvoj mobilnih uređaja, naročito pametnih (*Android*, *iOS*), uvodi nove bezbednosne probleme. Postavlja se pitanje koliko smo sigurni, ko je programirao programe koje preuzimamo sa Interneta i instaliramo na našim telefonima? Da li je možda i to jedan od načina da se pokupe ključevi? U svakom slučaju ostaje u domenu mogućeg da besplatan program „krade“ ključeve.

Ovo nije potpuna priča. Nismo još pričali o naporima oko servisa za autentifikaciju ili proveru identiteta na Internetu ili kako *NSA* rešava probleme na Internetu (*Snouden* predstavlja iskrivljenu sliku). On ističe, da je politika pošla pogrešno na samom početku Internet doba. Šifrovanje nije srebrni metak, u kontekstu nije nepobedivo, ali veća upotreba bi značila značajno veći nivo bezbednosti podataka na mreži.

1.2. ULOGA FIZIKE, PRETPOSTAVKI I POVERENJA

Algoritmi, kako za realizaciju, tako i za razbijanje kriptografskih mehanizama su matematički objekti i kao takvi idealizovani. Međutim, svi procesi u realnom svetu, uključujući računanje i komunikacije, predstavljaju fizičke procese, koji u sebe uključuju šumove, kvantne efekte, i ostale faktore neodređenosti. Ovi fizički faktori mogu ići na ruku kriptografiji ili mogu da joj odmažu.

Prvo ćemo razmotriti otežavajuće faktore. Krenućemo od kvantnog računara, koji je moguće realizovati, a za sada ne postoje pretpostavke da nije moguće realizovati kvantni računar. Postojanje jednog super kvantnog računara potencijalno obezvređuje sve asimetrične šifarske sisteme. Ako izuzmemo ovu mogućnost, postoji nešto što je bliže realnosti, a to su kanali bočnih informacija (engl. *Side information channels*) na dometu kriptanalitičara, a koji postoje kao rezultat neke fizičke implementacije:

1. Vreme obavljanja pojedinih računarskih operacija;
2. Potrošnja pri napajanju u zavisnosti šta se računa;
3. Elektromagnetna zračenja;
4. Odziv uređaja na provocirane kvarove (neregularno napajanje, udari, zračenje);

Prvi problem se odnosi na prvu i drugu tačku. Na primer, kada koristimo operacije koje se odnose na *AES* algoritam, moguće je detaljnom analizom kripto procesora na osnovu prosleđenih instrukcija rekonstruisati kriptološki ključ. Ova mogućnost nije više samo pretpostavka, ona danas postoji i kao komercijalno rešenje. Tako da je u današnje vreme, ukoliko se profesionalno bavimo sa kriptografijom, neophodno na neki od načina zaštititi procesor računara.

Drugi problem je kompromitujuće elektromagnetno zračenje - *KEM*. Rad računarskog procesora u spektralnom domenu emituje jedan vrlo bogat signala. Ukoliko napadač poseduje široko pojasni prijemnik, moguće je snimiti spektar na osnovu koga napadač dobija određene informacije (demodulacijom signala moguće je rekonstruisati ključeve). Ne preduzimanjem odgovarajućih mera za sprečavanje ove vrste problema, ostavljamo mogućnost za lako kompromitovanje kriptografskog uređaja.

Postoji više načina da se spreči kompromitovanje uređaja od elektromagnetnog zračenja. Jedan način je da se takav krypto uređaj postavi u Faradejev kavez. Zadatak Faradejevog kaveza je da spreči dovedeni otvoreni signal da izađe van oklopljenog provodničkog zatvorenog sistema u krypto procesoru.

Poslednji problem je odziv uređaja na provocirane kvarove. Postavlja se pitanje kako će kriptografski uređaj (zamislimo neku crnu kutiju) reagovati na neregularno napajanje (jače ili slabije) i druga zračenja koja mogu da izazovu neplansku pobudu kod uređaja i na taj način otkrije neke informacije o stanjima krypto uređaja.

Sve ovo predstavlja multidisciplinarnost ove oblasti, možete da napišete idealan matematički algoritam (na primer, *One-Time pad* – dokazivo bezbedan kriptografski sistem), ali njegova fizička realizacija ga stavlja u jednu neprijateljsku sredinu koju smo predstavili ovim otežavajućim faktorima.

Nastavljamo ovaj odeljak sa diskusijom o olakšavajućim faktorima. Fizika sama po sebi daje nekakve neodređenosti i te neodređenosti su jako bitne u kriptologiji. Interesantno je zapaziti da u savremenim sistemima šumovi koji postoje u komunikacionim kanalima, predstavljaju osnovu za razvoj novih oblasti za zaštitu informacija, ali da je drugačije verovatno ta oblast ne bi mogla da se razvija. Treba zapaziti da šumovi predstavljaju drugu vrstu izvora neodređenosti, na osnovu kojih je moguće generisati kriptološki ključ.

Drugi olakšavajući faktori mogu biti predstavljeni na način da kryptoanalitičar ne može da zna tačno stanje fizičkog sistema. Na primer, u kvantnoj kriptografiji, kryptoanalitičar može merenjem da dobije najviše 1 bit informacije o polarizaciji. Apstraktno gledano, zahvaljujući fizici moguće je projektovati sistem koji i bez implementacije kriptografskog algoritama obezbeđuje zaštitu podataka na visokom nivou.

Stanja fizičkih sistema često se nalaze na strani kriptografa i mogu poslužiti za dizajniranje sistema za detekciju upada. Na primer, pretpostavimo da imamo čašu vode i da je za kryptoanalitičara informacija koju želi da otkrije, upravo temperatura vode u čaši. Kryptoanalitičar će uzeti neki termometar, staviće u vodu i izmeriti temperaturu vode. Ovaj upad će biti detektovan iz razloga što termome-

tar ima neku svoju temperaturu kojom će izazvati promenu temperature vode. Na ovaj način, kriptograf će detektovati promenu temperature, a time i napad.

Do sada smo stekli utisak da se ova oblast razlikuje od drugih oblasti nauke i da kažemo tehnike u širem smislu. U klasičnoj nauci obično napadamo neke prirodne fenomene, trudimo se da napravimo neke modele pomoću kojih ćemo to bolje da razumemo i da ovladamo nekim zakonitostima. U zaštiti informacija sa one druge strane nemamo prirodu, već imamo protivnika. Sa ovakvog stanovišta posmatranja postavljamo pitanje šta mi u takvoj sredini pretpostavljamo i šta su to pretpostavke kada projektujemo neki sistem i na čemu zasnivamo bezbednost takvog sistema?

Bezbednost svakog kriptografskog sistema zavisi od određenih pretpostavki. Tačnije, nemoguće je izreći za jedan sistem da će ostvariti svoj proklamovani cilj, a da pri tome ne navodite pod kojim uslovima. Pri projektovanju sistema postoje opšte implicitne pretpostavke.

Prva implicitna opšta pretpostavka, koja često nije eksplicitna, je egzistencija slučajnosti kao takve, odnosno pretpostavka da naš svet nije deterministički, predstavlja filozofsko pitanje. Drugim rečima, mogli bismo ovako da kažemo, ako bismo živeli u svetu u kome je sve determinističko, tada kriptologija ne bi bila onakva kakva je sad. Zapravo ne bismo mogli da računamo na efekte slučajnosti koji su na neki način u srcu kriptoloških sistema. Prema tome, implicitna pretpostavka je da u prirodi postoji čista slučajnost, odnosno naš svet nije deterministički kako smo već rekli. Ova prva pretpostavka je sama po sebi interesantna.

Druga implicitna pretpostavka je da slučajne veličine mogu biti nezavisne. Na primer, kada govorimo o slučajnim veličinama, uzmimo scenario generisanja kriptološkog ključa. Ne samo da pretpostavljamo da je upotrebljen prirodni izvor informacije (slučajnosti), mi pretpostavljamo i da je svaki generisani bit ključa nezavisan jedan od drugog.

Jedna opšta pretpostavka, koja je gotovo uvek eksplicitna, je da imamo poverenja u neke entitete ili komponente sistema kada projektujemo neki sistem. Nemoguće je reći kada projektujemo kriptografski sistem, da ne postoji bar neka tačka sistema u koju smo delegirali poverenje. Na primer, ako uzmemo jedan profesionalni sistem kao što je *One-Time pad*, on obezbeđuje komunikaciju između dve

tačke. Šta je poverenje koje smo delegirali u ovom sistemu? Delegirali smo poverenje, tako što verujemo osobi koja je prenosila ključ od Alise do Boba i pravila kopiju, da nije napravila treću kopiju ključa. Drugi primer, kada koristimo neki pseudo slučajni generator u običnim sistemima, mi verujemo prvo našem operativnom sistemu i aplikacijama koje su instalirane na njemu i verujemo njegovim specifikacijama, to znači ako smo sačuvali ključeve u neki deo za koji smatramo da je pod našom kontrolom i da u specifikaciji piše da niko drugi ne može tom mestu pristupiti (ni operativni sistem), ili ako je pod nekim uslovima koje mi kontrolišemo. Ovo je primer delegiranja poverenja u isporučiooca softvera, koji je tvrdio da se to zaista tako ponaša.

Cilj profesionalne sinteze kriptografskog sistema je da sve pretpostavke, kako implicitne tako i eksplicitne, učini što je moguće slabijim. Sada nakon ove diskusije možemo da zamislimo šta je idealan kriptografski sistem, kao i pitanje da li je on moguć? Idealan sistem bi bio onaj u kome su svi servisi tajnosti zadovoljeni, a da nigde ništa nismo delegirali. Dakle, to znači da naš sistem ne podrazumeva određene zavisnosti, ako bismo ovo mogli da postignemo, imali bismo jedan idealan sistem u kome nije delegirano nikakvo poverenje. Sa druge strane, kada poređimo dva kriptografska sistema u smislu koji je bolji, pod istim kriptološkim uslovima proglasilićemo boljim onaj sistem koji je najmanje delegirao poverenje po nekim tačkama sistema. Međutim, ako bismo hteli da zamislimo kako izgleda jedan idealan kriptografski sistem, verovatno bismo zamislili dve crne kutije u dve tačke, u kojima ništa nije delegirano kao poverenje, i koje nekako stalno rade u pozadini.

U praktičnom svetu teško je projektovati jedan idealni sistem. Obzirom da nije moguće ili je jako teško izbeći potrebu za delegiranjem poverenja, postoji ideja da se projektuju nove komponente koje bi detektovale korumpiranost nekog entiteta kome je poverenje delegirano. Postojanje ovakvog sistema za detekciju pronevere poverenja dalo bi ovom kriptografskom sistemu prednost u odnosu na bilo koji drugi.

Navešćemo jedan interesantan primer iz oblasti mašinskog učenja koji je dosta aktuelan danas u svetu, a može da nađe primenu u kriptografskom sistemu. Reč je o jednom stranom projektu, gde je napravljen eksperiment u kome ispitanici za računarom, svojim mislima (moždanim talasima) pomeraju kursor miša (gore, dole, levo i desno). Sve ovo može biti iskorišćeno u druge svrhe. Stvarno pitanje

za ovakav sistem bi glasilo, da li je moguće detektovati da ispitanik svojim mislima kaže hoću levo, a zapravo misli da hoće desno. Upravo ova mogućnost može biti jedna za sintezu sistema za detekciju pronevere delegiranog poverenja. Na primer, ako onom kome delegiramo poverenje, ispišemo spisak bezbednosnih procedura kojih se on mora striktno pridržavati (politika o tajnosti ključeva itd.), tada je jako bitno preko ovih sistema za detekciju utvrditi da li će postojati dvosmisleno ponašanje. Redukcija ovih pretpostavki i zahteva za poverenjem u cilju postizanja zadatog nivoa bezbednosti je centralna tema svakog budućeg razvoja kriptografije.



1.3. ONTOLOGIJA DOMENA ZAŠTITE

Kriptologija predstavlja izvorno vojnu tehnologiju sa izuzetnom državnom kontrolom. Možemo da kažemo da je ona igrom slučaja razvojem Interneta prešla u javni domet, ali bez obzira na sve i dalje je ostala dominantno vojna tehnologija.

Napomenućemo osnovne savremene servise zaštite koji spadaju u ovu oblast.

- Servis tajnosti;
- Servis za autentifikaciju;
- Servis za obezbeđenje integriteta;
- Servis za obezbeđenje neporecivosti.

Svi navedeni servisi su nametnuti kao aktuelni od strane Interneta kao globalne IT infrastrukture. Međutim ako se pažljivo analizira, svi ovi servisi su pažljivo razvijani i plod hladnog rata za kontrolu i upotrebu nuklearnog oružja.

Tajnost je nastala kao potreba za skrivanjem informacija. Na primer, ako se stvara velika presija između dve države, a krajnji rezultat potencijalno može biti rat između njih, bitno je zaštititi tajnost poruke koja u sebi sadrži poruku „Ispali prvu raketu, predsednik!“. U slučaju da druga država pročita poruku, tada bi ona prva odreagovala i pokvarila planove.

Autentifikacija je jako bitna kao servis. Ostanimo na prethodnom primeru. Vojske kao rukovaoca sa nuklearnim oružjem mora da bude sigurna da je baš tu poruku poslao predsednik države.

Integritet podrazumeva u prethodnom primeru zaštitu poruke od izmena. Pretpostavimo da je druga strana presrela poruku i izmenila je tako da glasi „Nemojte još ispaljivati raketu!“. U tom slučaju druga strana bi prva odreagovala.

I na kraju neporecivost, da onaj ko je primio naredbu (vojnik, vojna baza) ne može da kaže da nije primio naredbu. Za ovaj servis neophodno je da postoji pisani trag o tome, dovoljan da može da snosi konsekvence.

Međutim, ako govorimo o vrstama tehnologije, njihovoj bezbednosnoj osetljivosti i rangu važnosti, zaključujemo da naša tehnologija ima sva tri plusa. To znači da

ona može biti vojna, civilna, poseduje određene stepene osetljivosti i ima rang važnosti koji se u doktrinarnim dokumentima *NATO* pakta tretira kao nuklearno oružje, slika (Slika 1.1).

Vrsta tehnologije		Bezbednosna osetljivost	Rang važnosti
Vojna	Civilna		
+	+	+	A (Cyber + nuklearno raktno oružje)
+	-	+/-	
-	+	+/-	

Slika 1.1 Status tehnologije

Doktrinarni dokumenti za 21. vek podjednako tretiraju važnost svih kriptoloških mehanizama za zaštitu informacija i nuklearnog oružja na isti način. Jedina dva slučaja za koja se ne čeka da se donose kolektivni dogovor u zapadnim državama, a pri tome treba odmah da se reaguje su nuklearni napad i *sajber* (engl. *Cyber*) napad.

Doktrinarni dokumenti govore o tome kolika se važnost pridaje ovoj oblasti i kako je ona u jednom velikom usponu na zapadu. Američki predsednik ima svoj tim od 9 profesora iz ove oblasti sa poznatih američkih univerziteta i oni predstavljaju stalni komitet koji mu daje godišnji izveštaj o stanju u oblasti i šta treba novo preduzeti u njoj.

Predstavićemo nekoliko interesantnih konstatacija iz jednog godišnjeg izveštaja, koji predstavlja zvanični izveštaj Bele kuće:

- Iako današnje stanje tehnike izlazi u susret neposrednim potrebama, još uvek ne obezbeđuje odgovarajuću zaštitu u računarima i mrežama.
- Fundamentalno različite arhitekture i tehnologije se očekuju i potrebne su da bi *IT* infrastruktura bila bezbedna.
- *US* akademske institucije danas imaju skoro 250 aktivnih profesionalaca iz ove oblasti na koje se oni mogu osloniti.

U izveštaju pored konstatacija, date su i preporuke, od kojih smo izdvojili jednu:

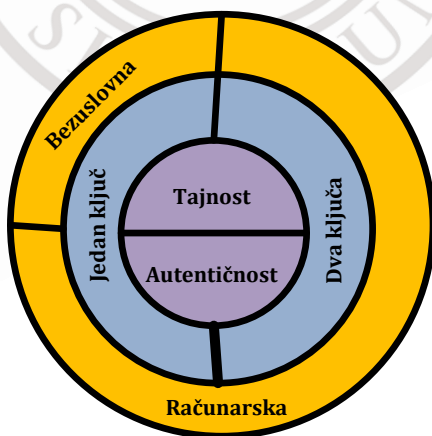
- Prvo da se pojača rad na univerzitetima u ovoj oblasti, tačnije da se koliko god je moguće da se ovi predmeti po studijskim predmetima uvode, kao i da se otvaraju novi projekti.

Iznećemo nekoliko naših zaključaka o ovoj oblasti. Ovi sistemi koje mi koristimo i o kojima pričamo, nisu samo tehnološki, oni su i socijalni, jer ih koriste i obični ljudi. Sve ovo zajedno treba da generiše jednu bezbednu *IT* infrastrukturu.

Poverenje u sistem bezbednosti zahteva kvantitativnu metodologiju. To ne može biti deskriptivna priča, već to mora biti naučno zasnovana priča. Zahtevani su dokazivi nivoi bezbednosti koji imaju ontološku težinu prirodnih zakona.

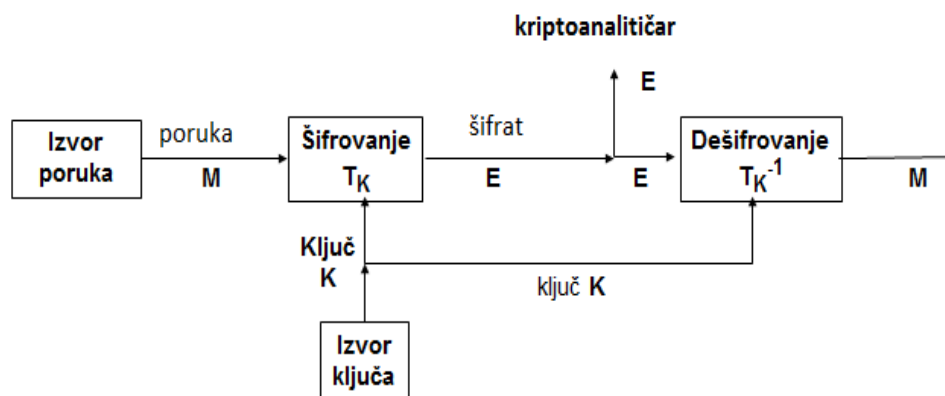
Socijalno ekonomske i bezbednosne dimenzije zahtevaju rešenje u kom sistemsko izučavanje bazičnih teorijskih pristupa predstavlja nezaobilazan zahtev.

Preko slike (Slika 1.2) posmatraćemo celu oblast - kriptologije. Ljubičasta boja predstavlja cilj, zelena boja vrstu algoritma i žuta tip bezbednosti. Ako nam je cilj tajnost i autentičnost, tada algoritmi sa kojima to možemo postići mogu biti sa jednim ključem ili sa dva ključa. Algoritmi sa jednim ključem su simetrični algoritmi, a algoritmi sa dva ključa su asimetrični šifarski algoritmi. Tip bezbednosti koju postizemo može biti bezuslovna i računarska. Na slici treba приметiti da je polje bezuslovne sigurnosti vezano samo za jedan ključ, dok je računarska (ili praktična) vezana za algoritme sa jednim i sa dva ključa.



Slika 1.2 Deskriptivni dijagram kriptologije kao oblasti

U nastavku ovog odeljka diskutovaćemo o tome kako je Šenon postavio teorijske osnove analize šifarskih sistema, posebno kada je reč o bezuslovnoj bezbednosti koja je propagirana preko perfektnih šifarskih sistema, slika (Slika 1.3). Pre Šenonovih naučnih radova, to nije imalo svoju matematičku postavku.



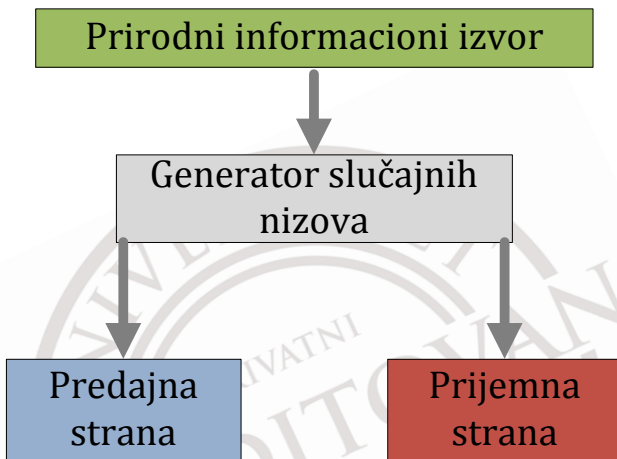
Slika 1.3 Šenonov model tajnog komuniciranja

Po Šenonu, „Prvi korak u matematičkoj analizi kriptografije zahteva idealizaciju procesa komuniciranja na takav način da omogući definiciju kriptografskog sistema na matematički prihvatljiv način“.

Njegova osnovna generička šema prikazana je na slici (Slika 1.3). Pretpostavimo da imamo neki izvor poruka i generisane poruke ćemo označiti sa M . U bloku šifrovanje imamo jedan skup transformacija koje ćemo da označimo sa T_K . Indeks K je vezan za kriptološki ključ. Ključ K je dobijen preko bloka izvor ključeva. Rezultat jedne iz skupa različitih transformacija za zadatu poruku M i ključ K , generisaće šifrat E . Druga strana ili prijemna strana da bi dešifrovala poruku, mora da primeni odgovarajuću inverznu transformaciju T_K^{-1} , nakon čega će generisati poruku M , koja će biti identična poruci na predajnoj strani. Ova šema predstavlja neki osnovni koncept. Pored svih funkcionalnih blokova u šemi, postoji i neko ko napada ovaj sistem i ta tačka je označena sa „neprijateljski kriptoanalitičar“.

Principijelna ideja cele kriptologije je da transformacije koje se koriste budu poznate i kriptografu i kriptoanalitičaru, a jedino što kriptoanalitičar ne zna su ključevi (Kerkehofi principi). Ova šema je dizajnirana na osnovu simetričnih siste-

mima sa javnim ključem. Da bi smo bolje razumeli počecemo od Šenona koji je definisao dva tipa bezbednosti. Prva je bezuslovna bezbednost, što znači da se za zadati kriptografski sistem može rigorozno dokazati nominovana bezbednost u odnosu na protivnika koji raspolaže neograničenim vremenskim i računarskim resursima. Danas se ova bezbednost naziva informaciono-teorijska bezbednost. Šifra koja odgovara datom opisu bezuslovne bezbednosti je *One-time pad* i predstavlja Šenonov ideal apsolutne bezbednosti (simetrična šifra).

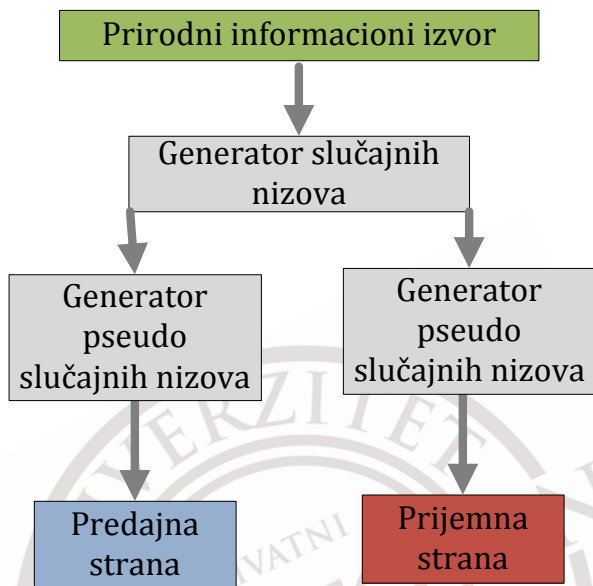


Slika 1.4 Šenonov ideal

Na slici (Slika 1.4) prikazan je prirodni informacioni izvor koji se koristi kao generator slučajnih nizova (kriptoloških ključeva). Najkvalitetnije generatore slučajnih nizova moguće je pronaći u prirodnim okruženjima. Ujedno, dobijeni slučajni niz iz datog informacionog izvora predstavlja ključ koji se koristiti za šifrovanje kod *One-time pad* šifarskog algoritma. Način koji je prikazan na slici je isuviše zahtevan. Potrebno je obezbediti kopije nizova na obe strane, a oni će se kasnije koristiti kao ključevi. Drugi problem je što dužina ključeva mora da bude jednake dužine kao i poruka.

Druga bezbednost koju je Šenon definisao je dokaziva računarska bezbednost, što znači da se za zadati kriptografski sistem može rigorozno dokazati nominovana bezbednost u odnosu na protivnika koji poseduje specifične vremenske i računarske resurse. Šifre koje najviše odgovaraju definiciji računarske sigurnosti su iz

kategorije simetričnih (sekvencijalne šifre) i asimetričnih (*RSA*) algoritama i po Šenonu predstavljaju pseudo ideal računarske sigurnosti.



Slika 1.5 Šenonov pseudo ideal

Na slici (Slika 1.5), prikazan je prirodni informacijski izvor koji ima ulogu generatora slučajnih nizova koji se koriste kao inicijalna stanja pseudo slučajnih generatora za generisanje pseudo slučajnih nizova. Na ovaj način je iskorišćena neodređenost prirodnog izvora u fiksnim dimenzijama, nezavisno od dužine poruke. Na primer, *A5/1* sekvencijalna šifra u svoja tri registra smešta 64 bita unutrašnjeg ključa, na osnovu koga kasnije generiše radni ključ za šifrovanje ogromnog broja poruka. *A5/1* se uglavnom koristi za zaštitu govora (*GSM*), zbog svoje podobnosti za hardversku realizaciju.

U ovom primeru možemo da pretpostavimo scenario u kome smo generisali niz od 64 bita, koji smo zatim iskoristili kao unutrašnji ključ *A5/1*, a pseudo generator sa slike je upravo sekvencijalni algoritam *A5/1* koji generiše radene ključeve za proces šifrovanja.

Prednost pseudo ideala je velika u odnosu na Šenonov apsolutni ideal kada je reč o kriptografskim sistemima. Sada je potrebno distribuirati kopiju ključa od 64

bita na drugu stranu, nakon čega može da otpočne šifrovanje velike količine podataka.

U slučaju pseudo ideala sa *One-Time pad* šifrom, proces šifrovanja se svodi na *XOR* operaciju nad bitovima otvorene poruke i bitovima pseudo slučajne sekvence (radnog ključa). Dešifrovanje se vrši identičnim pseudo slučajnim nizom na prijemu koji se *XOR*-uje sa dobijenim bitovima šifrata. Korišćenje pseudo slučajne sekvence (engl. *Keystream*) je identično korišćenju ključa kod *One-Time pad*-a i naziva se radni ključ koji je generisan na osnovu ključa dobijenog preko prirodnog informacionog izvora. Kod sistema koji se odnose na Šenonov pseudo ideal, upotrebom pseudo generatora žrtvovana je apsolutna tajnost – perfektna tajnost.

Često smo koristili termin nominovana bezbednost. Nominovana bezbednost predstavlja pažljiv i kompletan opis operacionog scenarija, u kome se egzaktno daje:

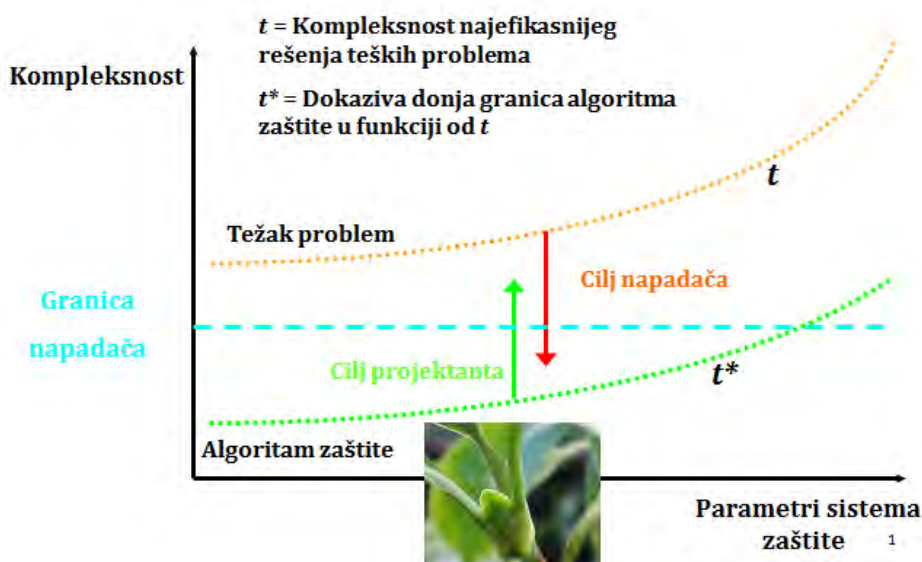
- Od kakvih napada kriptografski sistem treba da obezbedi zaštitu?
- Šta je poznato napadaču?
- Šta je poznato korisnicima sistema?
- Sve fizičke pretpostavke, koje bliže određuju šta napadač i korisnici sistema mogu da urade?

Međutim, paradoks savremenog stanja stvari po pitanju dokazive bezbednosti je neočekivan. Krajnji zaključak je da dokaziva bezuslovna bezbednost predstavlja „REALNOST“, dok dokaziva računarska – praktična bezbednost predstavlja „MIT“.

1.4. PRAKTIČNA BEZBEDNOST

Razmotrićemo malo detaljnije praktičnu bezbednost. Ako koristimo ključeve koji su nezavisni od poruka, ako koristimo ključeve koji su dužine iste kao poruka i ako se ključevi ne ponavljaju, tada imamo apsolutno tajan sistem. Tačnije, ukoliko imamo napadača koji napada na sistem pod ovim uslovima, tako što isprobava sve moguće ključeve, dobijaće sve smislene poruke na svetu. Napadač kada dobije sve smislene poruke shvatiće i da nije morao to da radi, jer neće znati šta je prava smisljena poruka. Ovakav sistem nazivamo perfektnim šifarskim sistemima, ali u ovom odeljku nije reč o takvim sistemima već o uslovno bezbednim ili praktično bezbednim šifarskim sistemima.

Kod praktično bezbednih sistema ključevi su žrtvovani, tako što su značajno kraći u odnosu na poruke. Ovim oni nude neku drugu vrstu tajnosti koju je Šenon definisao kao količinu rada koju treba da sprovede kriptanalitičar da bi došao do pravog ključa. Pogledaćemo šta zapravo praktična bezbednost predstavlja u matematičkom smislu. Razmotrimo dijagram sa slike (Slika 1.6).



Slika 1.6 Praktična sigurnost

Da bismo projektovali jedan sistem koji obezbeđuje praktičnu bezbednost, recimo jedan pseudo slučajni generator (*AES*, *DES*) i tvrdili šta je njegova praktična bezbednost, morali bismo da uradimo nekoliko sledećih koraka.

Prvo moramo da kažemo da je rešavanje problema kriptanalize tog algoritma ekvivalentno sa nekim matematičkim problemom i da formulišemo o kom je matematičkom problemu reč. U sledećem koraku treba da se bavimo sa kompleksnosti tog matematičkog problema i da pokušamo u njemu da nađemo donju granicu. Donja granica tog problema označena je sa zelenom linijom i predstavlja cilj projektanta tog sistema. Donja granica pretpostavlja neophodan računarski resurs koji je potreban napadaču za rešavanje tog problema. Da bismo razumeli značaj donje granice, navešćemo uslov koji ona treba da ispuni. Donja granica uvek mora biti ispod granice napadača. Da bi ovaj uslov bio ispunjen, projektant sistema mora da zna kolika je računarska snaga tog napadača. Ako je računarska snaga napadača veća od donjih granica, to znači da kriptanalitičar koji napada taj sistem, može da reši taj problem koji je ekvivalentan matematičkom problemu.

Ovakva teorija nam omogućava da podešavamo parametre šifarskog sistema. Ukoliko bismo mogli da podignemo granicu napadača iznad donje granice sistema, to bi praktično značilo da imamo bezbedan sistem nalik na onaj koji je apsolutno tajan. Da bismo mogli da uradimo ovako nešto, neophodno je da posegnemo za nekom matematičkom teorijom koja se bavi proučavanjem algoritamske kompleksnosti. Međutim, može se učiniti da takva teorija nije osmišljena za kriptologiju i iz tog razloga je treba izbegavati.

1.4.1. EKVIVOKACIJA KLJUČA I TAČKA JEDINSTVENOSTI

U praksi se često odstupa od perfektnih šifara zbog kompromisa između nivoa potrebne tajnosti i cene uvođenja jednog šifarskog sistema. Široko je rasprostranjena klasa neperfektnih šifarskih sistema, čiji je ključ znatno manji od poruka i koristi se veliki broj puta. Šenon je uveo tzv. ekvivokacionu funkciju, definisanu na skupu prirodnih brojeva:

$$\alpha(n) = H(K|C_1 \dots C_n).$$

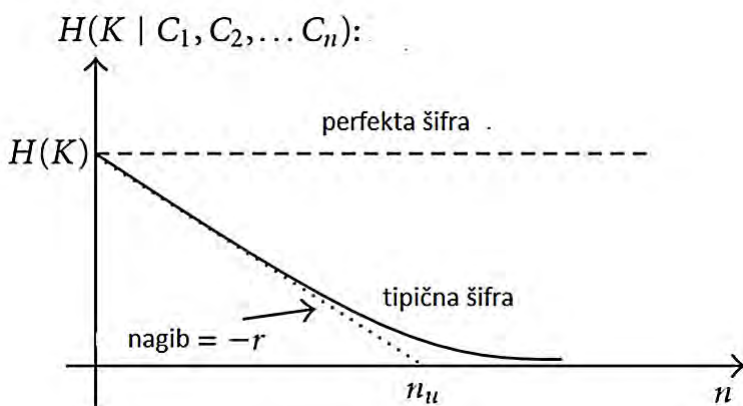
Intuitivno je jasno da što više šifrata C imamo na raspolaganju, sve će se više smanjivati neodređenost ključa K . Formalno, to bi značilo:

$$\lim_{n \rightarrow \infty} \alpha(n) = 0$$

Tačka jedinstvenosti se definiše kao najmanje n za koje je $\alpha(n) \cong 0$. Tačka jedinstvenosti datog kriptosistema je najmanje n za koje važi:

$$H(K|C_1 \dots C_n) \cong 0.$$

Po definiciji, tačka jedinstvenosti je najmanja količina šifrata kojom mora raspolagati kriptanalitičar, da bi mogao da odredi ključ K jednoznačno. Drugim rečima to je najmanja količina šifrata koja omogućava da sistem bude razbijen.



Slika 1.7 Tačka jedinstvenosti – perfektne i neperfektne šifre

M i C su iste dužine n i pripadaju istom alfabetu. Šifrovane poruke imaju približno maksimalnu neodređenost:

$$H(C_n) \cong n \log D,$$

što je kriterijum kome teže svi dizajneri kriptosistema.

Ključevi i poruke su nezavisni

$$H(M_n, K) = H(M_n) + H(K),$$

što je uobičajeno i prirodno. Tada je tačka jedinstvenosti aproksimativno jednaka

$$u \approx \frac{H(K)}{R(M) \cdot \log D},$$

gde je $R(M)$ redundansa poruka M koje se šifruju, definisana sa:

$$R(M) = 1 - \frac{H_\infty(M)}{\log D}.$$

DOKAZ:

Pretpostavimo da je n dovoljno veliko, tako da važi:

$$H(M_n) \approx n \cdot H_\infty(M),$$

$$\begin{aligned} H(K|C_n) &= \overbrace{H(M_n K C_n) - H(M_n | K C_n)}^{H(K C_n)} - H(C_n) = H(M_n K C_n) - H(C_n) \\ &= H(M_n K) - H(C_n) = H(M_n) + H(K) - H(C_n) \\ &= n \cdot H_\infty(M) + H(K) - n \cdot \log D \end{aligned}$$

Tačka jedinstvenosti je definisana sa:

$$H(K|C_u) = 0,$$

odnosno:

$$u(H_\infty(M) - \log D) + H(K) = 0,$$

odakle sledi:

$$u = \frac{H(K)}{\log D - H_\infty(M)} = \frac{H(K)}{R(M) \cdot \log D}.$$

Na primer, posmatrajmo poruke pisane na engleskom jeziku sa 27 znakova uključujući razmake između reči i šifrovane ključem koji se sastoji od 20 nezavisnih karaktera engleskog alfabeta.

Tada je

$$H(K) = 20 \log 27.$$

Ako za engleski jezik usvojimo entropiju od 2 bita po znaku, redundansa poruka je data sa $R(M) = 1 - 2/\log 27 \approx 0.58$. Tačka jedinstvenosti ovog šifarskog sistema je data sa:

$$u = \frac{H(K)}{R \log D} = \frac{20 \cdot \log(27)}{\log(27) - 2} \cong 35$$

Ovaj rezultat znači da sa poznavanjem šifrata dužine oko 35 karaktera, ključ se može odrediti jednoznačno.

Primetimo da je tačka jedinstvenosti u , principijelno, količina šifrata dovoljna za jednoznačno određivanje ključa. Međutim, o samom konkretnom načinu i složenosti određivanja ključa K na osnovu poznavanja šifrata nema nijedne reči u Šenonovim radovima.

1.4.2. POVEĆANJE TAČKE JEDINSTVENOSTI

Iz same definicije tačke jedinstvenosti vidimo da je jedan mogući način za njeno povećavanje, smanjivanje redundanse poruka koje se šifruju, odnosno povećanje njihove entropije.

Stoga je na primer dobra ideja komprimovati poruke pre šifrovanja. Predlažemo uvođenje nekog metoda za kompresiju. Na primer, Hafamanovo tzv. entropijsko kodovanje.

I zaista za najbolje moguće komprimovanje:

$$H(M_n) \cong n \log D, \quad R(M) \cong 0, \quad u \rightarrow \infty.$$

PRIMER 1

Tačka jedinstvenosti kriptosistema kojim se šifruju poruke iz alfabeta od 96 znakova, pri čemu je entropija poruka 3 bita/po znaku, dok je entropija ključa 33 bita je:

$$u = \frac{33}{\log 96 - 3} = 9.2,$$

$$R = 1 - \frac{3}{\log 96} = 54.4\%.$$

PRIMER 2

Tačka jedinstvenosti kript sistema kojim se šifruju binarne poruke, redundanse 25%, dok su ključevi dužine 16 bita i uniformno su raspodeljeni je:

$$u = \frac{16}{0.25 \cdot 1} = 64.$$



1.5. VEROVATNOSNI MODEL ŠIFROVANJA

U ovom primeru verovatnosnog modela šifrovanja upotrebićemo samo jedan ključ i izvršiti jedno šifrovanje. Neka postoji raspodela verovatnoće nad prostom poruka P . Označimo apriornu verovatnoću izbora otvorenog teksta x sa $P_P(x)$.

Neka je ključ K izabran u skladu sa nekom fiksnom raspodelom verovatnoće. Najčešće se ključ bira slučajno, tako da su svi ključevi jednako verovatni, što u opštem slučaju ne mora biti tako.

Označimo ovu raspodelu ključeva sa $P_K(K)$. Podsetimo se da se ključ bira nezavisno od poruke, tako da su ključ K i poruka x , dve nezavisne slučajne veličine.

Dve raspodele verovatnoća nad skupovima P i K indukuju (određuju) raspodelu verovatnoća nad skupom šifrata C . Nađimo ovu raspodelu.

Za fiksno $K \in K$, definišemo:

$$C(K) = \{e(K, x) : x \in P\},$$

odnosno $C(K)$ predstavlja skup mogućih šifrata ako se upotrebi konkretni ključ K . Sa $e(K, x)$ je označen šifrat koji se dobija šifrovanjem poruke x sa ključem K .

Tada za svako $y \in C$ imamo:

$$P_C(y) = \sum_{\{K: y \in C(K)\}} P_K(K) P_P(d(K, y)),$$

gde je sa $d(K, y)$ označen otvoren tekst x dobijen na osnovu šifrata y postupkom dešifrovanja $d(K, \cdot)$ sa ključem K .

Za svako $y \in C$ i $x \in P$, možemo izračunati uslovnu raspodelu verovatnoće $P_C(y|x)$, odnosno verovatnoću da je y šifrat, pod uslovom da je x otvoreni tekst

$$P_C(y|x) = \sum_{\{K: x=d(K,y)\}} P_K(K).$$

Sada je moguće naći i uslovnu raspodelu verovatnoća $P_P(x|y)$, odnosno verovatnoću da je x otvoreni tekst, kada se zna da je y šifrat, korišćenjem Bajesove teoreme:

$$P_P(x|y) = \frac{P_P(y)P_C(y|x)}{P_y(y)} = \frac{P_P(y) \sum_{\{K: x=d(K,y)\}} P_K(K)}{P_C(y) = \sum_{\{K: y \in C(K)\}} P_K(K)P_P(d(K,y))}.$$

Prosledimo računanje ovih verovatnoća na jednom primeru.

PRIMER 1

Neka je $P = \{a, b\}$, pri čemu je $P_P(a) = \frac{1}{4}$, $P_P(b) = \frac{3}{4}$. Neka je $K = \{K_1, K_2, K_3\}$, sa verovatnoćama $P_K(K_1) = \frac{1}{2}$, $P_K(K_2) = \frac{1}{4}$, $P_K(K_3) = \frac{1}{4}$.

Neka je $C = \{1, 2, 3, 4\}$ i pretpostavimo da je šifrovanje predstavljeno Tabelom 1:

Tabela 1.1 Matrica šifrovanja za krypto sistem iz Primera 1

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Izračunajmo raspodelu verovatnoće:

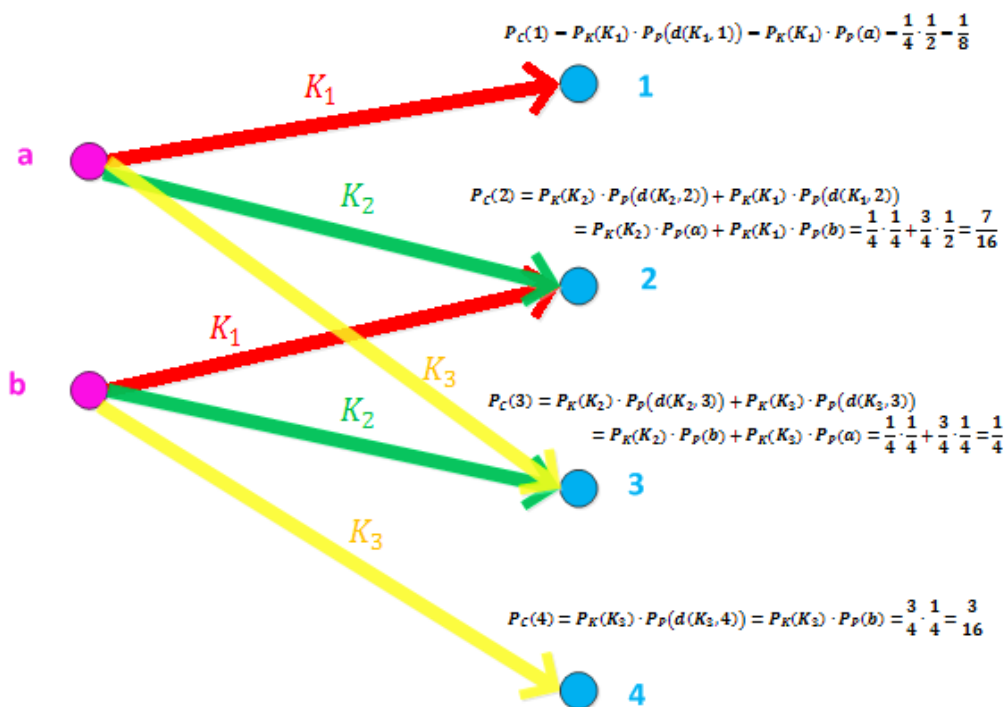
$$P_C(1) = P_K(K_1) \cdot P_P(d(K_1, 1)) = P_K(K_1) \cdot P_P(a) = \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{8}$$

$$\begin{aligned} P_C(2) &= P_K(K_2) \cdot P_P(d(K_2, 2)) + P_K(K_1) \cdot P_P(d(K_1, 2)) \\ &= P_K(K_2) \cdot P_P(a) + P_K(K_1) \cdot P_P(b) = \frac{1}{4} \cdot \frac{1}{4} + \frac{3}{4} \cdot \frac{1}{2} = \frac{7}{16} \end{aligned}$$

$$\begin{aligned} P_C(3) &= P_K(K_2) \cdot P_P(d(K_2, 3)) + P_K(K_3) \cdot P_P(d(K_3, 3)) \\ &= P_K(K_2) \cdot P_P(b) + P_K(K_3) \cdot P_P(a) = \frac{1}{4} \cdot \frac{1}{4} + \frac{3}{4} \cdot \frac{1}{4} = \frac{1}{4} \end{aligned}$$

$$P_C(4) = P_K(K_3) \cdot P_P(d(K_3, 4)) = P_K(K_3) \cdot P_P(b) = \frac{3}{4} \cdot \frac{1}{4} = \frac{3}{16}$$

Na slici (Slika 1.8) dat je graf šifarskog sistema, iz koga se vidi jasnije postupak izračunavanja verovatnoća simbola šifrata na osnovu verovatnoća simbola otvorenog teksta i verovatnoća simbola ključeva.



Slika 1.8 Graf šifarskog sistema

Graf šifarskog sistema iz Primera 1, sa odgovarajućim verovatnoćama šifrata. Nakon izračunavanja raspodele verovatnoća šifrata, možemo pristupiti računanju uslovnih verovatnoća otvorenog teksta, kada je kriptanalitičaru dostupan odgovarajući šifrat.

$$P_P(a|1) = \frac{P_P(a) \cdot P_C(1|a)}{P_C(1)} = \frac{P_P(a) \cdot P_K(K_1)}{P_K(K_1) \cdot P_P(a)} = 1,$$

$$P_P(a|2) = \frac{P_P(a) \cdot P_C(2|a)}{P_C(2)} = \frac{P_P(a) \cdot P_K(K_2)}{P_K(K_2) \cdot P_P(a) + P_K(K_1) \cdot P_P(b)} = \frac{\frac{1}{4} \cdot \frac{1}{4}}{\frac{7}{16}} = \frac{1}{7}$$

$$P_P(a|3) = \frac{P_P(a) \cdot P_C(3|a)}{P_C(3)} = \frac{P_P(a) \cdot P_K(K_3)}{P_K(K_2) \cdot P_P(b) + P_K(K_3) \cdot P_P(a)} = \frac{\frac{1}{4} \cdot \frac{1}{4}}{\frac{1}{4}} = \frac{1}{4}$$

$$P_P(a|4) = \frac{P_P(a) \cdot P_C(4|a)}{P_C(4)} = \frac{P_P(a) \cdot 0}{P_C(4)} = 0.$$

$$P_P(b|1) = \frac{P_P(b) \cdot P_C(1|b)}{P_C(1)} = \frac{P_P(b) \cdot 0}{P_K(K_1) \cdot P_P(a)} = 0$$

$$P_P(b|2) = \frac{P_P(b) \cdot P_C(2|b)}{P_C(2)} = \frac{P_P(b) \cdot P_K(K_1)}{P_K(K_2) \cdot P_P(a) + P_K(K_1) \cdot P_P(b)} = \frac{\frac{3}{4} \cdot \frac{1}{2}}{\frac{7}{16}} = \frac{6}{7}$$

$$P_P(b|3) = \frac{P_P(b) \cdot P_C(3|b)}{P_C(3)} = \frac{P_P(b) \cdot P_K(K_2)}{P_K(K_2) \cdot P_P(b) + P_K(K_3) \cdot P_P(a)} = \frac{\frac{3}{4} \cdot \frac{1}{4}}{\frac{1}{4}} = \frac{3}{4}$$

$$P_P(b|4) = \frac{P_P(b) \cdot P_C(4|b)}{P_C(4)} = \frac{P_P(b) \cdot P_K(K_3)}{P_K(K_3) \cdot P_P(b)} = 1.$$

Odavde vidimo da nisu zadovoljeni uslovi apsolutne tajnosti, budući da je:

$$P_P(a|1) = 1 \neq P_P(a) = \frac{1}{4}$$

$$P_P(a|2) = \frac{1}{7} \neq P_P(a) = \frac{1}{4}$$

$$P_P(a|3) = \frac{1}{4} = P_P(a) = \frac{1}{4}$$

$$P_P(a|4) = 0 \neq P_P(a) = \frac{1}{4}$$

$$P_P(b|1) = 0 \neq P_P(b) = \frac{3}{4}$$

$$P_P(b|2) = \frac{6}{7} \neq P_P(b) = \frac{3}{4}$$

$$P_P(b|3) = \frac{3}{4} = P_P(b) = \frac{3}{4}$$

$$P_P(b|4) = 1 \neq P_P(b) = \frac{3}{4}$$

Izračunajmo sada uslovne raspodele verovatnoća $P(K_i|j)$, $1 \leq i \leq 3$, $1 \leq j \leq 4$.
Primenjujući Bajsovu formulu dobijamo:

$$P(K_i|j) = \frac{P_K(K_i) \cdot P_C(j|K_i)}{P_C(j)}$$

$$P(K_1|1) = \frac{P_K(K_1) \cdot P_C(1|K_1)}{P_C(1)} = \frac{P_K(K_1) \cdot P_P(a)}{P_K(K_1) \cdot P_P(a)} = 1$$

$$P(K_1|2) = \frac{P_K(K_1) \cdot P_C(2|K_1)}{P_C(2)} = \frac{P_K(K_1) \cdot P_P(b)}{P_K(K_2) \cdot P_P(a) + P_K(K_1) \cdot P_P(b)} = \frac{\frac{1}{2} \cdot \frac{3}{4}}{\frac{7}{16}} = \frac{6}{7}$$

$$P(K_1|3) = \frac{P_K(K_1) \cdot P_C(3|K_1)}{P_C(3)} = \frac{P_K(K_1) \cdot 0}{P_K(K_2) \cdot P_P(b) + P_K(K_3) \cdot P_P(a)} = 0$$

$$P(K_1|4) = \frac{P_K(K_1) \cdot P_C(4|K_1)}{P_C(4)} = \frac{P_K(K_1) \cdot 0}{P_K(K_3) \cdot P_P(b)} = 0$$

$$P(K_2|1) = \frac{P_K(K_2) \cdot P_C(1|K_2)}{P_C(1)} = \frac{P_K(K_2) \cdot 0}{P_K(K_1) \cdot P_P(a)} = 0$$

$$P(K_2|2) = \frac{P_K(K_2) \cdot P_C(2|K_2)}{P_C(2)} = \frac{P_K(K_2) \cdot P_P(a)}{P_K(K_2) \cdot P_P(a) + P_K(K_1) \cdot P_P(b)} = \frac{\frac{1}{4} \cdot \frac{1}{4}}{\frac{7}{16}} = \frac{1}{7}$$

$$P(K_2|3) = \frac{P_K(K_2) \cdot P_C(3|K_2)}{P_C(3)} = \frac{P_K(K_2) \cdot P_P(b)}{P_K(K_2) \cdot P_P(b) + P_K(K_3) \cdot P_P(a)} = \frac{\frac{1}{4} \cdot \frac{3}{4}}{\frac{1}{4}} = \frac{3}{4}$$

$$P(K_2|4) = \frac{P_K(K_2) \cdot P_C(4|K_2)}{P_C(4)} = \frac{P_K(K_2) \cdot 0}{P_K(K_3) \cdot P_P(b)} = 0$$

$$P(K_3|1) = \frac{P_K(K_3) \cdot P_C(1|K_3)}{P_C(1)} = \frac{P_K(K_3) \cdot 0}{P_K(K_1) \cdot P_P(a)} = 0$$

$$P(K_3|2) = \frac{P_K(K_3) \cdot P_C(2|K_3)}{P_C(2)} = \frac{P_K(K_3) \cdot 0}{P_K(K_2) \cdot P_P(a) + P_K(K_1) \cdot P_P(b)} = 0$$

$$P(K_3|3) = \frac{P_K(K_3) \cdot P_C(3|K_3)}{P_C(3)} = \frac{P_K(K_3) \cdot P_P(a)}{P_K(K_2) \cdot P_P(b) + P_K(K_3) \cdot P_P(a)} = \frac{\frac{1}{4} \cdot \frac{1}{4}}{\frac{1}{4}} = \frac{1}{4}$$

$$P(K_3|4) = \frac{P_K(K_3) \cdot P_C(4|K_3)}{P_C(4)} = \frac{P_K(K_3) \cdot P_P(b)}{P_K(K_3) \cdot P_P(b)} = 1$$

Ekvivokacija ključeva

$$H(K|C) = H(K) + H(P) - H(C)$$

Proverimo ovaj stav, prvo računanjem svih komponenti pojedinačno:

$$H(P) = -\frac{1}{4} \log_2 \frac{1}{4} - \frac{3}{4} \log_2 \frac{3}{4} = -\frac{1}{4}(-2) - \frac{3}{4}(\log_2 3 - 2) = 0.8113$$

$$H(C) = -\frac{1}{8} \log_2 \frac{1}{8} - \frac{7}{16} \log_2 \frac{7}{16} - \frac{1}{4} \log_2 \frac{1}{4} - \frac{3}{16} \log_2 \frac{3}{16} = 1.8496$$

$$H(K) = -\frac{1}{2} \log_2 \frac{1}{2} - \frac{1}{4} \log_2 \frac{1}{4} - \frac{1}{4} \log_2 \frac{1}{4} = 1.5$$

Stoga je:

$$H(K|C) = H(K) + H(P) - H(C) = 1.5 + 0.8113 - 1.8496 = 0.4617.$$

Direktnim računanjem uslovne entropije $H(K|C)$ dobijamo:

$$H(K|C) = - \sum_C P_C(c) \sum_K P(k|c) \log_2 P(k|c) =$$

$$[-P(K_1|1) \cdot \log_2 P(K_1|1) - P(K_2|1) \cdot \log_2 P(K_2|1) - P(K_3|1) \cdot \log_2 P(K_3|1)] \cdot P_C(1) -$$

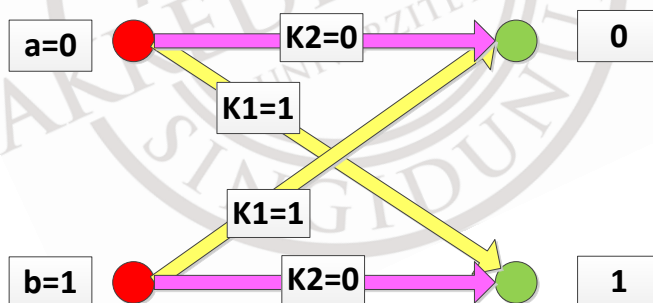
$$\begin{aligned}
& [-P(K_1|2) \cdot \log_2 P(K_1|2) - P(K_2|2) \cdot \log_2 P(K_2|2) - P(K_3|2) \cdot \log_2 P(K_3|2)] \cdot P_C(2) - \\
& [-P(K_1|3) \cdot \log_2 P(K_1|3) - P(K_2|3) \cdot \log_2 P(K_2|3) - P(K_3|3) \cdot \log_2 P(K_3|3)] \cdot P_C(3) - \\
& [-P(K_1|4) \cdot \log_2 P(K_1|4) - P(K_2|4) \cdot \log_2 P(K_2|4) - P(K_3|4) \cdot \log_2 P(K_3|4)] \cdot P_C(4) = \\
& \frac{1}{8} \cdot 0 + \frac{7}{16} \cdot 0.59 + \frac{1}{4} \cdot 0.81 + \frac{3}{16} \cdot 0 = 0.4617,
\end{aligned}$$

čime se uveravamo u identičnost rezultata dobijenih direktnim računanjem i na osnovu Šenonove formule za ekvivokaciju ključa u odnosu na šifrat.

PRIMER 2 - One-Time pad

Tabela 1.2 Tabela prikaz šifarske transformacije

	a=1	b=0
K ₁ =1	0	1
K ₂ =0	1	0



Slika 1.9 Grafovski prikaz šifarske transformacije

Verovatnoće simbola šifrata

$$P_C(0) = P_P(a)P(K_2) + P_P(b)P(K_1)$$

$$P_C(1) = P_P(a)P(K_1) + P_P(b)P(K_2)$$

Uslovne verovatnoće simbola poruka za poznati šifrat

$$P_P(a|c=0) = \frac{P_C(c=0|a)P_P(a)}{P_C(c=0)} = \frac{P(K_2)P_P(a)}{P_P(a)P(K_2) + P_P(b)P(K_1)}$$

$$P_P(a|c=1) = \frac{P_C(c=1|a)P_P(a)}{P_C(c=1)} = \frac{P(K_1)P_P(a)}{P_P(a)P(K_1) + P_P(b)P(K_2)}$$

$$P_P(b|c=0) = \frac{P_C(c=0|b)P_P(b)}{P_C(c=0)} = \frac{P(K_1)P_P(b)}{P_P(a)P(K_2) + P_P(b)P(K_1)}$$

$$P_P(b|c=1) = \frac{P_C(c=1|b)P_P(b)}{P_C(c=1)} = \frac{P(K_2)P_P(b)}{P_P(a)P(K_1) + P_P(b)P(K_2)}$$

Uslovne verovatnoće ključeva za poznat šifrat

$$P(K_1|0) = \frac{P_K(K_1) \cdot P_C(0|K_1)}{P_C(0)} = \frac{P_K(K_1) \cdot P_P(b)}{P_P(a)P(K_2) + P_P(b)P(K_1)}$$

$$P(K_1|1) = \frac{P_K(K_1) \cdot P_C(1|K_1)}{P_C(1)} = \frac{P_K(K_1) \cdot P_P(a)}{P_P(a)P(K_1) + P_P(b)P(K_2)}$$

$$P(K_2|0) = \frac{P_K(K_2) \cdot P_C(0|K_2)}{P_C(0)} = \frac{P_K(K_2) \cdot P_P(a)}{P_P(a)P(K_2) + P_P(b)P(K_1)}$$

$$P(K_2|1) = \frac{P_K(K_2) \cdot P_C(1|K_2)}{P_C(1)} = \frac{P_K(K_2) \cdot P_P(b)}{P_P(a)P(K_1) + P_P(b)P(K_2)}$$

Neka je $P(K_1) = P(K_2) = 0.5$, tada je:

$$P_C(0) = P_P(a) 0.5 + P_P(b) 0.5 = 0.5,$$

$$P_C(1) = P_P(a) 0.5 + P_P(b) 0.5 = 0.5,$$

nezavisno od toga kolike su verovatnoće simbola izvora $P(a)$ i $P(b)$. Dalje je:

$$P_P(a|c = 0) = \frac{P(c = 0|a)P_P(a)}{P(c = 0)} = \frac{P_P(a)}{P_P(a) + P_P(b)} = P_P(a),$$

$$P_P(a|c = 1) = \frac{P(c = 1|a)P_P(a)}{P(c = 1)} = \frac{P_P(a)}{P_P(a) + P_P(b)} = P_P(a),$$

$$P_P(b|c = 0) = \frac{P(c = 0|b)P_P(b)}{P(c = 0)} = \frac{P_P(b)}{P_P(a) + P_P(b)} = P_P(b)$$

$$P_P(b|c = 1) = \frac{P(c = 1|b)P_P(b)}{P(c = 1)} = \frac{P_P(b)}{P_P(a) + P_P(b)} = P_P(b)$$

Odakle sledi da se iz šifrata ništa ne može saznati o porukama, budući da su uslovne verovatnoće poruka, ako znamo šifrat, jednake безусловnim verovatnoćama poruka.

Ekvivokacija ključeva

$$H(K|C) = H(K) + H(P) - H(C)$$

$$H(K) = -0.5 \log_2 0.5 - 0.5 \log_2 0.5 = 1$$

$$H(P) = -P_P(a) \log_2 P_P(a) - P_P(b) \log_2 P_P(b)$$

$$\begin{aligned}
 H(C) &= -P_C(1) \log_2 P_C(1) - P_C(0) \log_2 P_C(0) = - (P_P(a)P(K_1) \\
 &\quad + P_P(b)P(K_2)) \log_2 (P_P(a)P(K_1) + P_P(b)P(K_2)) - (P_P(a)P(K_1) \\
 &\quad + P_P(b)P(K_2)) \log_2 (P_P(a)P(K_1) + P_P(b)P(K_2)) \\
 &= -0.5 \log_2 0.5 - 0.5 \log_2 0.5 = 1
 \end{aligned}$$

Ekvivokacija ključeva

$$\begin{aligned}
 H(K|C) &= H(K) + H(P) - H(C) = H(P) = -P_P(a) \log_2 P_P(a) - P_P(b) \log_2 P_P(b) \\
 &= \text{const.}
 \end{aligned}$$



2. AUTENTIFIKACIJA

Protokol predstavlja skup pravila kojih se pridržavamo u nekoj komunikaciji. Dobar i jednostavan primer su ljudski protokoli u kojima postoje jasna pravila kojih se pridržavamo u komunikaciji sa drugim ljudima.

U praksi to može biti razgovor između studenta i profesora u momentu kada student želi da postavi pitanje profesoru. Tu komunikaciju možemo da predstavimo kroz nekoliko koraka koji zajedno čine jedan ljudski protokol.

Na primer:

1. Student podiže dva prsta u vis.
2. Profesor mu daje mogućnost da postavi pitanje.
3. Student postavlja pitanje.
4. Profesor odgovara na pitanje.

Svakako, ovo je primer jednostavnog ljudskog protokola. Postoji ogroman broj ljudskih protokola od kojih neki mogu da budu vrlo složeni i mogu da uključuju u komunikaciju više od jednog sagovornika.

Sada, u kontekstu umrežavanja možemo da nastavimo priču u smeru mrežnih protokola koji predstavljaju skupove pravila u mrežnim komunikacionim sistemima. U mrežnim protokolima imamo hardver umesto čoveka i algoritme koji simuliraju komunikaciju, nalik na onu između dva čoveka u stvarnom životu.

Najpoznatiji mrežni protokoli su: *HTTP, FTP, UDP, TCP, PPP* i mnogi drugi protokoli. Zapravo proučavanje računarskih mreža u velikoj meri se odnosi na proučavanje mrežnih protokola.

U nastavku prelazimo sa standardnih računarskih protokola na bezbednosne protokole ili kriptografske protokole koji primenjuju dodatne pod skupove pravila u cilju uspostavljanja bezbedne komunikacije između učesnika u računarskoj mreži na mestima gde je to neophodno. Najpoznatiji kriptografski protokoli su: *SSL, SSH, IPsec, WEP* i *Kerberos*.

Protokoli koje smo naveli, isuviše su složeni da bismo mogli odmah da se bavimo njihovim dizajnom i pravilima koja odlikuju njihov dizajn. Iz tog razloga u ovom

poglavlju bavićemo se pojednostavljenim protokolima koji imaju zadatak da obezbede autentifikaciju. Na ovaj način ćemo lakše razumeti osnovne elemente sigurnosti koji su implementirani kod ovih protokola. Kasnije kada budemo dublje ulazili u dizajn kriptografskih protokola današnjice, biće neophodno dobro poznavanje gradiva iz udžbenika „Kriptologija 1“.

U nastavku ovog teksta upoznaćemo se sa osnovnim elementima bezbednosti koji su vezani za poruke koje se šalju preko mreže za proveru identiteta učesnika komunikacije. Videćemo primere poznatih vrsta napada na protokole i daćemo neke smernice za sprečavanje tih potencijalnih napada.

Imajte u vidu da su svi primeri i analize u ovom udžbeniku neformalni i intuitivni. Primenom ovog principa možemo da pokrijemo sve osnovne koncepte veoma brzo i sa minimalnom pozadinom znanja o protokolima.

Kod svake analize protokola treba imati na umu da su protokoli po prirodi vrlo suptilni. Ovo znači da i najmanja promena dizajna protokola može da utiče na pouzdanost samog protokola. Mnogi danas dobro poznati protokoli imaju ozbiljne nedostatke, uključujući *IPSec*, *GSM* i *WEP*. Problem ne nastaje samo kod dizajna protokola, naprotiv dizajn može da bude proveren i dobar, ali česti su problemi na strani implementacije samog protokola. Na primer, pronađene su ozbiljne greške u implementaciji *SSL* protokola u Internet pregledaču *IE*.

Idealni bezbednosni protokoli moraju da zadovoljavaju zahteve sa aspekta:

1. Bezbednosti;
2. Efikasnosti;
3. Otpornosti;
4. Ergonomičnosti;

Svi bezbednosni protokoli prvo moraju da zadovoljavaju bezbednosne zahteve. Pretpostavka je da su svi zahtevi vrlo precizno definisani. Sa druge strane, neophodno je voditi računa o efikasnosti protokola. Pogotovo kada je reč o upotrebi „skupih operacija“ koje se uglavnom vezuju za javne ključeve ili asimetričnu kriptografiju, što iziskuje potrebu za minimizacijom računarskih zahteva.

Minimizacijom računarskih zahteva pravimo kompromis sa minimizacijom kašnjenja i propusnog opsega nekog komunikacionog sistema koji upotrebljava dizajnirani protokol.

Idealni bezbednosni protokol mora da bude otporan na napadača, što znači da će raditi i kada napadač aktivno pokušava da ga prekine u radu. Drugi izazov je otpornost protokola. Protokol mora da ostane operativan čak i ako mu se promeni radno okruženje. Mnogi protokoli su dizajnirani tako da promenom radnog okruženja njegove osvedočene osobine mogu biti narušene. Većina protokola je dizajnirana u prošlosti za prijateljska Internet akademska okruženja, koja možda ne odgovaraju stvarnosti modernog Interneta i zahtevanim Internet servisa današnjice.

Ergonomičnost je i te kako važan aspekt kod dizajna idealnog protokola. Ergonomičnost garantuje jednostavnost korišćenja, jednostavnu implementaciju i fleksibilnost za različite platforme. Od jednostavnosti korišćenja zavisiće njegova široka upotreba i zastupljenost u mnogim komunikacionim sistemima. Jednostavna implementacija će smanjiti broj potencijalnih grešaka koje utiču na bezbednost protokola. Važno je napomenuti da je najveći broj uspešnih napada uspeo upravo zbog loše implementacije.

Nakon svih ovih zahteva koje smo naveli, možemo da zaključimo da je jako teško zadovoljiti sve ove zahteve, a ovom činjenicom smo daleko od sinteze idealnog bezbednosnog protokola, ali to ne znači da treba odustati od ideje o sintezi perfektnih bezbednosnih protokola.

2.1. JEDNOSTAVNI PROTOKOLI ZA AUTENTIFIKACIJU NA RAČUNARU

Prvi bezbednosni protokol o kom ćemo govoriti je protokol koji se koristi za kontrolu fizičkog pristupa u ustanovama od izuzetne važnosti za jednu državu. Pod tim ustanovama podrazumevamo vojne objekte - nuklearna postrojenja, vojne institute, policiju i industrijska postrojenja.

Za pristup ovakvim objektima zaposleni dobija identifikacionu karticu koju mora da ima kod sebe u svakom trenutku dok boravi u objektu i kada dolazi u objekat. Da bi zaposleni fizički pristupio objektu neophodno je da ubaci identifikacionu karticu u čitač kartica i nakon toga da unese *PIN* kod koji je samo njemu poznat. U nastavku ćemo opisati jedan ovakav protokol.

1. Zaposleni ubacuje karticu u čitač kartica.
2. Zaposleni unosi *PIN* kod preko tastature.
3. Sistem proverava ispravnost *PIN* koda, nakon čega odobrava ulaz ili zabranjuje. Pogrešan *PIN* može da alarmira službu obezbeđenja da preduzme neke mere predostrožnosti.

Skoro sličan protokol koristimo kada želimo da podignemo novac preko bankomata. Protokol je sa aspekta bezbednost identičan, jedino je završetak malo drugačiji.

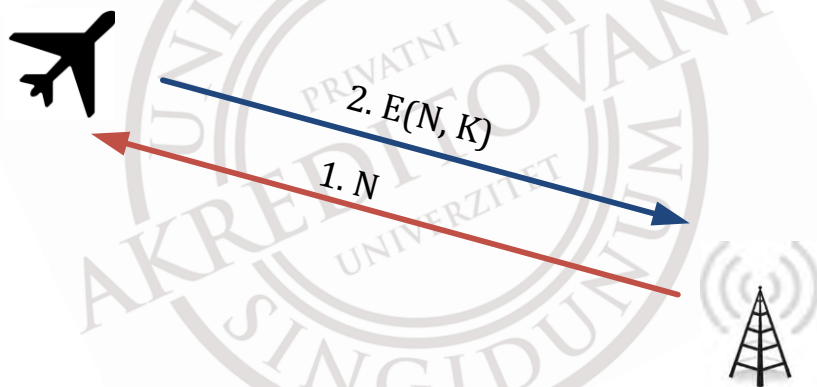
1. Korisnik ubacuje karticu u čitač kartica.
2. Korisnik unosi *PIN* kod.
3. Sistem u bankomatu proverava ispravnost *PIN* koda, u zavisnosti od ishoda transakcija se odobrava ili bankomat guta karticu.

Međutim, protokoli koji se razvijaju u vojne svrhe su daleko specijalizovaniji. Jedan primer takvog protokola je *IFF* (engl. *Identify Friend or Foe*) bezbednosni protokol. *IFF* protokol se koristi u avijaciji. Njegov osnovni cilj je da se spreči otvaranje vatre po prijateljskoj strani. Ovakve incidente u vreme rata je moguće vrlo lako izazvati, a to je situacija kada borbeni avion otvori vatru na prijateljski avion ili na prijateljsku vojsku.

Jednostavan primer *IIF* protokola prikazan je na (Slika 2.1). Ovaj protokol je prema nekim izvorima korišćen od strane južnoafričkog vazduhoplovstva ili poznatijeg kao *SAAF*, kada su se borili u Angoli sredinom 1970-ih.

IIF protokol koji je prikazan na (Slika 2.1) radi na sledeći način. Kada *SAAF* radar detektuje da se bazi približava neki nepoznat borbeni avion, radar generiše neki slučajan broj N i šalje ga borbenom avionu u vidu izazova na koji avion mora brzo dati odgovor. Svi *SAAF*-ovi avioni međusobno dele isti kriptološki ključ K koji se koristi za šifrovanje simetričnim algoritmima. Avion nakon prijema slučajne vrednosti N , Vrednost N šifrjuje sa ključem K i dobijeni šifrat kao odgovor na izazov šalje *SAAF* radaru. Neprijateljski avioni kod sebe nemaju originalni ključ K u cilju potvrđivanja pravog identiteta.

Na izgled ovaj protokol vrlo jednostavno daje mogućnost radaru da utvrdi da li se približava neprijateljski ili prijateljski avion.

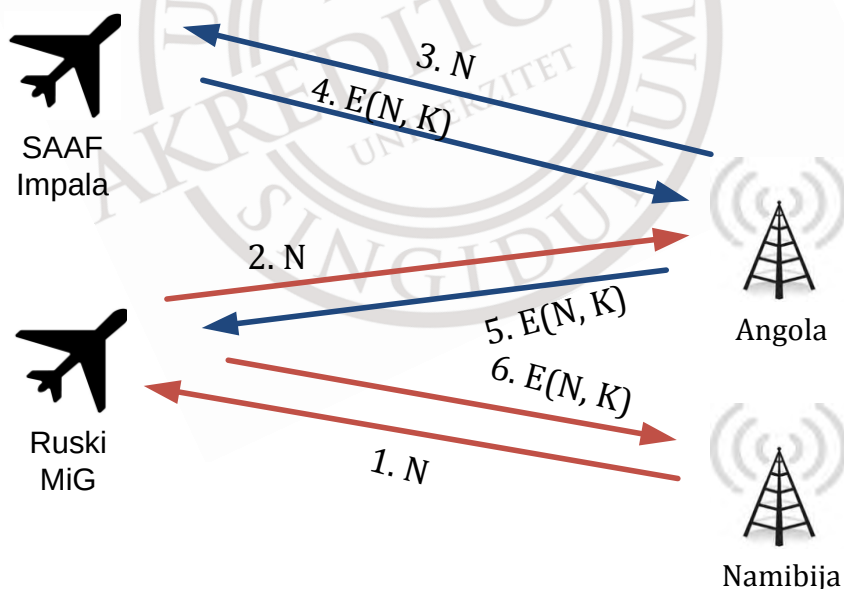


Slika 2.1 Radar sa *IIF* bezbednosnim protokolom

Da li je stvarno ovaj bezbednosni protokol besprekoran za identifikaciju prijateljskog ili neprijateljskog aviona saznaćemo u sledećem scenariju poznatim pod nazivom „Mig u sredini“. Na osnovu ovog scenarija napravićemo uvod u aktivne i pasivne napade na bezbednosni protokole. Konkretno scenario napada koji je prikazan na slici (Slika 2.2) je aktivan napad napadača u sredini.

Kao što je na slici prikazano, napad se realizuje preko šest koraka.

1. U prvoj fazi ruski *MiG* se približava neprijateljskoj teritoriji u Namibiji. Radar u Namibiji ga detektuje i generiše slučajnu vrednost N na osnovu koje pokušava da utvrdi njegov identitet.
2. U drugoj fazi ruski *MiG* dobija slučajnu vrednost N koju brzo šalje prijateljskom radaru u Angoli.
3. U trećoj fazi radar u Angoli detektuje neprijateljski avion od *SAAF* vojnih snaga i šalje mu izazov u vidu slučajne vrednosti koju je dostavio ruski *MiG*.
4. U četvrtoj fazi avion *SAAF*-a šifrira slučajnu vrednost N sa ključem koji je poznat samo radarima iz Namibije. Zatim šifrat šalje radaru u Angoli.
5. U petoj fazi radar iz Angole dostavlja šifrat ili odgovor na izazov ruskom *MiG*-u.
6. U poslednjoj šestoj fazi ruski *MiG* odgovara na izazov radaru iz Namibije, nakon čega ruski avion uspeva da lažira svoj identitet i uspešno izvede vazdušne napade u Namibiji.



Slika 2.2 Napad na IIF, „Čovek u sredini“

2.2. JEDNOSTAVNI PROTOKOLI ZA AUTENTIFIKACIJU NA MREŽI

Pretpostavimo da Alisa mora da dokaže pred Bobom da je ona Alisa, u slučaju gde Alisa i Bob komuniciraju preko mreže. Treba imati na umu da Alisa može biti čovek ili mašina, isto važi i za Boba. U narednim scenarijima Alisa i Bob će skoro uvek biti mašine u protokolima koje budemo razmatrali.

U većini slučajeva je dovoljno da Alisa dokaže svoj identitet u komunikaciji sa Bobom, bez potrebe da Bob dokazuje svoj identitet u komunikaciji sa Alisom. Ponekad u bezbednosnim protokolima uzajamna autentifikacija može biti zahtevana, a to znači da Alisa i Bob u tom protokolu moraju da se predstave jedno pred drugim. U tom scenariju isti protokol je moguće koristiti samo u drugom smeru. Da li je uvek uzajamnu autentifikaciju moguće rešiti uvođenjem drugog smera, videćemo da u bezbednosnim protokolima taj pristup nije uvek siguran.

Pored autentifikacije, sesijski ključ je neminovno potreban za bezbednu komunikaciju. Sesijski ključ je simetrični kriptološki ključ koji se u komunikaciji koristi za zaštitu poverljivosti ili integriteta postojeće sesije, ali sve pod uslovom da je autentifikacija između Alise i Boba uspela. Na početku ćemo ignorisati sesijske ključeve, tako da ćemo fokus prebaciti samo na autentifikaciju.

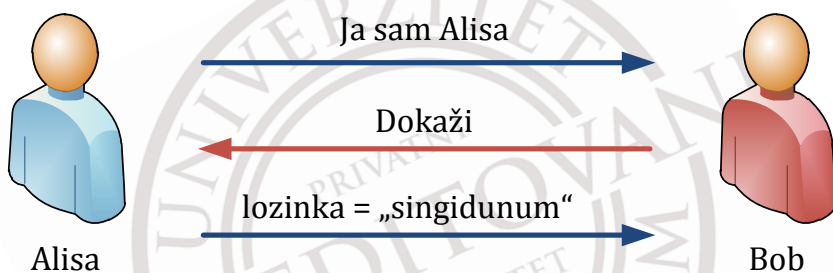
U određenim situacijama, mogu postojati drugi zahtevi prilikom dizajniranja bezbednosnog protokola, kao što su:

- Upotreba samo javnog ključa;
- Upotreba samo simetričnog ključa;
- Upotreba zajedno javnog i simetričnog ključa;
- Upotreba samo *heš* funkcije;
- Anonimnost, verodostojno odbijanje itd;

Autentifikacija na jednom zasebnom računaru je relativno jednostavna. Osnovno pitanje se odnosi na napade na softver za autentifikaciju. Dok je potvrda identiteta ili autentifikacija preko mreže daleko kompleksnija, predstavlja svoj sopstveni skup izazova. Napadač Trudi može pasivno da opservira poruke koje se razmenjuju između Alise i Boba. U slučaju da napadač pasivno opservira poruke, postoji mogućnost za ponovnu reprodukciju poruke.

Kod mrežnih protokola pored pasivnih, mogući su i aktivni napadi preko kojih napadač može da umetne novu poruku, da obriše celu poruku ili samo deo poruke ili da napravi neku promenu u sadržaju poruke.

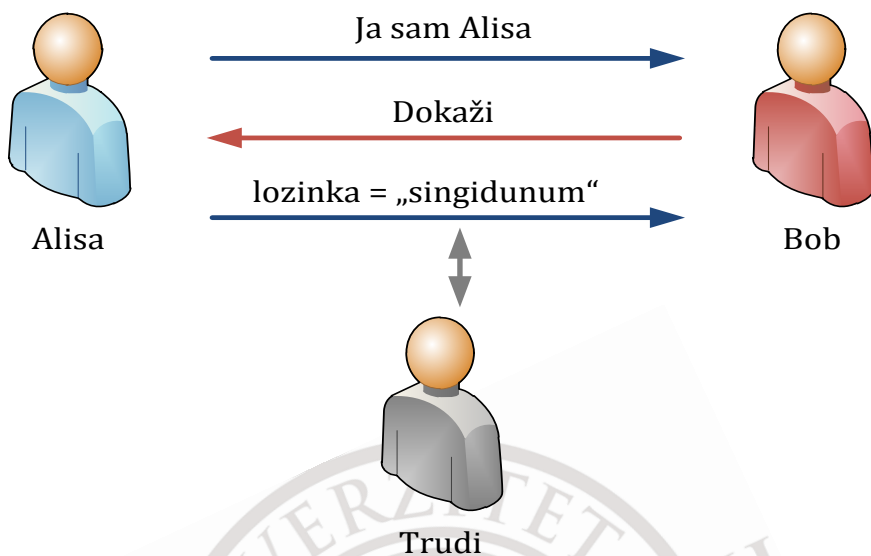
Naš prvi pokušaj autentifikacije na mreži je prikazan na (Slika 2.3). Protokol je jednostavan i može biti u redu za autentifikaciju na zasebnom računaru. Protokol zahteva tri poruke između Alise i Boba. Alisa ima ulogu klijentskog računara, dok Bob ima ulogu serverskog računara. U prvoj poruci Alisa se predstavlja pred Bobom „Ja sam Alisa“, u drugoj poruci Bob traži od Alise da dokaže da je ona zaista Alisa. Alisa zna svoju lozinku „Singidunum“ i šalje je Bobu. Kod Boba se nalazi baza podataka koja sadrži lozinke svih svojih korisnika. Bob pretražuje Alisin lozinku i nakon toga potvrđuje Alisin identitet.



Slika 2.3 Primer jednostavne autentifikacije

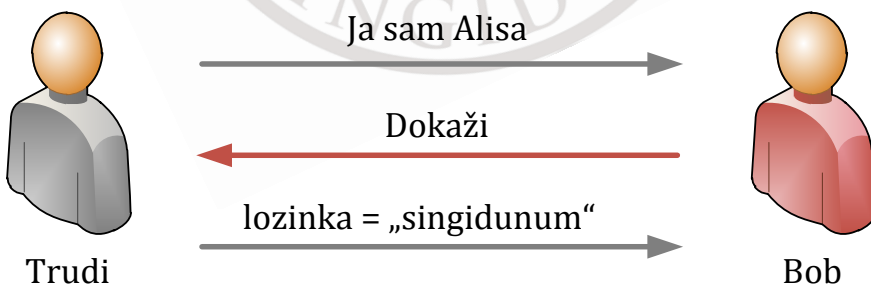
Sada postavljamo pitanje da li je ovaj protokol nebezbedan u mrežnom okruženju? Prvo, podlozan je napadu zasnovanom na ponovnom reprodukovanju poruka. Drugo, Bob mora da zna šta je Alisina lozinka.

Na (Slika 2.4) prikazan je napad na autentifikaciju. Prvi put kada je Alisa koristila ovaj protokol za autentifikaciju pred Bobom, Alisa je pasivno opservirala njihovu komunikaciju. Alisa i Bob ne znaju da postoji u njihovom komunikacionom kanalu ovakva aktivnost od strane Trudi. Trudi je uspela da iz komunikacionog kanala sazna šta je lozinka, a zatim da pokuša napad sa ponovnim reprodukovanjem poruka.



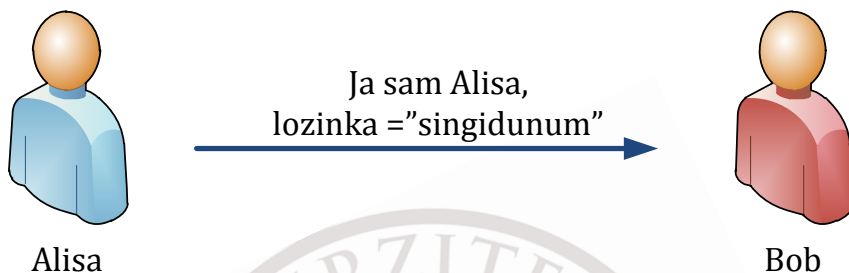
Slika 2.4 Napad na autentifikaciju – prva faza

Na (Slika 2.5) prikazan je napad na autentifikaciju sa ponovnim reprodukcijom poruka. U prvoj poruci, Trudi šalje poruku Bobu „Ja sam Alisa“, u drugoj poruci, Bob šalje poruku „dokaži“ da si ti zaista Alisa. U poslednjoj, trećoj poruci Trudi šalje lozinku „Singidunum“, nakon čega Bob proverava da li postoji lozinka u bazi podataka i odobrava Alisi pristup ne znajući da se sa druge strane protokola nalazi Trudi.



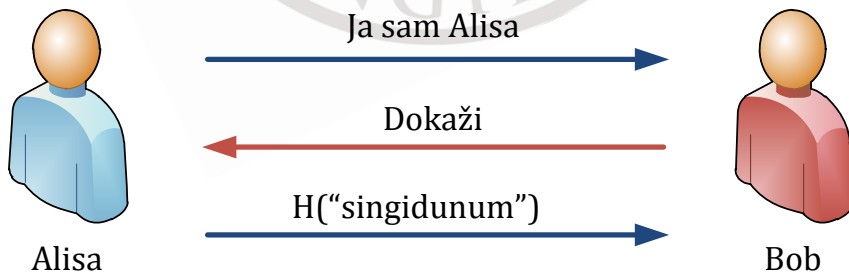
Slika 2.5 Napad na autentifikaciju – druga faza

Da li postoji način da se spreči ovaj tip napada na protokol za autentifikaciju? Možda postoji efikasniji način koji je prikazana na (Slika 2.6), ali definitivno ostaju isti problemi kao u prethodnom dizajnu protokola. Trudi ništa ne sprečava da na isti način ponovi napad. Tačnije, ovaj napad postaje efikasniji za Trudi od prethodnog napada.



Slika 2.6 Efikasniji protokol za autentifikaciju

Na slici (Slika 2.7) prikazan je poboljšani protokol za autentifikaciju koji možda na izgled deluje kao bolje rešenje od prethodne dve verzije. Komunikacija između Alise i Boba izgleda identično, osim u poslednjoj poruci kada Alisa šalje Bobu poruku tako što računa otisak poruke „heš od lozinku“ preko neke jednosmerne funkcije, kao što su *MD5*, *SHA1* i td. Na ovaj način Alisa krije lozinku od Boba i napadača. Da objasnimo, Bob sada u svojoj bazi podataka čuva samo Alisinu heš vrednost od lozinke, na osnovu koje na identičan način prihvata ili odbacuje Alisin identitet.



Slika 2.7 Poboljšani protokol za autentifikaciju

Međutim, i ova modifikacija protokola je još uvek podložna napadu zasnovanom na ponovnoj reprodukciji poruka. Trudi ništa ne sprečava da na identičan način falsifikuje Alisin identitet.

Česta je pojava da kod razvoja Internet servisa programeri budu vođeni pogrešnom logikom i da na ovaj način kako je prikazano na slici (Slika 2.7) pokušavaju da zaštite lozinke korisnika. Tačno je, da je lozinka nepoznata napadaču kao i administratoru servisa, međutim to ne sprečava napadača da ostvari legitiman pristup. Zapravo, modifikacija je samo podrazumevala transformaciju lozinke koja se nalazila u otvorenom tekstu.

Nastavljamo dalje i postavljamo pitanje da li je moguće nešto uraditi u vidu nove modifikacije protokola, a u cilju sprečavanja napada zasnovanom na ponovnom reprodukovanju poruka? Kao odgovor na ovaj problem, primenjuje se takozvani „izazov odgovor“ (engl. *Challenge-response*).

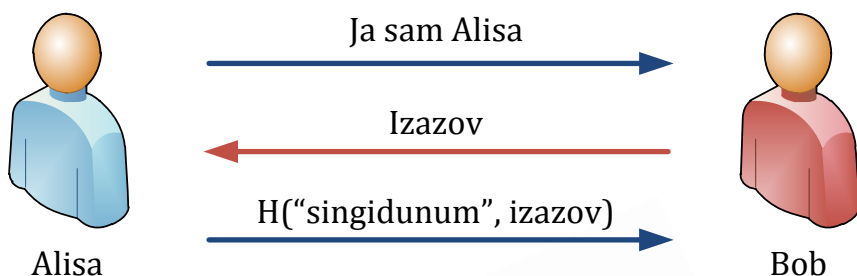
Da li je moguće uraditi ovakvu modifikaciju u sigurnosnom protokolu? Pretpostavimo da Bob želi da autentifikuje Alisu, u tom slučaju Bob šalje izazov Alisi na koji samo Alisa može da odgovori korektno. Izazov se tako bira da nije moguće ponovno reprodukovanje poruka.

Kako se ovo postiže? Lozinka je vrednost koju samo Alisa treba da zna. Radi svežine lozinke, koristi se jednokratno jedan broj koga ćemo nazvati izazov (engl. *nonce*). Izazov ili jednokratna vrednost je vrednost koju je generisao Bob, ova vrednost ne sme da se ponovi više u protokolu za autentifikaciju.

Na slici (Slika 2.8) je predstavljena nova modifikacija preko koje ćemo sprečiti tip napada ponovne reprodukcije poruka. Zapravo, u ovom protokolu izazov sada predstavlja izazov na koji Alisa treba da odgovori. *Heš* vrednost koju je Alisa generisala predstavlja odgovor na Bobov izazov. U ovom dizajnu protokola izazov je vrednost koja onemogućava ponovnu reprodukciju, obezbeđujući stalnu svežinu lozinke.

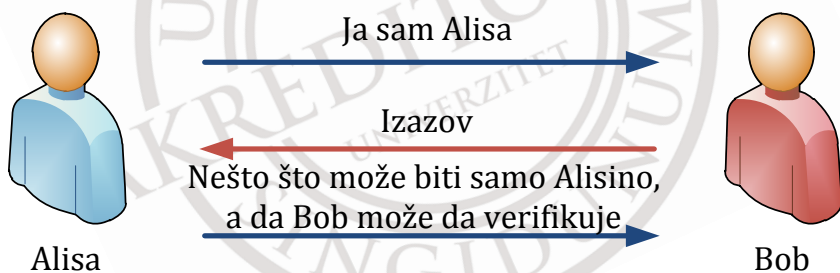
Šta je sada promenjeno novim dizajnom protokola? Primetićemo da Bob mora da zna šta je Alisina lozinka. Ovo nije dobro rešenje iz više razloga. Uvek postoji opasnost da lozinke budu kompromitovane na Bobovoj strani, pored protokola za autentifikaciju koji bi prestao da radi između Alise i Boba, postojala bi mogućnost

da Alisin identitet bude ugrožen i na drugim protokolima ukoliko je Alisa koristila istu lozinku.



Slika 2.8 Protokol za autentifikaciju, izazov - odgovor

Šta treba da uradimo da bismo ovo ostvarili? Računanje *heš* vrednosti od lozinke je jedno rešenje. Osnovna ideja kod autentifikacije jeste ideja da Alisa koristi nešto što može biti samo Alisino, a da Bob sa druge strane komunikacionog kanala može da verifikuje.



Slika 2.9 Autentifikacioni protokol, izazov – odgovor 2

Ovde ćemo istaći da algoritmi koji se koriste za računanje *heš* vrednosti (*MD5*), ne spadaju u grupu kriptografskih tehnika, iz tog razloga kažemo da je uvođenjem kriptografskih tehnika moguće doći do još boljih rešenja koja će u velikoj meri doprineti podizanju nivoa sigurnosti kod bezbednosnih protokola – kriptografskih bezbednosnih protokola.

2.3. AUTENTIFIKACIJA – INFORMACIONO TEORIJSKA ANALIZA

U ovom odeljku razmatraćemo teorijsku nekompatibilnost autentifikacije i tajnosti, kao i kako obezbediti autentifikaciju u praksi, u praktičnim šifarskim sistemima. Servis autentifikacije se zasniva na određenim procedurama. Primer takvih procedura su protokol za razmenu ključeva *DH* (engl. *Diffie-Hellman*) i *RSA* asimetrični šifarski algoritam.

Podsetićemo se šta je servis za autentifikaciju? Autentifikacija je servis bezbednosti kojim se osigurava da je poruka poslata od strane autorizovane osobe. Drugim rečima, pitamo se da li je primljeni šifrat C validan (poslat od strane autorizovane osobe) ili je podmetnut od strane neke neautorizovane osobe (a samim tim sa lošim namerama). Podmetnuti šifrat može biti modifikovani legalni šifrat C ili potpuno zamenjen nekim drugim šifratom.

Autentifikacija se dugo vremena smatrala nerazlučivom od tajnosti. Kriptolozi su relativno nedavno otkrili da su ova dva servisa bezbednosti međusobno nezavisna i da su čak međusobno nekompatibilna u čisto teorijskom smislu. Ovo znači da kriptografski sistemi koji obezbeđuju maksimalnu (apsolutnu) tajnost ne mogu obezbediti nikakvu autentičnost. Sa ovim problemom ćemo se susresti u narednim poglavljima koji se odnose na perfektno šifarske sisteme.

Krenućemo od Sajmonove teoreme. Verovatnoća P_i da je šifrat falsifikovan, odnosno prihvaćen iako je poslat od neautorizovane osobe, je ograničena sa:

$$P_i = 2^{-I(C;K)},$$

gde je C šifrat, a K ključ datog šifarskog sistema.

Neka je $\phi(C, K)$ autentifikaciona funkcija:

$$\phi(C, K) = \begin{cases} 1 & \text{ako } \exists M | C = e(M, K) \\ 0 & \text{u ostali slučajevima} \end{cases}.$$

Verovatnoća da se šifrat C prihvati kao autentičan je data sa:

$$P(\text{acc}(C)|C) = \sum_K \phi(C, K)P(K),$$

odnosno verovatnoća falsifikovanja autentičnosti je data sa:

$$\begin{aligned}
 P(\text{acc}(C)|C) &= \sum_C P(C, \text{acc}(C)) \\
 &= \sum_C P(C, \text{acc}(C)|C) = \sum_{C,K} \phi(C, K) P(C) P(K) \\
 &= \sum_{C,K, P(C,K) \neq 0} P(C) P(K) = \sum_{C,K} P(C, K) \frac{P(C) P(K)}{P(C, K)} = E \left[\frac{P(C) P(K)}{P(C, K)} \right]
 \end{aligned}$$

odnosno:

$$\log(P_i) = \log E \left[\frac{P(C) P(K)}{P(C, K)} \right],$$

korišćenjem Jensenove nejednakosti dobijamo:

$$\log E \left[\frac{P(C) P(K)}{P(C, K)} \right] \geq E \left[\log \frac{P(C) P(K)}{P(C, K)} \right] = -I(C; K),$$

odnosno:

$$P_i \geq 2^{-I(C; K)},$$

sa jednakošću, ako i samo ako je $\frac{P(C) P(K)}{P(C, K)}$ konstantno za sve $(C; K)$ (tako da je $P(C, K) > 0$), tj. C i K su nezavisni.

Da bi smo garantovali autentifikaciju, verovatnoća P_i mora biti mala, a to znači da uzajamna informacija između šifrata i ključa mora biti velika. S druge strane znamo da bismo obezbedili apsolutnu tajnost mora važiti $I(C; M) = 0$, što je oprečno zahtevu autentifikacije.

Sa stanovišta informaciono teorijskog pristupa, autentifikacija i tajnost su oprečni zahtevi. Zaista,

$$I(C; K) = I(C; M) + H(K) - H(M) - H(K|M, C),$$

ako stavimo:

$$I(C; M) = 0, i H(K|M, C) = 0,$$

sledi da je:

$$I(C; K) = H(K) - H(M),$$

što implicira:

$$P_I \geq 2^{(H(M) - H(K))} > 0.$$

Odavde sledi da bi apsolutno tajni kriptografski sistem morao da ima ekstremno kompleksne ključeve $H(K) \gg H(M)$ da bi se istovremeno obezbedila pouzdana autentifikacija.

Jedno moguće rešenje je da važi $I(C; K) \gg 0$, da bi se ostvarila autentifikacija, a da se tajnost obezbedi algoritamski. Ovo je jedan od razloga zašto su kriptografski sistemi zasnovani na algoritamskoj kompleksnosti danas u širokoj upotrebi.

Osnovna ideja je da se koristi digitalni potpis poruke. Ovim se obezbeđuje da je pošiljalac poruke zaista i osoba koja tvrdi da je to ona, a da u slučaju neslaganja, pošiljalac koji je digitalno potpisao poruku ne može da porekne da je on zaista poslao tu poruku.

3. OSNOVE KRIPTOGRAFSKIH PROTOKOLA

U ovom delu udžbenika prelazimo sa protokola koji se zasnivaju na lozinkama na nove kriptografske protokole. Pokušaćemo da objasnimo dizajn protokola za bezbednu autentifikaciju upotrebom nekih kriptografskih tehnika. Prvi izazov su kriptografski protokoli koji koriste simetrične algoritme za šifrovanje ili se zasnivaju na simetričnim kriptološkim ključevima.

Definisaćemo prvo oznake koje ćemo koristiti za označavanje određenih faza u protokolu koji implementira simetrične algoritme.

Šifrovanje otvorenog teksta P sa ključem K :

$$C = E(P, K);$$

Dešifrovanje šifrata C sa ključem K :

$$M = D(C, K);$$

Označavanje određenih faza u protokolu koji implementira asimetrične algoritme.

Šifrovanje poruke M sa Alisinim javnim ključem:

$$\{M\}_{Alisa};$$

Potpisivanje poruke M sa Alisinim privatnim ključem:

$$[M]_{Alisa};$$

Uvek je važno da zapamtimo da u kriptografiji sa javnim ključevima, bilo ko može koristiti javne ključeve za kriptografske operacije, dok samo Alisa može koristiti svoj privatni ključ.

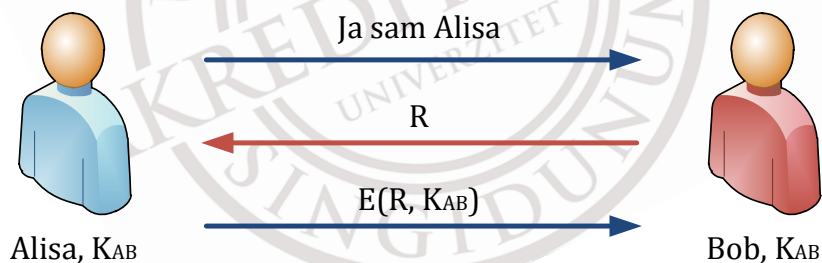
Sada se naše interesovanje izmešta ili usmerava na potencijalne napade na protokole, a ne direktno na kriptografske algoritme. Pretpostavićemo da je kriptografija sigurna i da ne trebamo razmatrati o kriptografskoj snazi algoritama koje koristimo za dizajniranje autentifikacionih protokola.

3.1. AUTENTIFIKACIJA SA SIMETRIČNIM KLJUČEVIMA

Autentifikacija zasnovana na kriptografskim tehnikama koristi simetrične ili asimetrične algoritme. Krenućemo sa razmatranjem protokola koji koriste simetrične algoritme, ali pre nego što počnemo podsetićemo se da simetrična kriptografija podrazumeva prethodno razmenjen isti kriptološki ključ između dve legitimne strane koje treba da započnu komunikaciju.

U ovom novom scenariju Alisa i Bob treba da dele zajednički simetrični ključ koji ćemo označiti K_{AB} . Pretpostavka je da ključ K_{AB} mora da bude poznat samo Alisi i Bobu. Upravo, na osnovu ovog ključa se autentifikacija obavlja dokazom o poznavanju deljenog simetričnog ključa.

Kako se ovaj scenario dizajnira? Ključ se ne sme otkriti i ne sme se omogućiti napad ponovnim reprodukovanjem poruka. Na slici (Slika 3.1) prikazan je jedan bezbedan metod preko koga Bob autentifikuje Alisu, dok Alisa nema mogućnost da autentifikuje Boba.



Slika 3.1 Jednosmerna autentifikacija simetričnim ključem

Objasnićemo kako radi ovaj protokol na osnovu zajedničkog ključa K_{AB} .

1. Alisa se predstavlja Bobu „Ja sam Alisa“.
2. Bob generiše slučajnu vrednost – izazov, zatim šalje Alisi.
3. Alisa šifruje sa simetričnim algoritmom slučajnu vrednost R , dobijeni šifrat šalje Bobu.

4. Bob dešifruje šifrat koji mu je Alisa poslala i verifikuje Alisu na osnovu izazova R koji je poslao u drugom koraku.

Ovaj metod je pouzdan jer je jasno da niko drugi osim Alise nije mogao da generiše korektan šifrat na osnovu koga je Bob verifikovao Alisu. Očigledan nedostatak kod ovog protokola je uzajamna autentifikacija. Pod uzajamnom autentifikacijom podrazumevamo predstavljanje u oba smera Alisa $\rightarrow$ Bob, Bob $\rightarrow$ Alisa.

U sledećem dizajnu protokola na slici (Slika 3.2) razmotrićemo mogućnost uzajamne autentifikacije uvođenjem drugog smera autentifikacije, oba smera zasnovana na simetričnim ključevima.



Slika 3.2 Uzajamna autentifikacija sa simetričnim ključem, 1

Objasnićemo kako radi ovaj protokol za uzajamnu autentifikaciju na osnovu zajedničkog ključa K_{AB} .

1. Alisa se predstavlja Bobu „Ja sam Alisa“ i generiše slučajnu vrednost R – izazov, zatim šalje Bobu.
2. Bob šifruje sa simetričnim algoritmom slučajnu vrednost R, ključem K_{AB} i dobijeni šifrat šalje Alisi.
3. Alisa preko primljenog šifrata verifikuje Boba i **ponavlja identičan korak kao i Bob**. Alisa šifruje istu vrednost R ključem K_{AB} , zatim generisani šifrat šalje Bobu na osnovu koga Bob verifikuje Alisu.

Bob dešifruje šifrat koji mu je Alisa poslala i verifikuje Alisu na osnovu izazova R koji je poslao u drugom koraku. Ovde nastaje veliki problem, drugi korak je identičan trećem koraku, ovakva situacija omogućava da se Trudi predstavi kao Alisa ili bilo ko drugi.

Predložićemo modifikaciju ovog protokola, tako ćemo sprečiti mogućnost da se bilo ko predstavi kao Alisa.

U sledećem dizajnu protokola na slici (Slika 3.3) razmotrićemo mogućnost poboljšanja protokola za uzajamnu autentifikaciju uvođenjem posebnih vrednosti R . U ovom slučaju Alisa će generisati R_A preko koga će autentifikovati Boba, a Bob će generisati R_B preko koga će autentifikovati Alisu.



Slika 3.3 Uzajamna autentifikacija sa simetričnim ključem, 2

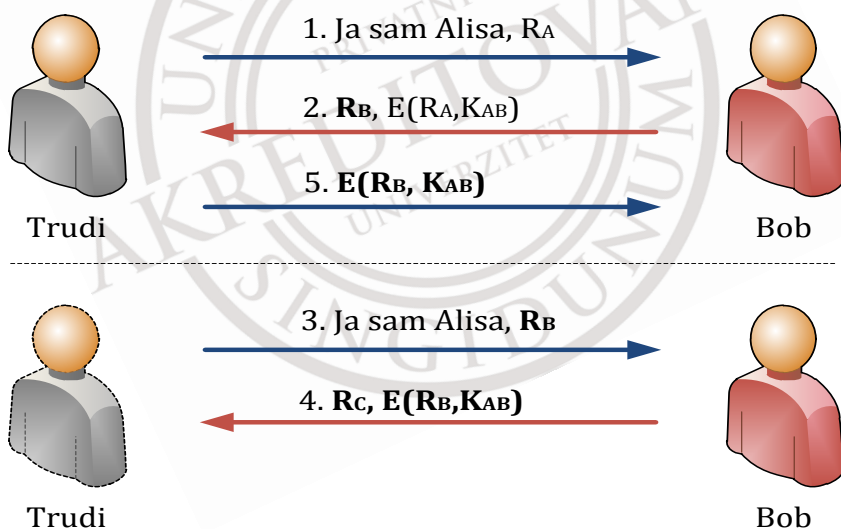
Objasnićemo kako radi ovaj protokol za predloženu modifikaciju na osnovu zajedničkog ključa K_{AB} .

1. Alisa se predstavlja Bobu „Ja sam Alisa“ i generiše slučajnu vrednost R_A – izazov, zatim šalje Bobu.
2. Bob šifrjuje sa simetričnim algoritmom slučajnu vrednost R_A ključem K_{AB} , generiše R_B za Alisu, zatim dobijeni šifrat i vrednost R_B šalje Alisi.
3. Alisa preko primljenog šifrata verifikuje Bobov identitet. Alisa šifrjuje vrednost R_B ključem K_{AB} , zatim generisani šifrat šalje Bobu na osnovu koga Bob verifikuje Alisin identitet.

Preko ovog dizajna protokola sa slike (Slika 3.3) omogućili smo uzajamnu autentifikaciju između Alise i Boba na osnovu postojanja jednosmernog autentifikacionog protokola. Da li je ovaj protokol bezbedan za uzajamnu autentifikaciju? Videćemo to na slici (Slika 3.4).

Objasnićemo kako je Trudi uspela da nadmudri Boba i lažno se predstavi pod Alisanim identitetom. I dalje svi parametri ostaju u funkciji, kao što su ključ K_{AB} , K_A i K_B .

1. Trudi se predstavlja Bobu „Ja sam Alisa“ i generiše slučajnu vrednost R_A – izazov, zatim šalje Bobu.
2. Bob šifrjuje sa simetričnim algoritmom slučajnu vrednost R_A ključem K_{AB} , generiše R_B za lažnu Alisu-Trudi, zatim dobijeni šifrat i vrednost R_B šalje ka Trudi.
3. Trudi paralelno započinje još jednu autentifikaciju sa Bobom (donji deo slike), predstavlja se Bobu „Ja sam Alisa“ i prosleđuje Bobu Bobovu R_B vrednost umesto R_A .
4. Bob prelazi u drugu fazu paralelnog protokola, šifrjuje sa simetričnim algoritmom slučajnu vrednost R_B ključem K_{AB} , generiše neko R_C (koje nije bitno u ovom scenariju) za Trudi, zatim dobijeni šifrat i vrednost R_C šalje ka Trudi.
5. Trudi preko primljenog šifrata verifikuje Bobov identitet (što nije bitno u ovom scenariju). Trudi šalje šifrat Bobu koji je Bob generisao sa ključem K_{AB} u paralelnom protokolu. Na kraju Bob potvrđuje Alisin identitet.

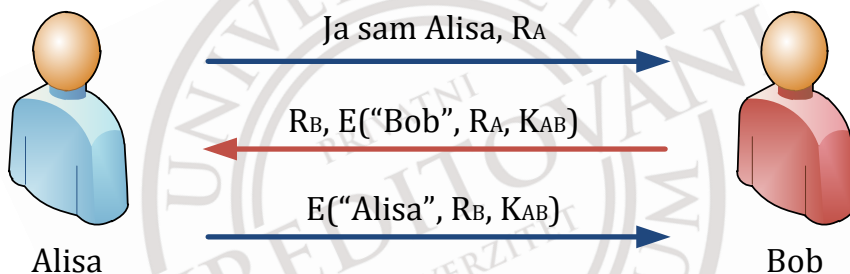


Slika 3.4 Napad na uzajamnu autentifikaciju sa simetričnim ključem

Izgleda da naš protokol za uzajamnu autentifikaciju nije bezbedan. Trudi je jednostavno uspeła da se predstavi kao Alisa, a da Bob ne zna za to. Ovaj protokol još jednom potvrđuje činjenicu da su protokoli veoma suptilni!

Prvi zaključak je da protokol za uzajamnu autentifikaciju ne može biti bezbedan za uzajamnu autentifikaciju. Drugi zaključak je da protokoli (napadi na protokole) mogu biti suptilni. Još jedan zaključak je očigledan iz ovih primera, da izmene ili modifikacije mogu da dovedu do neočekivanih bezbednosnih problema.

U nastavku imamo zadatak da pokušamo da otklonimo propust iz prethodnog primera. Na slici (Slika 3.5) predstavljeno je rešenje sa malom modifikacijom protokola. Uveden je dodatni parametar sa obe strane, a to je identitet Alise i identitet Boba. Pored slučajne vrednosti R_A ili R_B u zavisnosti od strane, šifruje se i Alisin i Bobov parametar koji određuje identitet sa zajedničkim ključem K_{AB} . Da li ove nevažne promene u protokolu pomažu? Odgovor je DA! Na ovaj način onemogućili smo Trudi da koristi odgovor od Boba za treći korak u protokolu. Ukoliko pokuša Bob će odmah otkriti da je u pitanju napad.



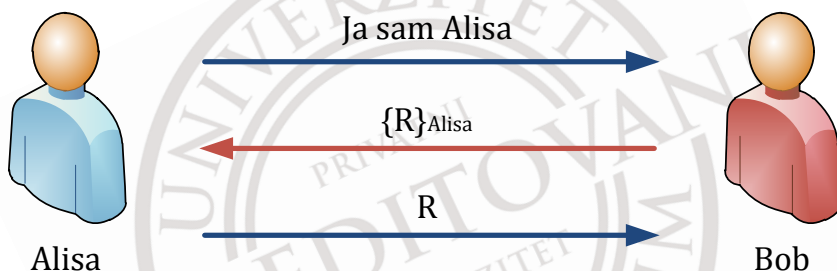
Slika 3.5 Uzajamna autentifikacija, modifikovani protokol

Prva lekcija koju treba da zapamtimo iz ovoga odeljka je da dve strane koje komuniciraju (Alisa i Bob) ne smeju uraditi identične stvari, jer to može otvoriti vrata za napadača. Druga lekcija je da male modifikacije mogu da dovedu do velikih promena sa aspekta bezbednosti, kako na bolje tako na lošije. Očigledne stvari ne moraju biti bezbedne. Takođe, ukoliko se pretpostavke ili okolnosti promene, protokoli mogu i da ne rade. Ovo predstavlja zajednički izvor bezbednosnih propusta, dobar primer su Internet protokoli.

3.2. AUTENTIFIKACIJA SA JAVNIM KLJUČEVIMA

U prethodnom odeljku smo uspeli da dizajniramo protokol za uzajamnu autentifikaciju zasnovanu na simetričnim ključevima. Da li možemo dizajnirati identičan protokol sa korišćenjem javnih ključeva?

Oznake koje su potrebne za razumevanje slika, nalazi se na početku poglavlja. Polazimo sa prvim primerom koji koristi kriptografiju sa javnim ključem. Protokol na slici (Slika 3.6) omogućava Bobu da autentifikuje Alisu, jer samo ona može da uradi operaciju sa svojim privatnim ključem i da prosledi korektan odgovor vrednost (dešifrovano R) u trećem koraku.



Slika 3.6 Autentifikacija sa javnim ključem - šifrovanje

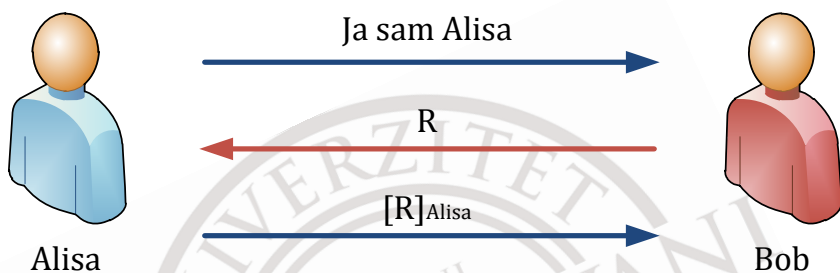
Objasnićemo kako radi protokol sa slike (Slika 3.6) za jednosmernu autentifikaciju na osnovu javnog ključa - šifrovanje.

1. Alisa se predstavlja Bobu „Ja sam Alisa“.
2. Bob šifrjuje sa Alisinim javnim ključem vrednost R (izazov) i dobijeni šifrat šalje Alisi.
3. Alisa u ovoj fazi koristi svoj privatni ključ za dešifrovanje poruke koju je dobila od Boba u drugom koraku. Nakon dešifrovanja Alisa dobija poruku R koju šalje u trećem koraku Bobu na osnovu koga Bob verifikuje Alisu.

Jasno je da u ovom protokolu samo Alisa sa svojim privatnim ključem može da dešifruje poruku koju je Bob poslao kao izazov, jer je Bob za generisanje šifrata koristio Alisin javni ključ.

Koliko je ovaj dizajn protokola siguran? Nije siguran, jer Trudi može da natera Alisu da dešifruje bilo šta! Recimo neku ranije poslatu šifrovanu poruku $\{M\}_{Alisa}$, umesto $\{R\}_{Alisa}$. Ovaj problem je moguće rešiti upotrebom dva različita para ključeva. Jedan par će biti upotrebljen za šifrovanje, a drugi za digitalno potpisivanje.

Prelazimo na drugi primer protokola u kome koristimo digitalni potpis. U ovom protokolu Bob će pokušati da verifikuje Alisu na osnovu njenog potpisa. Na sledećoj slici (Slika 3.7) prikazan je protokol.



Slika 3.7 Autentifikacija sa javnim ključem - dešifrovanje

Objasnićemo kako radi protokol sa slike (Slika 3.7) za jednosmernu autentifikaciju na osnovu javnog ključa – digitalno potpisivanje.

1. Alisa se predstavlja Bobu „Ja sam Alisa“.
2. Bob generiše slučajnu vrednost R (izazov) i šalje je Alisi.
3. Alisa u ovoj fazi koristi svoj privatni ključ za potpisivanje poruke (vrednost R - izazov) koju je dobila od Boba, zatim šalje potpisanu poruku R Bobu, na osnovu koga Bob verifikuje Alisu.

Koliko je ovaj dizajn protokola siguran? Problem je sličan kao i u prethodnom protokolu, Trudi ponovo može da natera Alisu da potpiše bilo šta! Očigledan je nedostatak kod oba protokola, moraju se imati dva različita para ključeva, kao što smo već rekli jedan za šifrovanje, a drugi za potpis.

Podsetićemo se nekih elementarnih stvari iz kriptografije sa javnim ključem kod operacija za šifrovanje i potpisivanje. Pretpostavimo da Alisa i Bob komuniciraju preko nekog komunikacionog kanala. Na svakoj strani se nalaze po dva para klju-

čeva. Jedan par se koristi za šifrovanje, a drugi za potpisivanje. Ukoliko Alisa želi da pošalje Bobu šifrovanu poruku, Alisa će saznati Bobov javni ključ i njega upotrebiti za šifrovanje poruke koja je namenjena Bobu. Ovu šifrovanu poruku može samo Bob dešifrovati sa svojim privatnim ključem.

U drugom slučaju, Alisa želi da potpiše poruku koju je namenila Bobu, Alisa koristi svoj privatni ključ za šifrovanje i tako šifrovanu poruku šalje Bobu. Bob na drugoj strani verifikuje Alisin potpis tako što dešifruje poruku sa Alisinim javnim ključem. Vidimo iz ovog primera da u slučaju šifrovanja i potpisivanja javni i privatni ključ menjaju svoje uloge. Ostaje još jedna napomena, a to je osnovno pravilo da se isti par ključeva ne sme koristiti za šifrovanje i za potpisivanje.

3.2.1. SESIJSKI KLJUČ

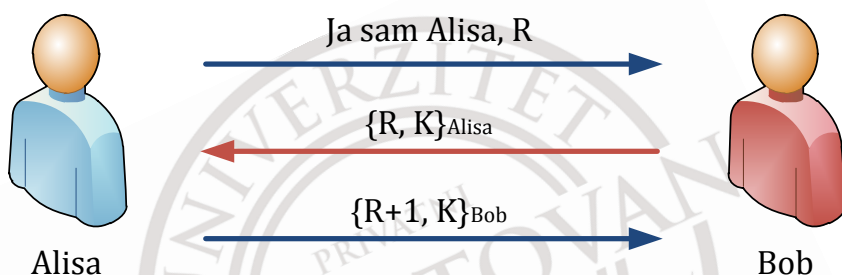
U većini kriptografskih protokola uz autentifikaciju zahtevan je sesijski ključ. Sesijski ključ je simetrični ključ koji je vezan za jednu sesiju. Ideja je da se u svakoj iteraciji (sesiji) razgovora koristi različit sesijski ključ za šifrovanje razmenjenih podataka u okviru jedne sesije.

Svrha sesijskog ključa je da se ograniči količina šifrovanih podataka sa jednim ključem, a sa druge strane da se smanji šteta ukoliko se kompromituje jedan sesijski ključ. Ovo je dobro prvenstveno sa aspekta kriptanalize. Pretpostavimo da je Trudi kriptanalitičar koji neko duže vreme opservira saobraćaj između Alise i Boba. Kada je skupila veću količinu podataka može da započne određene informacione analize na osnovu kojih može da dođe do poruke ili ključa. Međutim, upotreba sesijskih ključeva stvorila je ogromnu količinu nepovezanih podataka, podataka između kojih je uzajamna informacija jednaka nuli. Ova činjenica će pokušaje Trudi da uradi nešto, u startu osuditi na neuspeh.

Implementacijom sesijskih ključeva u protokole obezbedićemo poverljivost ili zaštitu integriteta razmenjenih poruka. Na ovaj način istovremeno obavljamo autentifikaciju i razmenjujemo zajednički simetrični ključ (sesijski ključ). Razmenjeni ključ možemo koristiti za servis tajnosti ili servis za proveru integriteta. Stoga, kada se analiziraju ovakvi protokoli za autentifikaciju, neophodno je posebno razmotriti potencijalne napade na autentifikaciju, a posebno na sesijske ključeve.

U nekim slučajevima koji se odnose na implementaciju sesijskih ključeva, zahteva se i „perfektna tajnost unapred“ (engl. *Perfect Forward Secrecy* - PFS). PFS predstavlja poseban dizajn protokola koji implementira DH (engl. *Diffie-Hellman*) protokol koji se koristi za razmenu simetričnih ključeva, ali diskusija na ovu temu sledi nešto kasnije.

Naš sledeći cilj u primerima koji slede jeste da dizajniramo protokol za proveru verodostojnosti koji takođe pruža mogućnost za uspostavljanje zajedničkog simetričnog ključa. Pokušaćemo prvo kroz jedan jednostavan primer protokola za autentifikaciju prikazan na slici (Slika 3.8), dodati fizički ključ sesije K.



Slika 3.8 Protokol za autentifikaciju i uspostavu sesijskog ključa – šifrovanje javnim ključevima

Objasnićemo kako radi protokol sa slike (Slika 3.8) za autentifikaciju i razmenu sesijskog ključa.

1. Alisa se predstavlja Bobu „Ja sam Alisa“, generiše slučajnu vrednost R.
2. Bob šifruje sa Alisinim javnim ključem vrednost R (izazov) i izabrani sesijski ključ K, zatim dobijeni šifrat šalje Alisi.
3. Alisa u ovoj fazi koristi svoj privatni ključ za dešifrovanje poruke koju je dobila od Boba u drugom koraku. Nakon dešifrovanja Alisa dobija vrednost R i ključ K. Računa inkrement vrednost R i sve to šifruje sa Bobovim javnim ključem, na osnovu čega Bob na kraju protokola verifikuje Alisu.

Koliko je ovaj dizajn protokola siguran? Pouzdan je kada su u pitanju ključevi, ali nema uzajamne autentifikacije. U ovom protokolu je Bob uspeo da autentifikuje

Alisu na osnovu ključa K , u poslednjoj fazi protokola. Primetimo da K igra ulogu Bobovog izazova. Međutim, Alisa nije uspela da autentifikuje Boba.

Da li možemo nešto da učinimo da poboljšamo protokol sa slike (Slika 3.8)? Možemo koristiti digitalno potpisivanje, umesto šifrovanja sa javnim ključem. Ova modifikacija je jednostavna, a novi modifikovani dizajn protokola prikazan je na slici (Slika 3.9).



Slika 3.9 Protokol za autentifikaciju i uspostavu sesijskog ključa – digitalno potpisivanje

Protokol sa slike (Slika 3.9) je sličan dizajnu protokola sa slike (Slika 3.8). Razlika između njih je jedino u operaciji sa javnim ključevima. Ovaj protokol koristi operaciju digitalnog potpisivanja umesto šifrovanja. Da li je sada problem rešen? Postigli smo uzajamnu autentifikaciju između Alise i Boba, ali ovaj protokol ima jedan fatalan problem. Ključ sesije K nije tajan. Svako ko opservira komunikaciju između njih može da dođe do ključa K preko javnog ključa Alise ili Boba.

Razmotrimo još jednom sve pre nego što odbacimo i ovaj protokol. Protokol sa slike (Slika 3.8) pruža uzajamnu autentifikaciju, a protokol sa slike (Slika 3.9) tajnost sesijskog ključa K . Sve ovo je stvorilo ideju o kombinovanju ova dva protokola. Upravo se tu i nalazi rešenje pojedinačnih problema oba protokola. Na ovaj način ćemo obezbediti bezbednu autentifikaciju i tajnost sesijskog ključa K . Postoji nekoliko načina da ovo uradimo.



Slika 3.10 Protokol za uzajamnu autentifikaciju i uspostavu sesijskog ključa –potpisivanje i šifrovanje javnim ključem

Prvi primer je prikazan na slici (Slika 3.10). U primeru obe strane prvo potpisuju vrednost R i ključ K sa privatnim ključem, a zatim šifruju sa javnim ključem druge strane. Da li je sada protokol koji obezbeđuje bezbednu autentifikaciju i razmenu zajedničkog sesijskog ključa siguran? Izgleda da je sada u redu, obezbeđena je autentifikacija i sigurna razmena sesijskog ključa.

Drugo pitanje je, da li ovaj protokol radi i u obrnutom slučaju? Na slici (Slika 3.11) prikazan je identičan protokol u kome je redosled operacija sa javnim ključem obrnut. Alisa i Bob u ovom dizajnu protokola prvo šifruju vrednost R i ključ K sa javnim ključem druge strane, a zatim potpisuju generisani šifrat svojim privatnim ključem.



Slika 3.11 Protokol za uzajamnu autentifikaciju i uspostavu sesijskog ključa – šifrovanje javnim ključem i potpisivanje

Ovaj dizajn protokola je takođe siguran, iako svako može da vidi $\{R, K\}_{\text{Alisa}}$ i $\{R+1, K\}_{\text{Bob}}$. Ovo se postiže skidanjem potpisa, operacija koju može bilo ko da ura-

di sa javnim ključem, ali tu se potencijalni napad zaustavlja obzirom da je ostao šifrat koji je nastao preko kriptografskog algoritma za koga važi pretpostavka da je bezbedan. Na kraju ovog odeljka možemo da izvedemo zaključak da su oba pristupa podjednako dobra, svakako pristup na slici (Slika 3.10) pored ključa K , zadržava i potpis u tajnosti.

3.2.2. PERFEKTNA TAJNOST UNAPRED

Sada kada smo konačno došli do pouzdanog dizajna protokola koji objedinjuje autentifikaciju i razmenu sesijskih ključeva, a sve to zasnovano na kriptografiji javnih ključeva, u cilju novog poboljšanja protokola usmerićemo se na razmatranje *PFS* (engl. *Perfect Forward Secrecy*) metoda. *PFS* predstavlja metod koji garantuje perfektnu tajnost unapred. Pre nego što dodemo do samih detalja, reci ćemo šta to nije *PFS* i kakva bojazan postoji kod trenutnog protokola o kome je reč.

Pretpostavimo da Alisa šifrue poruku sa zajedničkim simetričnim ključem K_{AB} i tako generisani šifrat šalje Bobu. Trudi konstantno neko vreme snima komunikaciju između Alise i Boba, tačnije snima šifrate koje oni razmenjuju, a kasnije napada Alisin ili Bobov računar u cilju pronalaženja K_{AB} . Ukoliko bi trudi uspela da pronađe K_{AB} , uspela bi da dešifruje sve snimljene šifrate.

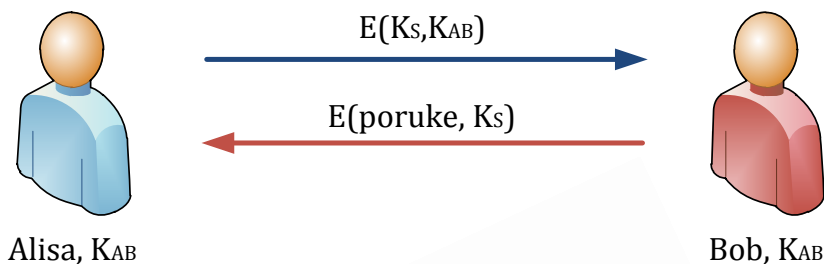
Scenario ovog napada je potpuno moguć u nekim radnim okruženjima. Trudi za tako nešto može upotrebiti maliciozni softver ili potpuno fizički pristupiti računaru i uzeti računar ili podatke sa računara.

Potrebno je preduzeti neke meri i pronaći metod kojim bi se i ovakva mogućnost napada mogla otkloniti. Perfektna tajnost unazad - *PFS* predstavlja metod koji sprečava Trudi da kasnije dešifruje snimljene šifrate, čak i pod uslovom da Trudi dođe do ključa K_{AB} ili nekih drugih načina.

Da li je *PFS* metoda moguća? Ako bi bila moguća to znači da moraju biti zadovoljeni sledeći uslovi:

1. Alisa i Bob ne mogu više da koriste K_{AB} za šifrovanje podataka;
2. Moraju od sada da koriste poseban ključ sesije K_s koji se zaboravlja nakon jednokratne upotrebe;

Upravo, na drugom uslovu nastaje problem. Kako Alisa i Bob ustanovljavaju ključ sesije K_S i ostvaruju pogodnosti koje nudi *PFS*? Na sledećoj slici (Slika 3.12) prikazaćemo jedan naivni protokol za ustanovljavanje ključa sesije.



Slika 3.12 Naivna *PFS* metoda

Šta je problem kod ovog protokola? Pretpostavimo da su Alisa i Bob završili sa prvom fazom protokola (autentifikacija i razmena ključa K_{AB}) i da sada žele da ustanove ključ sesije K_S .

U prvom koraku druge faze pre slanja privatnih poruka, Alisa šifruje generisani ključ sesije K_S sa ključem K_{AB} . U drugom protokolu Bob šifruje neku privatnu poruku sa ključem sesije K_S i tako generisani šifrat šalje Alisi. Alisa je uspešno dešifrovala i pročitala poruku.

U redu, ovaj protokol sada liči na protokol koji implementira *PFS*, a to znači da se koristi jednokratan sesijski ključ K_S . Međutim, trudi bi mogla da snimi šifrat $E(K_S, K_{AB})$ i da nakon nekog vremena dođe do ključa K_S pod uslovom da je uspeła da dođe do K_{AB} . Zaključak je da ovaj protokol ima neke osobine *PFS*-a, ali i dalje se bitno ne razlikuje od prethodnog protokola.

Odgovor na pitanje šta je *PFS* metoda i koje su prednosti ovog metoda, sam se nameće na osnovu mesta problema kod ovog naivnog *PFS* metoda sa slike (Slika 3.12). Cilj je upravo zaštititi Alisin i Bobov računar, tako da Trudi u budućnosti sa svim snimljenim šifratima ne može da zna šta su bili sesijski ključevi, čak i ako poseduje Alisin i Bobov računar. Takođe, ovo znači da su šifрати razmenjivani između Alise i Boba bili trenutno dešifrabilni, a da u budućnosti ni Alisa, ni Bob ne mogu više dešifrovati šifrate koji se nalaze kod Trudi.

I dalje nam ostaje da odgovorimo na pitanje kako se perfektно može implementirati PFS metoda, a da pri tome naše konstatacije i tvrdnje iz prethodnog pasusa važe.

Difi-Helman protokol predložili su Vitfild Difi (*Whitfield Diffie*) i Martin Helman (*Martin Hellman*)¹. Difi i Helman su tražili matematičke funkcije za koje redosled šifrovanja i dešifrovanja nije bitan, na primer:

$$f(g(x)) = g(f(x))$$

Ovakve funkcije postoje, većina ih je dvosmerna, odnosno mogu se lako izračunati ali je lako naći i njihovu inverznu vrednost. Primer dvosmernih funkcija:

$$f(x) = 2x; f(x) = x^2$$

Skraćenicu *DH* uglavnom ćemo koristiti za Difi-Helman algoritam ili protokol za razmenu ključa. Protokol je razvijen nezavisno na dva mesta². Predstavlja algoritam za razmenu zajedničkih simetričnih ključeva. Nije namenjen za šifrovanje ili digitalno potpisivanje. Bezbednost *DH* algoritma zasniva se na računski složenom računanju (jednosmerne funkcije) diskretnog algoritma za zadate g, p i $g^n \bmod p$ naći n . Za poznato g i x , gde je $x = g^n$, može da se odredi n :

$$n = \log_g(x)$$

Ako je $x = g^n \pmod{p}$, n se takođe određuje preko logaritma ali diskretnog (diskretni algoritam). U nastavku ćemo proći kroz matematičke osnove *DH* algoritma. Neka je p veliki prost broj i g takvo da se za svako $x \in \{1, 2, \dots, p-1\}$ može naći n tako da je:

¹ Vitfild Difi rođen je 1944. godine u Njujorku. 1965. diplomirao na Stanford Univerzitetu. Dostupno više na Veb sajtu: <http://en.wikipedia.org/wiki/Whitfield>.

Martin Helman rođen je 1945. godine, u Bronksu. Doktorirao na Stanford Univerzitetu. Dostupno više na sajtu: <http://en.wikipedia.org/wiki/MartinHellman>.

² *Government Communications Headquarters – GCHQ*: Džems Elis, Kliford Koks, Malkom Vilijamson. Stanford Univerzitet: Difi i Helman

$$x = g^n \pmod{p}$$

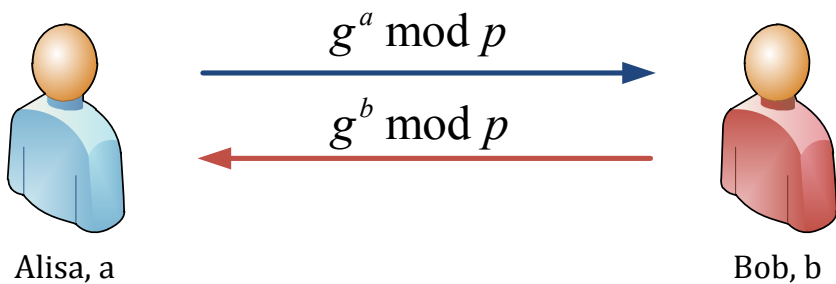
Vrednosti p i g su javne. U komunikaciji između Alise i Boba, ove parametre može da odredi bilo ko od njih, a zatim se parametri razmenjuju javnim kanalom. Alisa bira svoju tajnu vrednost a . Bob bira svoju tajnu vrednost b . Ove vrednosti predstavljaju velike slučajne proste brojeve.

U prvoj rundi, Alisa javno šalje vrednost $g^a \pmod{p}$ Bobu. Bob javno šalje vrednost $g^b \pmod{p}$ Alisi. U drugoj rundi, oboje na osnovu primljenih vrednost računaju zajedničku tajnu vrednost $g^{ab} \pmod{p}$. Dobijena zajednička tajna vrednost može da se koristi kao simetrični ključ.

Pretpostavimo da Alisa i Bob koriste vrednost $g^{ab} \pmod{p}$ kao simetrični ključ. Trudi može da sazna vrednosti $g^a \pmod{p}$ i $g^b \pmod{p}$ jer su poslate javno, kanalom veze. Međutim, Trudi ne može na osnovu ovih vrednosti da sazna vrednost a ili b , a ako bi to mogla da uradi, sistem bi bio razbijen, a to bi značilo da je rešila problem diskretnog algoritma. Standardom PKSC #3³, definisane su i preporučene vrednosti parametara a, b, g i p za generisanje i razmenu zajedničkih simetričnih ključeva. U praksi se za p vrednost koristi veliki broj koji je veći od 1024 bita. Nakon malog podsetnika na DH protokol, nastavice sa implementacijom PFS metoda čija osnova će upravo postati DH protokol za razmenu simetričnih ključeva. Na sledećoj slici (Slika 3.13) prikazan je dizajn DH protokola. podsetimo se još jednom, g i p su javni parametri, dok su a i b tajne vrednosti koje su samo poznate Alisi i Bobu.

³ PKCS #3: Diffie-Hellman Key Agreement Standard.

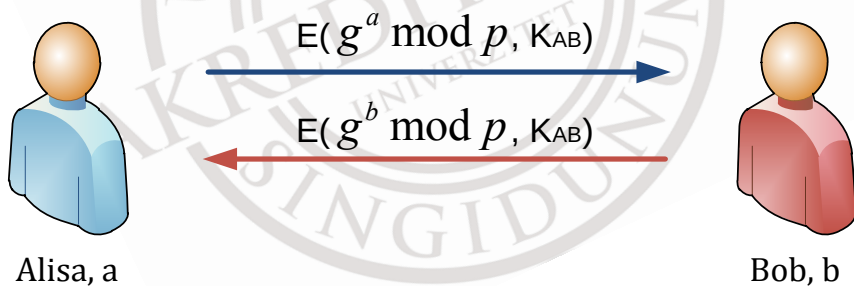
Dostupno na Veb sajtu: <http://www.rsa.com/rsalabs/node.asp?id=2126>



Slika 3.13 *DH* protokol za razmenu simetričnih ključeva

Sada kada smo upoznati sa problemima autentifikacije, jasno možemo da vidimo sa ove slike ne postoji autentifikacija između Alise i Boba. To znači da Alisa nije sigurna sa kim je razmenila zajednički ključ i obrnuto Bob nije siguran da je na drugoj strani Alisa. Ovim je omogućen *MiM* napad ili čovek u sredini, a to dalje znači da je *DH* protokol podložan ovoj vrsti napada.

Kako ostvariti *PFS* i istovremeno sprečiti *MiM* napad? Odgovor je dat na sledećoj slici (Slika 3.14).

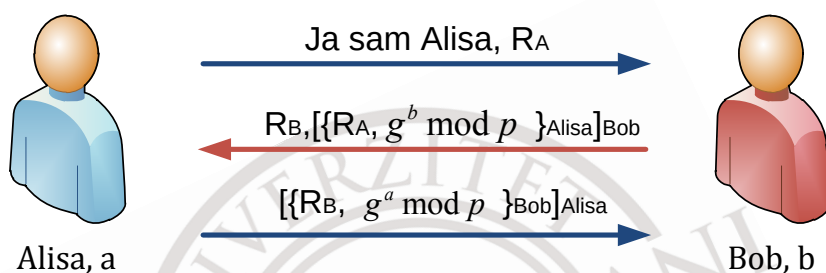


Slika 3.14 Pravilna implementacija *PFS* metoda

Ovo je interesantan pristup za implementaciju *PFS* metode koja ispunjava sve postavljene zahteve. U ovoj realizaciji *PFS*-a, ključ sesije K_s se više ne prenosi preko mreže. Možemo da primetimo da se K_s sada izračunava na Alisinoj i Bobovoj strani, a nakon izračunavanja Alisa i Bob permanentno zaboravljaju (uništavaju na siguran način) tajne parametre a i b koji su iskorišćeni samo za određeni ključ sesije. Za svaki novi ključ sesije, parametri će nanovo biti generisani na neki slu-

čajan način. Ovim smo dobili efemerni *DH* protokol u kojem čak ni Alisa ni Bob ne mogu kasnije da rekonstruišu K_s .

Da li postoji još neki drugi pristup koji će omogućiti implementaciju *PFS*-a? Postoji još jedan pristup, čiji je dizajn u osnovi većine savremenih kriptografskih protokola današnjice. On objedinjava na jednom mestu protokol za uzajamnu autentifikaciju, ključ sesije i *PFS*. Ovaj pristup dizajna kompletnog protokola kombinuje protokol sa slike (Slika 3.10) i *DH* protokolom na slici (Slika 3.13).



Slika 3.15 Protokol za uzajamnu autentifikaciju, razmeni sesijskog ključa sa *PFS* metodom

Sada smo stavili sve elemente protokola koje smo do sada razmatrali, zajedno u dizajn protokola, čime smo omogućili uzajamnu autentifikaciju, razmenu ključa sesije sa *PFS*-om. Sa slike (Slika 3.15) se jasno vidi da je to protokol potpiši pa šifruj, modifikovan sa *DH* protokolom. U ovom protokolu su Alisa i Bob autentifikovani, komunikacija u vidu sesija je bezbedna, obezbeđen je *PFS* i na osnovu svih ovih poboljšanja zaključujemo da nema očiglednih napada.

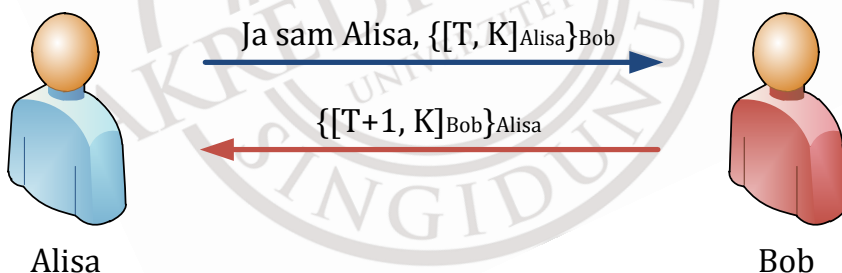
3.2.3. VREMENSKI PEČAT

Vremenski pečat predstavlja tekuće vreme koje je obično predstavljeno u milisekundama. Kod računara takvo vreme nazivamo vremenski pečat (engl. *Timestamp*). Vremenski pečat može da bude korišćen u protokolima na mestu iza-zova (engl. *Nonce*), jer vremenski pečat održava svežinu parametara. Omogućava nam beleženje trenutnog vremena u milisekundama, u momentu slanja ili prijema poruka. Ovakve vremenske oznake se koriste kod mnogih realnih bezbednosnih protokola, kao što su *Kerberos*, o kome ćemo govoriti u sledećem poglavlju.

Korišćenje vremenskog pečata implicira da je vreme bezbednosno-kritičan parametar. Zašto bezbednosno kritičan parametar? Zato što Trudi može pokušati da izvede napad na Alisin sat i tako uspe da reprodukuje poruku u dozvoljenim vremenskim okvirima koje nazivamo vremenska tolerancija. Dodatni problem je činjenica da vreme nije egzaktno jednako u dva odvojena trenutka, tako da se u protokolima mora predvideti određeno vremensko kašnjenje ili vremenska tolerancija. Kolika je vremenska tolerancija dovoljna u protokolima? Za određivanje vremenske tolerancije neophodno je da znamo koliki je stepen sinhronizacije između Alise i Boba, zatim koliko su vremenski zahtevani određeni procesi po fazama protokola između Alise i Boba.

U realnim protokolima, Alisa i Bob koriste *NTP*⁴ (engl. *Network Time Protocol*) protokol za vremensku sinhronizaciju, sinhronizujući njihove računare u svega par milisekundi.

Da bi predstavili značaj vremenskog pečata u protokolu, razmotrićemo dizajn protokola sa slike (Slika 3.16). Ovaj protokol sa vremenskim pečatom je u suštini verzija protokola potpiši pa šifruj, koji smo prikazali na slici (Slika 3.10). Uvodeći vremensku oznaku smanjili smo broj poruka, nemamo više trećeg koraka.



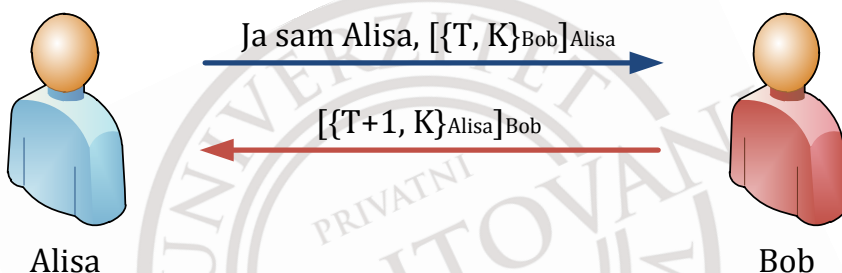
Slika 3.16 Autentifikacija sa vremenskim pečatom

Protokol na slici (Slika 3.16) koristi vremenski pečat ili vremensku oznaku. Dizajn protokola sadrži dva koraka:

⁴ Link: http://en.wikipedia.org/wiki/Network_Time_Protocol

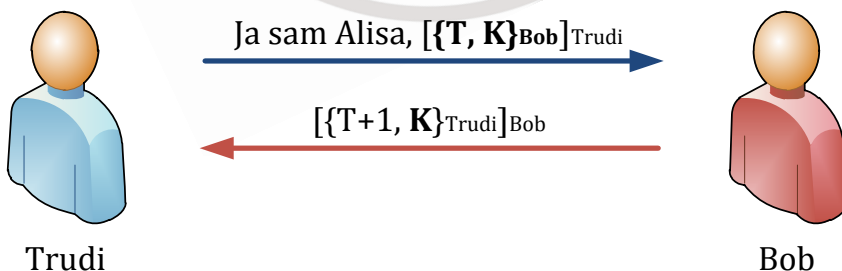
1. Alisa šalje poruku o svom identitetu „Ja sam Alisa“, vremensku oznaku T i ključ sesije K po principu potpiši pa šifruj.
2. Bob dešifruje poruku koja sadrži vremensku oznaku T i ključ sesije K , a zatim verifikuje Alisin potpis (autentifikuje Alisu). U narednoj fazi računa novu vremensku oznaku $T+1$ i zajedno sa ključem sesije K potpisuje i šifruje vrednosti sa Alisanim javnim ključem. Na kraju protokola, Alisa na identičan način autentifikuje Boba.

Primenjenim pristupom potpiši pa zatim šifruj, dobili smo dizajn protokola koji izgleda da je potpuno bezbedan. Ne zaboravimo da Alisa i Bob sada komuniciraju u okvirima neke zadate vremenske tolerancije.



Slika 3.17 Šifruj pa potpiši sa vremenskom oznakom

Razmotrimo sledeći scenario, Alisa i Bob koriste skoro sličan dizajn protokola, s tim što je promenjen redosled operacija sa javnim ključem. Sada umesto potpiši pa šifruj, primenili su pristup šifruj pa potpiši, protokol na slici (Slika 3.17).



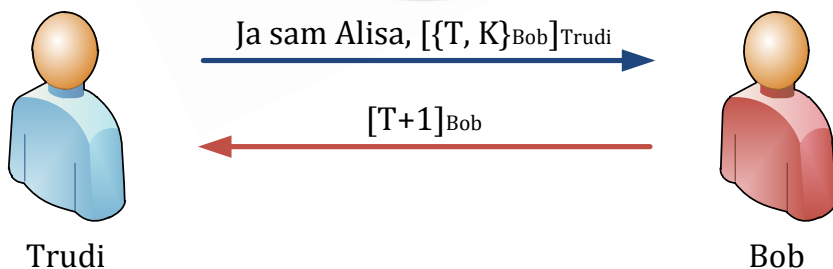
Slika 3.18 Trudi napada pristup šifruj pa potpiši

Koliko je bezbedan ovaj dizajn protokola? Izgleda da Trudi može da upotrebi Alisin javni ključ u cilju nalaženja $\{T, K\}_{\text{Bob}}$, a zatim da vrlo lako sazna šta je ključ K. Razmotrimo ovaj potencijalni napad koji je prikazan na slici (Slika 3.18).

Objasnićemo detaljno, kako Trudi realizuje ovaj napad? Na protokolu sa slike (Slika 3.17), Trudi je opservirala komunikaciju između Alise i Boba. Preko Alisinog javnog ključa došla je do šifrata $\{T, K\}_{\text{Bob}}$. Napominjemo da je cilj ovog napada ključ K. Od ovog momenta Trudi postaje aktivni napadač. U naredna dva koraka saznaje šta je ključ K i dešifruje sve šifrovane poruke koje su vezane za sesiju.

1. Trudi šalje poruku koja sadrži Alisin identitet “Ja sam Alisa” i potpisanu vrednost $\{T, K\}_{\text{Bob}}$.
2. U sledećem korak Bob odaje vrednost ključa K, tako što modifikuje vremensku oznaku sa $T+1$ i zajedno sa ključem K šifruje sa javnim ključem od Trudi. Trudi sada vrlo lako koristeći svoj privatni ključ, saznaje vrednost ključa K.

Na ovaj scenario napada potrebno je staviti malu primedbu, Trudi mora delovati u okviru vremenske tolerancija. Da li nebezbedni protokol sa slike (Slika 3.18) može da se popravi? Potrebne su manje modifikacije, nakon kojih bi ovaj protokol postao bezbedan. Na primer, ne postoji potreba da Bob vraća ključ K Alisi u drugoj poruci. Svrha druge poruke je da Alisa autentifikuje Boba. Vremenska oznaka u poruci je u potpunosti dovoljna za autentifikaciju Boba. Napad koji Trudi izvodi je fokusiran samo na ključ K u drugoj poruci. Sada kada smo predložili sve modifikacije, videćemo kako izgleda poboljšana verzija prethodno nebezbednog protokola, prikazan na slici (Slika 3.19).



Slika 3.19 Sigurna verzija protokola šifruj pa potpiši

Već na prvi pogled možemo da uočimo da ključ više ne postoji u drugoj poruci koju je Bob poslao Alisi. Trudi više ne može da napadne ovaj protokol.

Nakon upoznavanja sa konceptom vremenskih oznaka (vremenskih pečata), navešćemo prvo bezbedne pristupe u dizajnu ovih protokola za autentifikaciju.

- Potpisati i šifrovati sa izazov (vrednost R) - bezbedno;
- Šifrovati pa potpisati sa izazov (vrednost R) - bezbedno;
- Potpisati i šifrovati sa vremenskim pečatom - bezbedno;
- Šifrovati pa potpisati sa vremenskim pečatom - nebezbedno;

Ovo je još jedna potvrda teze da su protokoli vrlo suptilni i da bezbednosni problemi koji mogu da nastanu, ne moraju uvek biti očigledni. Koncept koji podrazumeva uvođenje vremenskih pečata primenjen je u svim stvarnim protokolima današnjice, o kojima će biti više reči u sledećem poglavlju.

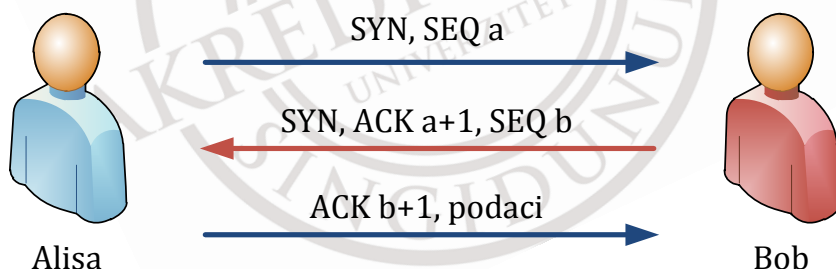


3.3. AUTENTIFIKACIJA ZASNOVANA NA TCP PROTOKOLU

U ovom odelju ukratko ćemo razmotriti *TCP* (engl. *Transmission Control Protocol*) protokol koji se ponekad može koristiti za autentifikaciju. *TCP* protokol u osnovi nije dizajniran da se upotrebljava za proveru identiteta i iz tog razloga ne treba da nas čudi što nije dovoljno bezbedan. Ali njegov dizajn ilustruje neka interesantna pitanja sa aspekta bezbednosti na mreži.

TCP u konekciji često koristi *IP* adresu kao parametar za autentifikaciju. Čak, jedan od načina rada *IPSec*-a koristi *IP* adresu za autentifikaciju, i iz tog razloga može da prouzrokuje bezbednosne probleme. Ukoliko bi scenario sa *IP* adresom bio bezbedan, onda nam ne bi bili potrebni neki kompleksni elementi protokola za autentifikaciju.

U nastavku ćemo dati primer *TCP* protokola koji se koristi za autentifikaciju, kao i potencijalne napade na njega. Da bismo razumeli kako radi *TCP* protokol, moramo se prvo upoznati sa fazom rukovanja (engl. *Handshake*). Faza rukovanja je implementirana kroz tri koraka (engl. *three-way handshake*), slika (Slika 3.20).



Slika 3.20 *TCP* – faze rukovanja

1. U prvom koraku, Alisa šalje Bobu zahtev za sinhronizaciju. Ovaj korak ne sadrži podatke aplikativnog nivoa, već sinhronizacioni bit - *SYN*, čija je vrednost postavljena na 1 i inicijalni redni broj *SEQ a*.
2. U drugom koraku, Bob odgovara sa tri veoma važna parametra. Prvi parametar je *SYN*, takođe vrednost postavljena na 1, drugi potvrđuje inicijalni redni broj *a*, koji je Alisa generisala (*ACK a+1*) i treći predstavlja inicijalni redni broj koji generiše Bob (*SEQ b*).

3. U trećem koraku, Alisa odgovara Bobu sa parametrom koji potvrđuje prijem Bobovog inicijalnog rednog broja b , tako što šalje ($ACK\ b+1$) i SYN parametar postavlja na vrednost 0, čime je konekcija uspostavljena.

Napominjemo da inicijalni parametar $SEQ\ a$ i $SEQ\ b$, moraju biti slučajni brojevi, generisani na slučajan način. Videćemo kasnije, zašto je ovo važno?

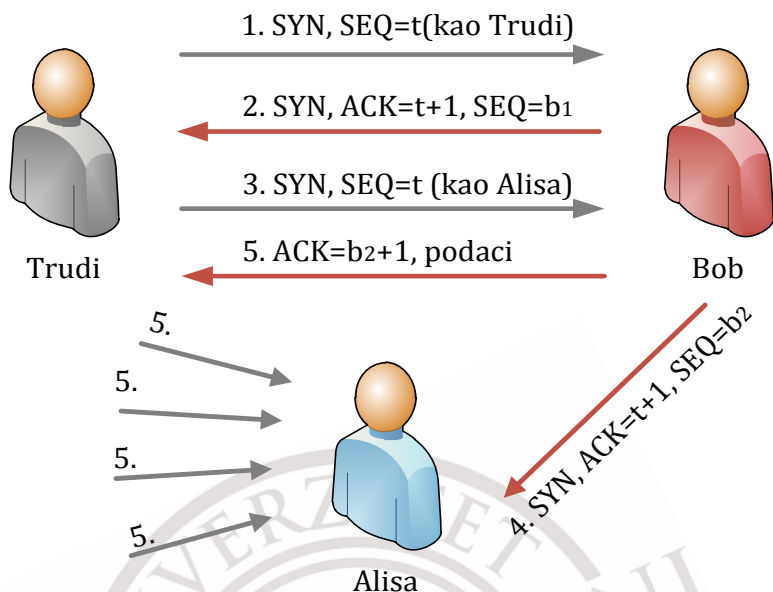
Pretpostavimo da Bob nakon uspostavljanja veze preko TCP protokola sa Alisom veruje da data IP adresa pripada Alisi. U ovom slučaju Bob je koristio TCP protokol za autentifikaciju Alise. Obzirom da Bob šalje $SYN-ACK$ indikator potvrde na Alisinu IP adresu, logično je da odgovarajući ACK mora da dođe sa Alisine adrese. Odnosno, ako Bob proveri $ACK\ b+1$ koji se pojavljuje u trećoj poruci, on ima neki razlog da veruje Alisi i njenoj IP adresi, preko koje je primila poruku i odgovorila.

Ne zaboravimo da druga poruka sadrži $SEQ\ b$, i da niko drugi ne sme da zna b . Ukoliko pretpostavimo da Trudi ne može da vidi $SYN-ACK$ paket u drugoj poruci, time neće da zna vrednost b i neće moći lako da napadne ovaj protokol. Međutim, u praktičnom smislu to je veoma teško za Trudi. Tačnije, da presretne poruku koja sadrži $SEQ\ b$, ako Trudi ne može da sazna parametar b , tada je zaključak da je protokol bezbedan.

Da li je moguć u ovom slučaju neki drugi tip napada na TCP protokol. Čak i ako Trudi ne može da sazna početne vrednosti ($SEQ\ b$), ona može biti u stanju da napravi razumne pretpostavke. Ovaj primer napada je prikazan na slici (Slika 3.21).

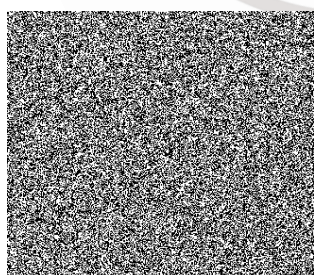
U ovom napadu Trudi prvo šalje običan zahtev Bobu za sinhronizaciju (SYN). Bob odgovara sa potvrdom ($SYN-ACK$), na osnovu koje Trudi ispituje i saznaje Bobovu inicijalnu vrednost $SEQ\ b1$ u paketu $SYN-ACK$.

Pretpostavimo sada da Trudi može koristiti $b1$, na osnovu koje može da predvidi sledeću Bobovu inicijalnu vrednost $SEQ\ b2$. Tada Trudi može poslati paket Bobu sa lažne IP adrese koja odgovara Alisinoj IP adresi. U nastavku, Bob će poslati $SYN-ACK$ na Alisinu IP adresu po pretpostavci, a koju Trudi ne može da vidi. Ali, ako Trudi može da pogodi $SEQ\ b2$, ona će moći da kompletira uspostavljanje protokola tako što će poslati Bobu $SYN-ACK\ b2+1$.

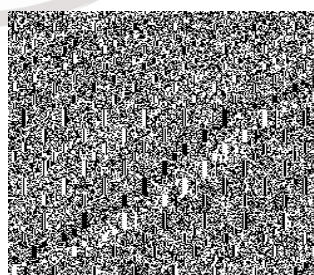


Slika 3.21 Napad na TCP protokol

Rezultat ovog napada je da Bob veruje da su podaci koje dobija Trudi stvarno otišli Alisi. Ovaj napad je dobro poznat u stvarnosti, a krivica je na inicijalnim *SEQ* brojevima koji treba da budu generisani na slučajan način, ali njihove osobine nisu u korelaciji sa slučajnim brojevima. Očekivano je da oni budu slučajni, ali oni obično u praksi nisu ni malo slučajni. Na primeru slika (Slika 3.22), data je vizuelna komparacija očekivanog stepena slučajnosti i slučajnost *SEQ* broja generisanog preko ranih verzija operativnih sistema.



Slučajni kvalitetni *SEQ* brojevi



Slučajni nekvalitetni *SEQ* brojevi

Slika 3.22 Komparacija slučajnosti *SEQ* brojeva

Ovo je samo potvrda da mnogi proizvođači softvera ne umeju da generišu slučajne brojeve i da mesto i način generisanja slučajnih brojeva predstavlja još jednu kritičnu tačku celokupne sigurnost protokola.

TCP protokol će predstavljati lošu ideju za obezbeđivanje servisa autentifikacije, čak i ako su inicijalni *SEQ* brojevi generisani na potpuno slučajan način preko prirodnih izvora informacija. Očigledno rešenje je uvođenje jednog sloja iznad *TCP* protokola, koji bi implementirao protokol za autentifikaciju nakon uspostavljanja *TCP* konekcije.

Ovo poboljšanje bi bilo značajno, čak i ako bismo uveli upotrebu lozinki, tada se ne bi oslanjali samo na *TCP* protokol. Razlog zbog čega se *TCP* i dalje koristi u praksi za autentifikaciju je zbog njegovog mesta u mrežnim slojevima i njegova jednostavnost koja obezbeđuje manje brige korisnicima, ali ne mislimo na brigu o bezbednosti *TCP* protokola. Zaključak je da *TCP* nije dobar za autentifikaciju, čak i ako se koriste informaciono kvalitetni *SEQ* brojevi.



3.4. DOKAZI SA NULTIM ZNANJEM – ZKP

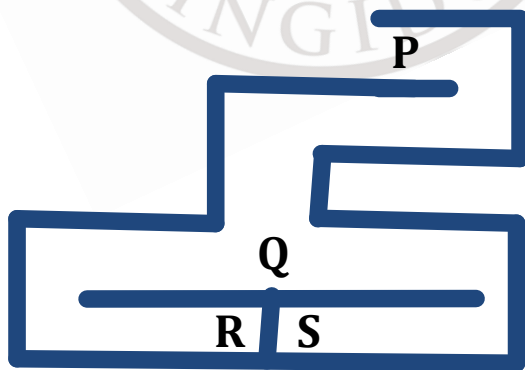
Sistemi sa nultim znanjem se primenjuju u situacijama kada Alisa želi da Bobu dokaže nešto, recimo da poseduje rešenje nekog teškog problema, a pri tom ne želi da oda samo rešenje, jer predstavlja tajnu.

Kod ovog dokaza, Alisa će dokazati Bobu da je neka tvrdnja X tačna, Bob će biti potpuno uveren da je X tačno, ali neće naučiti baš ništa. Samim tim Bob će steći „nulto znanje“. Dokaz nultog znanja se može uporediti sa izazov-odgovor (engl. *challenge-response*) protokolom.

Na prvi pogled ovakav dizajn protokola zvuči nemoguće. Međutim, zahvaljujući jednom interaktivnom procesu koji se odvija između Alise i Boba, Bob može da verifikuje da Alisa zna tajnu sa proizvoljno velikom verovatnoćom. Ovaj tip protokola predstavlja sistem interaktivnog dokazivanja.

U autentifikacionom protokolu dokazi sa nultim znanjem (engl. *Zero Knowledge Proof*), Alisa želi da dokaže Bobu da ona zna tajnu bez otkrivanja bilo koje informacije o tajni pred Bobom ili pred Trudi. Bob mora da verifikuje da Alisa zna tajnu, iako ne dobija nikakvu informaciju o tajni.

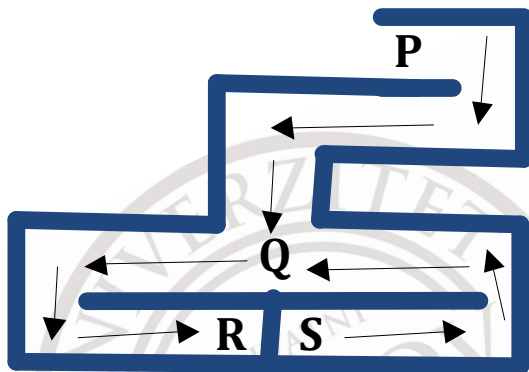
Pre nego što objasnimo jedan takav protokol, prvo treba da zamislimo Bobovu pećinu, koja je prikazana na slici (Slika 3.23).



Slika 3.23 Bobova pećina

Alisa tvrdi da zna tajnu reč koja otvara put između tačaka R i S („Sezame otvori se“). Da li ona može da uveri Boba da zna tajnu reč bez njenog otkrivanja?

Razmotrimo sledeći protokol u kom Alisa ulazi u Bobovu pećinu, baca novčić od kog zavisi da li će dospeti na stranu R ili S. Bob tada ulazi u pećinu i nastavlja do pozicije Q (pozicija sa koje Bob postavlja pitanje Alisi ili Trudi). Pretpostavimo da je Alisa dospela na stranu R. Ova situacija je prikazana na slici (Slika 3.24).



Slika 3.24 Bobov pećinski protokol

Tada Bob baca novčić i na slučajan način odabira jednu stranu, koja predstavlja korektnu stranu. Izabrana strana predstavlja pitanje na koje će Alisa sa velikom verovatnoćom tačno odgovoriti, pod uslovom da zna tajnu. Na slici (Slika 3.24), ako se dogodi da Bob izabere stranu R, Alisa će izabrati verovatno stranu R ili ako se dogodi da Bob izabere stranu S, tada će Alisa dospeti na stranu S, sve pod uslovom da ona zna tajnu. Na kraju protokola, vrata između R i S će se otvoriti.

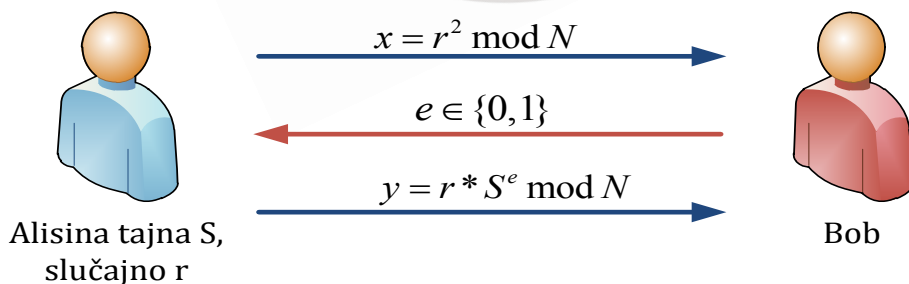
Drugim rečima ako Alisa ne zna tajnu, verovatnoća sa kojom ona može da prevari Boba je $1/2$. Jasno je da u ovom slučaju Alisa ne zna tajnu preko koje može da uveri Boba da je to zaista ona. Ova činjenica ne uliva mnogo poverenja u ovaj protokol, ali ukoliko se ovaj proces ponavlja iterativno n puta, tada je verovatnoća da Alisa prevariti Boba sa verovatnoćom $(1/2)^n$. Dakle, zaključak je da Alisa i Bob moraju da ponove protokol n puta i da Alisa pogodi odgovor svaki put da bi Bob poverovao da Alisa zna tajnu.

Treba imati na umu sledeće, obzirom da se radi o protokolu koji je zasnovan na verovatnoći, uvek postoji šansa da Alisa ili Trudi prevari Boba sa nekom verovatnoćom. Međutim, Bob može da kontroliše ovakvu mogućnost, tako što će sam odrediti broj iteracija n . Na primer, za zadati broj iteracija $n = 20$ verovatnoća prevare je jedan u milion slučajeva, to je zaista mala verovatnoća, ali sa povećanjem broja iteracija ova verovatnoća može da bude još manja. Takođe, druga je pretpostavka da Bob potpuno slučajno bira strane, jer ukoliko bi njegov odabir bio predvidiv, definisan nekim pravilom, tada bi Trudi mogla da projektuje napad na Boba.

Preko ovog apstraktnog primera protokola sa scenarijom pećini Bob je dokazao da je ovaj protokol po principu nultog znanja moguć, iako ovakvi protokoli nisu naročito popularni.

Da li možemo u praksi postići pećinski efekat, ali bez pećine? Odgovor je da, zahvaljujući *Fiat-Shamir* protokolu. U ovom odeljku razmatraćemo jednu fascinantnu šemu provere identiteta, koju je razvio *Fiege, Fiat* i *Shamir*. Ovaj protokol je u stručnoj literaturi poznat kao *Fiat-Shamir* protokol koji ćemo u nastavnu ovog odeljka proučiti.

Poznato je da nalaženje kvadratnog korena po modulu N predstavlja težak problem, slično kao i faktORIZACIJA velikih prostih brojeva. Upravo na tu činjenicu se oslanja *Fiat-Shamir* protokol. Neka je $N = pq$, gde su p i q prosti brojevi. Alisa poseduje neku tajnu S , koja se podrazumevano mora držati u tajnosti. Brojevi N i $V = S^2 \bmod N$ su jani parametri. Alisa sada mora da uveri Boba da ona zna S bez otkrivanja bilo kakve informacije o vrednosti S .



Slika 3.25 *Fiat-Shamir* protokol

Fiat-Shamir protokol prikazan je na slici (Slika 3.25). Alisa u prvo na slučajan način generiše r i računa $x = r^2 \bmod N$. Zatim, u prvoj poruci vrednost x šalje Bobu. U drugoj poruci, Bob generiše slučajnu vrednost $e \in \{0, 1\}$, koju šalje Alisi. U narednom koraku Alisa za uzvrat izračunava $y = rS^e \bmod N$, koje šalje Bobu. Na kraju protokola, Bob mora da verifikuje da važi:

$$y^2 = xv^e \bmod N,$$

i ako su oboje pravilno sledili faze protokola, sledeća tvrdnja mora da bude tačna:

$$y^2 = r^2 S^{2e} = r^2 (S^2)^e = xv^e \bmod N.$$

U drugoj poruci protokola sa slike (Slika 3.25), Bob šalje za vrednost e broj 1 ili broj 0. U nastavku ćemo odvojeno razraditi oba slučaja. Ako Bob pošalje vrednost $e = 1$, tada Alisa odgovara sa $y = r \cdot S \bmod N$ u trećoj poruci, tada važi jednakost

$$y^2 = r^2 = x \bmod N.$$

Imajte na umu da Alisa u ovom slučaju ne mora da zna tajnu S . Ovo može da deluje čudno, ali to je upravo ekvivalentno situaciju u Bobovoj pećini, gde Alisa ne mora da otvori tajni prolaz da bi dospela na korektnu stranu. Ova situacija deluje primamljivo, u kojoj Bob šalje $e = 1$. Međutim, videćemo da u nekom trenutku to ne bi bilo mudro.

Prva faza protokola je identična kao sa slike (Slika 3.25). Alisa ne mora da otkrije r , iz razloga što je pronalaženje kvadratnog korena po modulu veoma teško. druga poruka je faza izazova, u kojoj Bob izaziva Alisu da da tačan odgovor. Treća poruka je faza odgovaranja na izazov koji je postavio Bob, u kojoj Alisa mora odgovoriti sa tačnim odgovorom. Bob verifikuje Alisin odgovor koristeći jednakost

$$y^2 = r^2 S^{2e} = r^2 (S^2)^e = xv^e \bmod N.$$

Ova faza *Fiat-Shamir* protokola odgovara trećem koraku u Bobovoj pećini.

Matematička osnova *Fiat-Shamir* protokola će raditi ispravno pod uslovom da svi pravilno slede faze protokola. Bob može da verifikuje $y^2 = xv^e \bmod N$, na osnovu informacije koju on dobija na prijemu. Međutim to ne čini ovaj protokol sigurnim. Da bismo ga učinili sigurnim, moramo se uveriti da li potencijalni napadač Trudi može uveriti Boba da ona zna Alisinu tajnu S i time ubedi Boba da je ona Alisa.

Pretpostavimo sada da Trudi očekuje da Bob pošalje za izazov e vrednost $e = 0$ u drugoj poruci. Tada Trudi može da pošalje $x = r^2 \bmod N$ u prvoj poruci i $y = r \bmod N$ u trećoj poruci. U ovom slučaju Trudi jednostavno sledi faze protokola, jer ona i ne treba da zna tajnu S .

Sa druge strane, ako Trudi očekuje da Bob pošalje $e = 1$, tada ona može poslati $x = r^2 v^{-1} \bmod N$ u prvoj poruci i $y = r \bmod N$ u trećoj poruci. Sledeći protokol, Bob će izračunati $y^2 = r^2$ i $xv^2 = r^2 v^{-1} v = r^2$ i u tom slučaju pronaći da važi jednakost

$$y^2 = r^2 S^{2e} = r^2 (S^2)^e = xv^e \bmod N,$$

i iz tog razloga Bob prihvata rezultat kao važeći.

Na osnovu ovoga što smo naveli, zaključak je da Bob mora izabrati $e \in \{0, 1\}$ na slučajan način (engl. *Random*), jer tada Trudi može da prevari Boba samo sa verovatnoćom $p = 1/2$.

Iz svega ovoga zaključujemo da Fiat-Shamir protokol zahteva od Boba da izazovi koje generiše budu nepredvidljivi za Trudi. Pored toga, Alisa u svakoj iteraciji protokola mora generisati r na slučajan način, u protivnom njena tajna S će biti otkrivena.

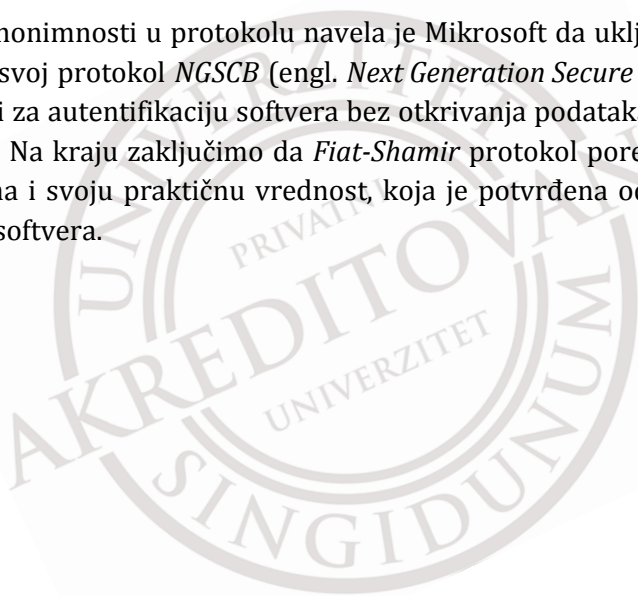
Da li Fiat-Shamir protokol stvarno pripada grupi protokola poznatim kao „dokaz sa nultim znanjem”? To jest, može li Bob ili bilo ko drugi saznati nešto o Alisinoj tajni S . Podsetimo se da su v i N javni parametri, gde je $v = S^2 \bmod N$. Pored toga Bob u ovoj poruci vidi $r^2 \bmod N$ i pod pretpostavkom da je $e = 1$, Bob u trećoj poruci vidi $rS \bmod N$. Ako Bob može da pronađe r od $r^2 \bmod N$, tada on može da pronađe S . Međutim, pronalaženje kvadratnog korena po modulu je računarski neizvodljivo. Čak, iako nekako uspe da pronađe takav kvadratni koren, on može da dobije tajno S direktno iz javnog parametra v bez maltretiranja sa protokolom. Iako obo nije rigorozni dokaz da je Fiat-Shamir protokol sa nultim znanjem, to ne ukazuje na to da ne postoji ništa što je očigledno u samom protokolu što pomaže Bobu da se odredi Alisin tajni S .

Da li imamo neke koristi od Fiat-Shamir protokola, ili je to samo zabavna igra matematičara. Na primer, ako koristimo javne ključeve za autentifikaciju, tada svaka strana mora da zna javni ključ one druge. Sada, ako bismo primenili Fiat-

Shamir dizajn protokola na protokol sa javnim ključevima, Alisa ne bi znala Bobov javni ključ i obrnuto. U protokolima sa javnim ključevima važi pretpostavka da Bob šalje svoj digitalni sertifikat Alisi. Međutim, taj sertifikat identifikuje Boba na osnovu koga Trudi zna da Bob učestvuje u komunikaciji. Možemo da zaključimo da javni ključevi onemogućavaju učesnicima da ostanu anonimni.

Potencijalna prednost protokola sa nultim znanjem je u postojanju anonimnosti u autentifikaciji. U Fiat-Shamir protokolu obe strane moraju da znaju vrednosti javnih parametara, ali nijedan parametar ne otkriva Alisin identitet i ne postoji nikakva skrivena informacija u porukama koje se razmenjuju koje bi mogle otkriti Alisin identitet.

Mogućnost anonimnosti u protokolu navela je Mikrosft da uključi protokol nultog znanja u svoj protokol *NGSCB* (engl. *Next Generation Secure Computing Base*), koji se koristi za autentifikaciju softvera bez otkrivanja podataka za identifikovanje računara. Na kraju zaključimo da *Fiat-Shamir* protokol pored svoje teorijske prednosti, ima i svoju praktičnu vrednost, koja je potvrđena od strane najvećih proizvođača softvera.



3.5. NAJBOLJI AUTENTIFIKACIONI PROTOKOLI

U realnom svetu ne postoji najbolji protokol za autentifikaciju. Teško je dizajnirati univerzalni protokol koji će biti toliko fleksibilan, a pored toga i sa aspekta bezbednosti najbolji. Upravo odgovor na pitanje šta je najbolje za određenu situaciju zavisice od mnogo faktora koji će uticati na stvaranje novog protokola namenskog dizajna, a koji će biti sposoban da odgovori na sve izazove nametnutog okruženja. Za stvaranje ovakvih specijalizovanih protokola za autentifikaciju, neophodno je razmotriti sledeća pitanja.

- Koliko je aplikacija osetljiva?
- Koliko je kašnjenje dozvoljeno?
- Da li je cena prihvatljiva?
- Koje su kriptografske tehnike podržane?
- Da li je potrebna uzajamna autentifikacija?
- Da li se zahteva sesijski ključ?
- Da li se zahteva *PFS*?
- Da li se zahteva anonimnost korisnika?

U narednom poglavlju bavićemo se važnim kriptografskim protokolima današnjice, kao što su:

- *SSH/SSL* – bezbednost na Veb-u;
- *IPSec* – bezbednost na IP sloju;
- *Kerberos* – distribucija simetričnih ključeva;
- *WEP* – bezbednost na bežičnim mrežama;
- *GSM* – bezbednost mobilnih telefona;

4. SAVREMENI KRIPTOGRAFSKI PROTOKOLI

U ovom poglavlju ćemo diskutovati o nekoliko protokola koji su pronašli široku primenu u stvarnom svetu bezbednosnih protokola. Prvo polazimo od *SSH* (engl. *Secure shell*) protokola koji se koristi u razne svrhe, zatim *SSL*-a (engl. *Secure Socket Layer*) koji se trenutno koristi najviše u protokolima za bezbednost Internet transakcija, *IPSec*-a (engl. *Internet Protocol Security*) koji predstavlja jedan kompleksan protokol sa nekim značajnim bezbednosnim problemima, *Kerberos* popularni protokol za proveru verodostojnosti na osnovu simetričnih ključeva i vremenskih pečata. Danas većina savremenih centralizovanih servisa za autentifikaciju koristi u osnovi dizajn *Kerberos* protokola. Konkretni primer je danas dobro poznati protokol *OPEN-ID*⁵.

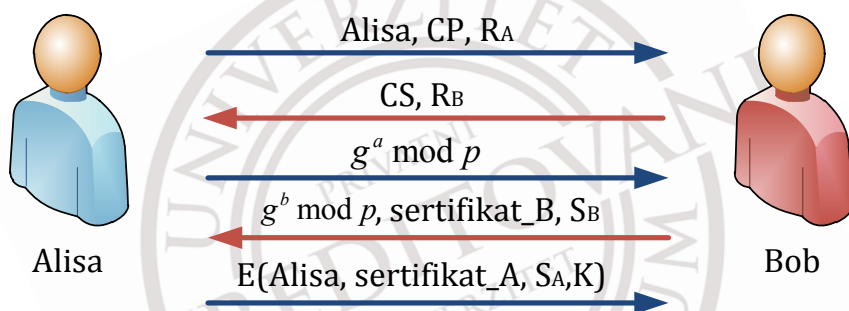
Na kraju, završavamo poglavlje sa *WEP* i *GSM* protokolom namenjenim za autentifikaciju na bežičnim mrežama. Ova dva protokola poseduju ozbiljne nedostatke, poprilično su zastareli, ali sa druge strane njihov je značaj što predstavljaju i dobre školske primere zbog velikog broja različitih dobro poznatih napada.

⁵ Link: <http://en.wikipedia.org/wiki/OpenID>

4.1. SSH

SSH protokol kreira bezbednosni tunel između Alisinog i Bobovog računara. Pretpostavimo da se Alisa povezuje sa Bobom, metodom udaljenog pristupa (engl. *Remote control*), gde SSH sesija obezbeđuje tajnost i zaštitu integriteta, čime se eliminiše mogućnost da Trudi dođe do lozinke ili neke druge poverljive informacije koja bi u drugom slučaju verovatno bila poslata nezaštićeno.

SSH protokol može biti dizajniran tako da koristi javne ključeve, digitalne sertifikate ili lozinke. U nastavku odeljka pojasnićemo rad protokola zasnovanog na digitalnim sertifikatima.



Slika 4.1 SSH jednostavan primer

Za SSH protokol prikazan na slici (Slika 4.1) korišćimo sledeće oznake:

- *sertifikat_A* – Alisin sertifikat
- *sertifikat_B* – Bobov sertifikat
- *CP* – predloženi kripto parametri
- *CS* – izabrani kripto parametri
- $H - h(Alisa, Bob, CP, CS, R_A, R_B, g^a \bmod p, g^b \bmod p)$
- $S_B - [H]_{Bob}$
- $K - g^{ab} \bmod p$
- $S_A - [H, Alisa, \text{sertifikat_A}]_{Alisa}$
- $h()$ – heš funkcija

U nastavku ćemo razmotriti protokol sa slike (Slika 4.1), kroz razmenjene poruke.

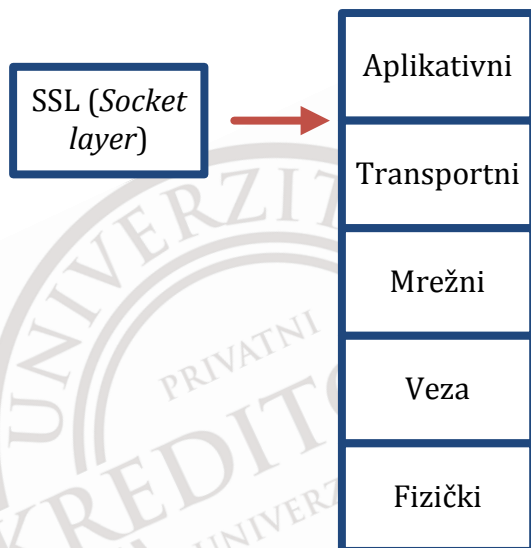
1. U prvoj fazi protokola, Alisa šalje prvu poruku sa sledećim parametrima:
 - Alisin identitet „Alisa“,
 - predložene krypto parametre CP (kripto algoritam, dužinu ključa, protokol za razmenu ključeva, *heš* funkciju itd),
 - Alisin parametar izazova R_A (na osnovu koga želi da autentifikuje Boba).
2. U drugoj fazi protokola, Bob selektuje krypto parametre koje je Alisa predložila u prvoj poruci i odgovara sa sledećim parametrima:
 - izabrani krypto parametri CS (kripto algoritam, dužinu ključa, protokol za razmenu ključeva, *heš* funkciju itd) ,
 - Bobov parametar izazova R_B (na osnovu koga želi da autentifikuje Alisu).
3. U trećoj fazi protokola, Alisa šalje svoje parametre DH (engl. *Diffie-Helman*) protokola:
 - vrednost $g^a \bmod p$ (na osnovu koje će Bob izračunati simetrični ključ K_{AB}) .
4. U četvrtoj fazi protokola, Bob odgovara sa sledećim parametrima na Alisinu poruku iz treće faze:
 - vrednost $g^b \bmod p$ (na osnovu koje će Alisa izračunati simetrični ključ K_{AB}),
 - *sertifikat_B* (Bobov sertifikat),
 - digitalno potpisane sve poruke koje su razmenjene do tog moment S_B .
5. U petoj fazi, Alisa ima sve parametre na osnovu kojih može da izračuna ključ K_{AB} , i u poslednjoj poruci šalje šifrovan blok koji sadrži:
 - Alisin identitet „Alisa“,
 - *sertifikat_A* (Alisin sertifikat),
 - digitalno potpisane sve poruke koje su razmenjene do tog moment S_A ,
 - uspostavljeni ključ K_{AB} .

Zadatak digitalnog potpisa u protokolu koji smo razmatrali je da obezbedi uzajamnu autentifikaciju preko parametara koji predstavljaju izazov sa Alisine i Bobove strane. Podsetimo se uloge vrednosti R_A koja predstavlja izazov. Ukoliko je Bob poslao Alisi izazov R_B , tada će samo Alisa moći tačno da odgovori. Na taj način Bob je uspešno autentifikovao Alisu i obrnuto. Protokol o kom smo diskutovali obezbeđuje uzajamnu autentifikaciju i razmenu simetričnog ključa K_{AB} .



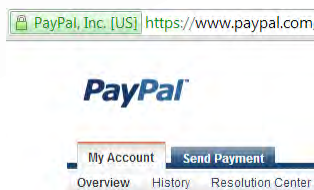
4.2. SSL/TLS

U savremenom elektronskom poslovanju *SSL* (engl. *Secure Sockets Layer*) protokol se koristi za većinu bezbednih transakcija preko Interneta. *SSL* protokol se nalazi između aplikativnog i transportnog sloja u *OSI* modelu (Slika 4.2), obično je smešten između *HTTP* i *TCP* protokola.



Slika 4.2 SSL u *OSI* modelu

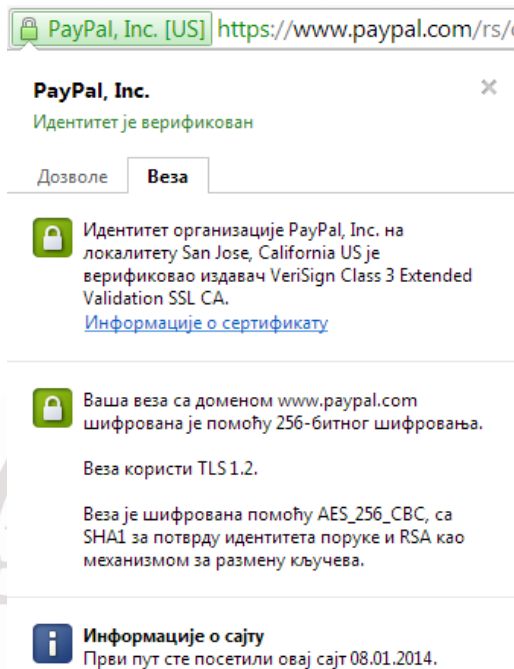
Na primer, ako Alisa želi kupiti neki proizvod preko *eBay*-a, verovatno će koristiti *PayPal* za plaćanje računa (Slika 4.3).



Slika 4.3 *PayPal* portal

U ovom slučaju, *PayPal* ima ulogu posrednika za finansijske transakcije između Alisine banke (i kreditne kartice) i Boba koji ima ulogu prodavca. Zapravo, njego-

va uloga je da Alisin novac na siguran način dostavi Bobu preko Interneta. Pretstavka je da Alisa i Bob veruju ovoj organizaciji, tada ova organizacija predstavlja treću stranu od poverenja.



Slika 4.4 *PayPal* sertifikat

Zašto nam je baš ovaj primer interesantan? Zato što Alisa koristi *SSL/TLS* protokol na osnovu koga autentifikuje *PayPal* organizaciju, a zatim šifrovano šalje svoje parametre (korisničko ime i lozinku) na osnovu čega Alisa potvrđuje svoj identitet.

Na slici (Slika 4.4) prikazane su osnovne informacije o protokolu i njegovim stanjima. Alisin Internet pregledač (*Chrome*) verifikuje ispravnost sertifikata, na osnovu koga je potvrđen identitet organizacije *PayPal*-a na lokalitetu *San Jose* u Kaliforniji *US*. Verifikacija je obavljena preko digitalnog potpisa koji pripada sertifikacionoj organizaciji *VeriSign*, u koju svi učesnici na Internetu imaju poverenje.

Nakon potvrđenog vlasništva, što govori o tome da sertifikat pripada organizaciji *PayPal*, Alisin računar stupa u bezbednu komunikaciju sa *PayPal* servisima. Nak-

nadno ćemo se baviti detaljima protokola koji se odnose na uspostavu veze, u ovom momentu navešćemo samo informacije koje se odnose na sigurnosne aspekte protokola.

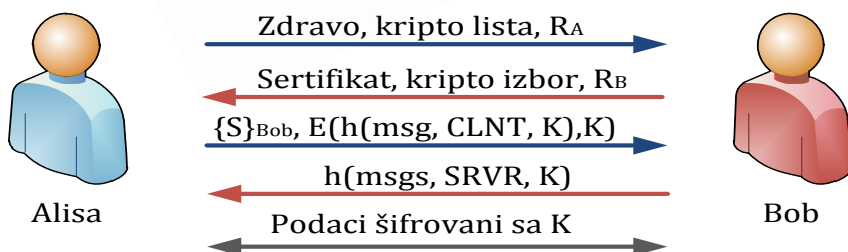
Za šifrovanje podataka, koristiće *AES_256_CBC* algoritme (*AES* je algoritam za šifrovanje, 256 bitova je dužina ključa, a *CBC* režim šifrovanja koji se koristi za ulančavanje blokova šifrata) sa *SHA1* (heš funkcija) za potvrdu identiteta poruke i *RSA* algoritam za razmenu simetričnog ključa. Zahvaljujući ovom protokolu uspostavljena je bezbedna veza, preko koje će Alisa započeti transakciju sa Bobom. Na ovaj način obezbeđena je autentifikacija i podaci sa kreditne kartice u prenosu su zaštićeni (poverljivost i/ili integritet).

4.2.1. ARHITEKTURA SSL PROTOKOLA

U nastavku ovog odeljka, na slici (Slika 4.5) prikazali smo kompletnu osnovu *SSL* protokola. Objasnićemo sada oznake koje ćemo koristili u razmatranju dizajna protokola.

- S – tajna pre glavne vrednosti
- $K = h(S, R_A, R_B)$
- $msgs$ – sve prethodne poruke
- $CLNT$ – klijentska konstanta
- $SRVR$ – serverska konstanta

gde je h heš funkcija. *SSL* protokol je daleko kompleksniji nego što je prikazano na slici (Slika 4.5).



Slika 4.5 Primer pojednostavljenog *SSL* protokola

U tekstu koji sledi, diskutovaćemo o svakoj fazi i poruci protokola.

1. U prvoj fazi protokola, Alisa šalje prvu poruku preko koje obaveštava Boba da želi da uspostavi *SSL* vezu, sa sledećim sadržajem u poruci:
 - listu krypto algoritama koje može da podrži (krypto algoritam, dužinu ključa, protokol za razmenu ključeva, heš funkciju itd),
 - parametar izazova R_A (na osnovu koga želi da autentifikuje Boba).
2. U drugoj fazi protokola, Bob je dobio prvu poruku od Alise i odgovara sa sledećim sadržajem u poruci:
 - sertifikat (*sertifikat_B*)
 - izabrane krypto parametre (krypto algoritam, dužinu ključa, protokol za razmenu ključeva, heš funkciju itd) ,
 - parametar izazova R_B (na osnovu koga želi da autentifikuje Alisu).
3. U trećoj fazi protokola, Alisa je dobila drugu poruku od Boba, zatim odgovara sa sledećim sadržajem u poruci:
 - digitalno potpisanu tajnu pre glavne vrednosti $S - (\{S\}_{Bob})$
 - šifrovanu vrednost $E(h(msgs, CLNT, K), K)$ (šifrovana vrednost sadrži heš vrednost od svih razmenjenih poruka, klijentsku konstantu i simetrični ključ K)
4. U četvrtoj fazi protokola, Bob odgovara Alisi sa porukom sledećeg sadržaja:
 - heš vrednost $h(msgs, SERV, K)$, na osnovu koga Alisa verifikuje da je Bob primio sve poruke korektno, jer samo Bob može da dešifruje S i da dođe do simetričnog ključa K .

Posle četvrte faze protokola, Alisa i Bob su uspostavili *SSL* vezu, preko koje mogu komunicirati na bezbedan način. Za zaštitu tajnosti i integriteta koristiće simetrični ključ koji su razmenili u trenutku uspostave *SSL* protokola. Međutim, u stvarnosti je više od jednog ključa proisteklo iz heš vrednosti $h(S, R_A, R_B)$, tačnije šest ključeva je generisano iz navedene heš vrednosti.

- Dva ključa za šifrovanje, jedan za poruke poslate od klijenta ka serveru i drugi za poruke poslate od servera ka klijentu.
- Dva ključa za proveru integriteta, slično kao i prethodna dva, jedan za slanje drugi za prijem poruka.

- Dva inicijalizaciona vektora, opet za slanje i prijem poruka.

Na ovaj način koristimo različite ključeve po smerovima komunikacije. Ovaj metod upravljanja sa ključevima trebao bi da spreči određene vrste napada. Pažljivom analizom protokola sa slike (Slika 4.5), zaključićemo da je $h(msgs, CLNT, K)$ nepotrebno šifrovano, jer ne povećava bezbednost protokola. Ovaj slučaj možemo smatrati propustom, obzirom da je za to utrošeno neko vreme i računarski resursi.

4.2.2. BEZBEDNOST SSL PROTOKOLA

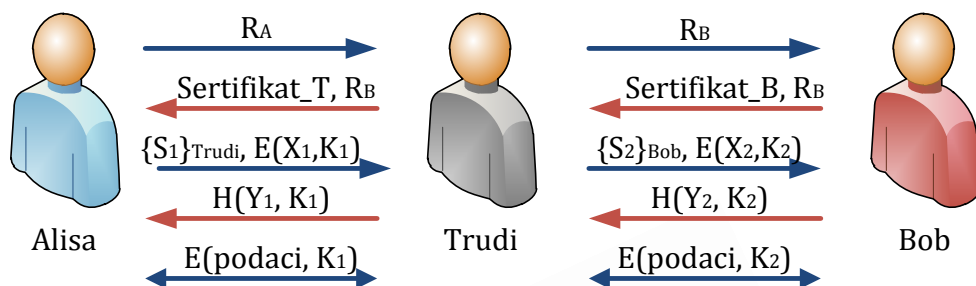
Zapažamo u razmatranju ovog protokola da Alisa autentifikuje Boba, ali ne i obrnuto (nema uzajamne autentifikacije). Na koji način je ovo urađeno? Bob je poslao Alisi u drugoj poruci svoj sertifikat na osnovu koga je Alisa autentifikovala Boba. Međutim, Bob (server) nije autentifikovao Alisu (klijent), ovo je već viđena situacija, posebno u elektronskoj trgovini. Ovaj nedostatak se uglavnom površno prevazilazi unošenjem korisničkog imena i lozinke na klijentskoj strani.

Pravo rešenje za postizanje uzajamne autentifikacije zahtevalo bi upotrebu Alisinog sertifikata, gde bi Bob u nekom trenutku uspostave veze zahtevao od Alise sertifikat, na ovaj način bi to bilo rešeno, a time bi bila obezbeđena uzajamna autentifikacija.

Zašto je uzajamna autentifikacija izostavljena u *SSL* protokolu, ostavićemo svakom čitaocu da pretpostavi na osnovu sledećih pitanja.

- Da li je *PKI* infrastruktura previše kompleksna?
- Da li je upravljanje sa sertifikatima na klijentskoj strani previše zahtevno?
- Da li se pružaoci Internet usluga plaše da ova dopuna može dovesti do smanjenja profita, smanjenjem obima Internet poslovanja iz više razloga?
- Da li je zahtevana dodatna procesorska snaga na klijentskoj/serverskoj strani zbog operacija sa javnim ključevima?
- Da li treća strana od poverenja (izdavači sertifikata) ne može da obezbedi kvalitetnu uslugu velikom broju korisnika (izdavanje, opoziv, reizdavanje, validacija itd)?
- Da li je uzajamna autentifikacija u suprotnosti sa nečijim interesima?

U nastavku, razmotrićemo sve mogućnosti za potencijalni napad „Čovek u sredini“. Jedna takav potencijalni napad prikazan je na slici (Slika 4.6).



Slika 4.6 SSL - „Čovek u sredini“

Da bi smo mogli da sprečimo ovu vrstu napada, neophodno je prvo da pretpostavimo da sertifikate izdaje treća strana od poverenja (*verisign, comodo* i td).

Razmotrimo sada potencijalne scenarije. U prvom scenariju napada, Trudi će poslati Alisi svoj sertifikat, Alisa će veoma lako da utvrdi da sertifikat nije Bobov i prekinuti SSL uspostavu veze.

U drugom scenariju, poslaće Bobov sertifikat Alisi, nakon čega će Alisa verifikovati Boba i u poslednjoj fazi šifrovati sa Bobovim javnim ključem, nakon čega Trudi ispada iz igre.

U trećem scenariju, generisaće Bobov lažni sertifikat, međutim standardna SSL veza ostvaruje su uz pomoć Internet pregledača i njihova uloga u tome je vrlo značajna. Zapravo, po prijemu sertifikata njihov zadatak je da provere njihovu validnost kod treće strane od poverenja. Citiramo sledeću poruku *Chrome* pregledača, nakon što utvrdi neispravnost sertifikata.

„Pokušali ste da kontaktirate www.Bob.rs, ali ste umesto toga kontaktirali server koji se identifikovao kao www.Trudi.rs. Ovo može da bude prouzrokovano pogrešnom konfiguracijom na serveru ili nečim još ozbiljnijim. Moguće je da napadač sa vaše mreže pokušava da vas namami da posetite lažnu (potencijalno štetnu) verziju domena www.Bob.rs. ne bi trebalo da nastavite naročito ako nikada ranije niste videli ovo upozorenje.“

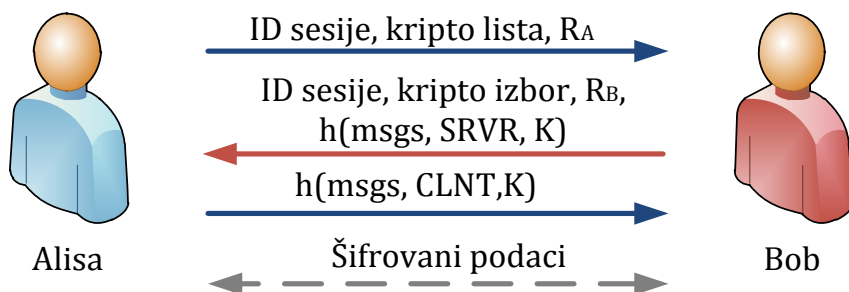
U ovom slučaju, adresa navedena u sertifikatu se ne podudara sa adresom *WEB* sajta na koju je pregledač pokušao da ode. Jedan od mogućih razloga za ovo je da poruke presreće napadač koji prikazuje sertifikat za drugi *WEB* sajt, što izaziva nepodudaranje. Još jedan od mogućih razloga je da je server podešen za vraćanje istog sertifikata za više *WEB* sajtova, uključujući onaj koji pokušavate da posetite, iako taj sertifikat nije važeći za sve te *WEB* sajtove. U ovom slučaju pretraživač ne može da tvrdi da ste posetili *www.trudi.rs*, ali ne može da potvrdi da je to isti sajt kao i *www.Bob.rs* koji ste nameravali da posetite.

U ovom momentu, ako korisnik ipak nastavi i tako ignoriše navedeno upozorenje, pretraživač više neće tražiti nepodudaranje naziva i neće preuzeti odgovornost za nastale posledice.

Pored svega navedenog, dodatno ćemo istaći još neke od bezbednosnih problema *SSL* protokola. Prvo, naveli smo da je *SSL* protokol dosta složeniji od pojednostavljene šeme preko koje smo razmatrali protokol. U realnom protokolu opciono postoji mogućnost za uvođenje kompresije. Uvođenje kompresije predstavlja skupu operaciju sa aspekta vremenskih performansi i procesorske snage. Kompresija podrazumeva kompresovanje svih poruka pre šifrovanja. Na žalost 99% implementacija *SSL* protokola isključuje mogućnost kompresije. Nedostatak kompresije predstavlja kritičnu tačku *SSL* protokola sa aspekta bezbednosti. Razlog za to su simetrični algoritmi za šifrovanje, koji na ulazu prihvataju fiksne blokove otvorenog teksta (64, 128, 192 ili 256 bitova). Otvoreni tekst se konvertuje preko *UTF8* standarda. Ova činjenica ukazuje na postojanje redundantnih podataka u otvorenom tekstu. Ne zaboravimo da kompresija otvorenog teksta povećava tačku jedinstvenosti. Kompresija zasnovana na entropijskom kodovanju, uklonila bi redundantne podatke i tako pojačala entropiju dobijenih šifrata. U drugom slučaju, Trudi bi mogla da sa velikom verovatnoćom pogodi do 50% bitova šifrovane poruke pod uslovom da je poruka sadržana od velikih i malih slova.

4.2.3. EFIKASNI METODI U *SSL* PROTOKOLU

U ovom odeljku govorićemo ukratko o efikasnom metodu kojeg koristi *SSL* za otvaranje novih konekcija na osnovu postojeće sesije (Slika 4.7) sa pretpostavkom da je prethodio protokol za uspostavu *SSL* konekcije.



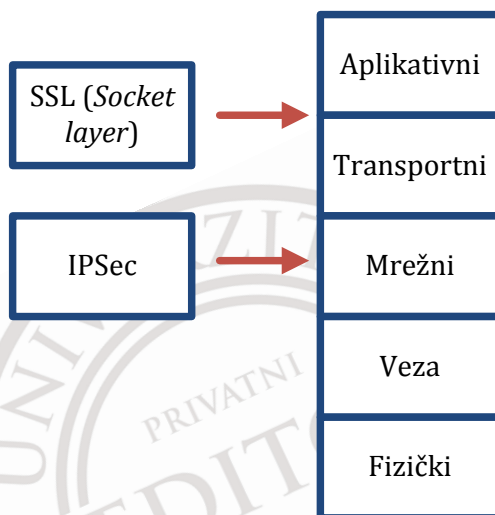
Slika 4.7 Protokol za nove SSL konekcije

Obzirom da je S vrednost već poznata Alisi i Bobu, dodatno je što obe strane moraju da pamte ID sesije, zatim računaju ključ za novu sesiju na osnovu $K = h(S, R_A, R_B)$. Iz priloženog vidimo da su izostavljene operacije *PKI*-a, a bezbednost metoda oslanja se na poznatu vrednost S .

Imajmo na umu da je *SSL* protokol u većini slučajeva implementiran u *WEB* pregledačima. Upravo je to razlog zbog čega je nastao i protokol za nove konekcije na osnovu postojeće sesije. Operacije sa javnim ključevima su dosta zahtevne i mogu izazvati određene probleme u radu, ako bi svaki put od početka koristili protokol za uspostavu *SSL* konekcije. Umesto toga, razvijen je poseban protokol za upravljanje novim konekcijama. Ideja je vrlo jednostavna, *SSL* inicijalizuje novu konekciju na osnovu već razmenjenog sesijskog ključa K . Sesijski ključ K će biti upotrebljen kao materijal za generisanje novog sesijskog ključa, umesto skupih operacija sa javnim ključevima. Na ovaj način su unapređene performanse protokola.

4.3. IPSEC

Na slici (Slika 4.8) je prikazana osnovna logička razlika između *SSL*-a i *IPSec*-a, *SSL* radi na *socket* sloju, dok *IPSec* radi na mrežnom sloju i tako predstavlja deo operativnog sistema.



Slika 4.8 *IPSec*

Međutim, *IPSec* je vrlo složen protokol, što se možda najbolje može dočarati ako kažemo da je preprojektovan protokol. Glavna prednost *IPSec*-a u poređenju sa *SSL*-om je da je u suštini transparentan za aplikacije, sa drug strane zahteva promene na operativnom sistemu. *IPSec* se najčešće koristi u *VPN* aplikacijama (engl. *Virtual Private Network*) koje obezbeđuju zaštićenu tunelovanu komunikaciju. Oba protokola, *SSL* i *IPSec* naišla su na otpor. *SSL* je naišao na otpor zbog potrebe prilagođavanja aplikacija, a *IPSec* zbog svoje složenosti i interoperabilnosti. Uglavnom, krajnji rezultat je da je Internet manje bezbedan nego što treba da bude!

IPSec poseduje mnogo sumnjivih i u suštini nepotrebnih funkcija, koje otežavaju njegovu implementaciju. Pored svoje složenosti, prisutni su i neki nedostaci, verovatno kao direktni rezultat njegove složenosti. U njemu postoje ozbiljni bezbednosni propusti, koji ga čine ranjivim. Pored toga, postoje i druga pitanja, kao

što je pitanje interoperabilnosti (složena dokumentacija), a to predstavlja ozbiljan problem, jer smanjuje mogućnosti da postane standard. Dodatni faktor koji komplikuje situaciju *IPSec*-a je dokumentacija, koja je podeljena u tri dela (*RFC* 2407, *RFC* 2408 i *RFC* 2409) i napisana od strane tri različita autora koja su koristila različitu terminologiju.

IPSec se sastoji od dva glavna dela:

1. *IKE* (engl. *Internet Key Exchange*) protokol obezbeđuje uzajamnu autentifikaciju i sesijske ključeve. *IKE* se sastoji od dve faze, slično kao i u *SSL* protokolu.
2. *ESP/AH* (engl. *Encapsulating Security Payload and Authentication Header*) predstavlja deo koji obezbeđuje šifrovanje i/ili zaštitu integriteta *IP* paketa, dok se *AH* koristi samo za obezbeđenje integriteta.

Tehnički gledano *IKE* je samostalni protokol koji bi mogao da opstane nezavisno od *ESP/AH* protokola. Međutim, pošto se primena *IKE* u realnom svetu jedino dovodi u vezu sa *IPSec*-om, oba glavna dela su zavedena pod nazivom *IPSec*. Komentar da je *IPSec* preprojektovan, prvenstveno se odnosi na *IKE* protokol.

Programeri *IKE* protokola, očigledno su mislili da stvaraju švajcarski nož bezbednosnih protokola, protokol koji će rešiti sve probleme autentifikacije. Ovo objašnjava zašto su ugradili mnoštvo opcija u vidu nepotrebnih funkcija ili funkcija koje nisu relevantne za *IPSec* protokol.

Prvo ćemo razmotriti *IKE*, zatim *ESP/AH*. *IKE* je dosta složeniji od ova dva. Sastoji se od dve faze, faza 1 i faza 2. Prva faza je dosta složenija od druge faze. Prva faza je osnovna faza ili *IKE SA* (*IKE* bezbednosna asocijacija) koja je uporediva sa *SSL* sesijom, dok je druga faza (*IPSec* bezbednosna asocijacija) ili *IPSec SA*, koja je uporediva sa *SSL* konekcijom.

Ne postoji očigledna potreba za dve faze u *IKE* protokolu. Zaključujemo na osnovu toga što nema višestrukih potreba za fazom 2 (u praksi ih nema), tada je skuplje imati dve faze. *SSL* protokol poseduje dve faze, ali kod *SSL* postoji evidentna potreba za tim kada je *HTTP* protokol korišćen. Ovo je prvi primer preprojektovanja u *IPSec*-u.

U prvoj fazi *IKE* protokola, postoje četiri različite opcije, kada je reč o ključevima.

- Javni ključ za šifrovanje (originalna verzija)
- Javni ključ za šifrovanje (poboljšana verzija)
- Digitalni potpis
- Simetrični ključ

Za svaku od ovih opcija, postoje dva različita režima rada, glavni i agresivni režim rada. Kao dokaz da je *IPSec* preopterećen funkcionalnostima, postoji 8 različitih verzija prve faze *IKE* protokola.

Možda se pitate zašto postoje javni ključ za šifrovanje i digitalni potpis kao opcije u prvoj fazi *IKE*. Odgovor na pitanje nije programersko preprojektovanje. Alisa uvek zna svoj privatni ključ, ali ona ne može da zna (inicijalno) Bobov javni ključ. Sa verzijom potpisa u prvoj fazi *IKE*, Alisa ne mora da ima Bobov javni ključ kod sebe za početak protokola. U svakom protokolu koji koristi kriptografiju javnog ključa, Alisi će biti potreban Bobov javni ključ da bi kompletirala protokol, ali u režimu potpisa, ona istovremeno može da započne protokol i da traži od Boba javni ključ. Nasuprot tome, u režimima šifrovanja sa javnim ključem, Alisi je potreban Bobov ključ odmah, zbog čega ona mora odložiti početak protokola, dok ne dobije Bobov javni ključ. Dakle, ovom opcijom nije ostvarena dobit na polju efikasnosti.

U nastavku razmotrićemo 6 od 8 verzija prve faze *IKE*.

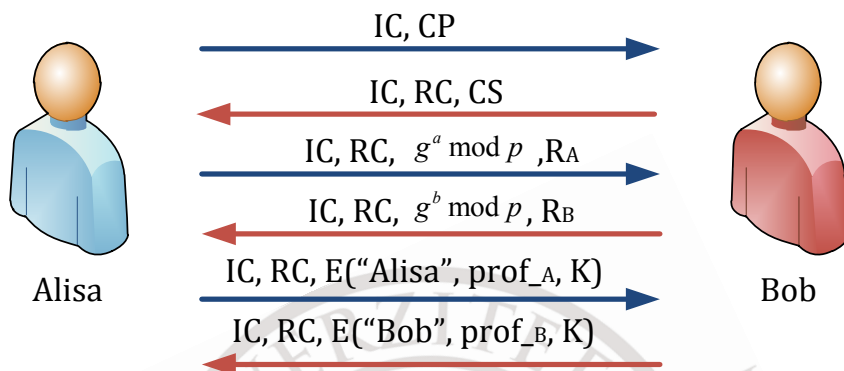
- Digitalni potpis (glavni i agresivni režim rada)
- Simetrični ključ (glavni i agresivni režim rada)
- Javni ključ za šifrovanje (glavni i agresivni režim rada)

Takođe, razmotrićemo originalnu verziju sa javnim ključem za šifrovanje, jer ova verzija je jednostavnija, iako manje efikasna od poboljšane verzije.

Svaka varijanta prve faze koristi efemerni *DH* protokol za razmenu ili uspostavu sesijskog ključa. Prednost ovog pristupa je u tome što pruža perfektnu tajnost u napred (*PFS*). U razmatranju ovih verzija prve faze, za *DH* protokol korišćićemo standardne notacije. Alisin tajni parametar a biće efemerni *DH* eksponent, Bobov tajni parametar b biće efemerni eksponent *DH* protokola, a p i g javni parametri.

4.3.1. IKE PRVA FAZA: DIGITALNI POTPIS

U prvoj fazi *IKE* protokola razmatraćemo verziju sa digitalnim potpisom u glavnom režimu rada. Ova verzija zahteva šest poruka, prikazanih na slici (Slika 4.9),



Slika 4.9 Digitalni potpis – glavni režim rada

gde je:

- CP – predloženi krypto parametri,
- CS – izabrani krypto parametri,
- IC – kolačić (engl. *cookie*) inicijatora,
- RC – kolačić odgovora,
- $K - h(IC, RC, g^{ab} \bmod p, R_A, R_B)$,
- $SKEYID - h(R_A, R_B, g^{ab} \bmod p)$,
- $dokaz_A = [h(SKEYID, g^a \bmod p, g^b \bmod p, IC, RC, CP, \text{"Alisa"})]_{Alisa}$,

h predstavlja *heš* funkciju i $dokaz_A$ je analogno $dokaz_B$.

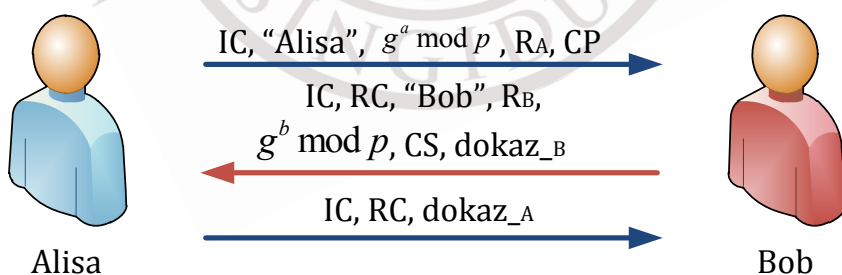
Pažljivo ćemo razmotriti svaku od ovih šest poruka sa slike (Slika 4.9).

1. U prvoj poruci, Alisa šalje informacije o krypto parametrima koje ona podržava, zajedno sa inicijalnim kolačićem;
2. U drugoj poruci, Bob bira na osnovu Alisinog predloga krypto parametre i šalje zajedno sa kolačićima, koji imaju ulogu kao identifikatori za ostale poruke u protokolu;

3. U treću poruku, Alisa uključuje parametar izazova R_A , DH parametre i kolačiće;
4. U četvrtoj poruci, Bob slično odgovara, uključuje svoj parametar izazova R_B , DH parametre i kolačiće;
5. U petoj i šestoj poruci, Alisa i Bob se međusobno autentifikuju koristeći digitalni potpis;

Podsetimo se da je napadač Trudi pasivan napadač, samo pod uslovom da može posmatrati poruke između Alise i Boba. Nasuprot tome, ako Trudi ima ulogu aktivnog napadača, ona takođe može umetnuti poruku, izbrisati, izmeniti i reprodukovati poruku. Protokol koji razmatramo obezbeđuje anonimnost, pod uslovom da je Trudi pasivni napadač. Ovo znači da Trudi posmatranjem poruka ne može razaznati Alisu i Boba. Međutim, ukoliko bi Trudi imala ulogu aktivnog napadača, verovatno bi situacija bila nešto drugačija.

Svaka opcija za ključeve u *IKE* protokolu ima glavni i agresivni režim rada. Osnovna uloga glavnog režima rada je da obezbedi anonimnost, dok to nije slučaj kod upotrebe agresivnog režima. U glavnom režimu rada cena anonimnosti je plaćena sa šest poruka, dok u agresivnom režimu postoje samo tri poruke. Agresivni režim rada digitalnog potpisa, prikazan je na slici (Slika 4.10). Možemo da vidimo da ne postoji pokušaj da se sakrije Alisin i Bobov identitet, koji značajno pojednostavljuje protokol. Oznake koje koristimo u ovoj verziji protokola su identične kao i na prethodnoj slici.



Slika 4.10 Digitalni potpis – agresivni režim rada

Glavna razlika između glavnog i agresivnog režima rada sa digitalnim potpisom je u anonimnosti i razmeni DH parametara g i p . Za razliku od glavnog režima, u agresivnom režimu anonimnost nije obezbeđena, tačnije, identitet nije zaštićen. U

agresivnom režimu nije moguće dogovarati DH parametre g i p kroz CS i CP , već se te vrednosti fiksiraju i šalju u prvoj poruci.

Prema *RFC* preporukama, glavni režim „mora“ biti implementiran, dok agresivni režim „treba“ da bude implementiran. Drugim rečima, ako agresivni režim nije implementiran „treba sa se osećate krivim zbog toga“- kako to tumače autori *RFC*-a. Sve ovo može otvoriti pitanje interoperabilnosti o kom smo govorili na početku.

Pretpostavlja se da kolačići (engl. *Cookies*) otežavaju i smanjuju mogućnost za *DoS* napade. *IKE* kolačići nisu u vezi sa *WEB* kolačićima. U *IKE* protokolu, u glavnom režimu bez obzira na postojećih osam verzija, Bob (Bob mora čuvati sva stanja poruka, od prve poruke pa na dalje – *IC* i *RC*). Međutim, ovi kolačići nude malu zaštitu od *DoS* napada.

Na kraju zaključujemo da u opciji ključa u prvoj fazi sa digitalnim potpisom, pasivni napadač može da zna identitet Alise i Boba u agresivnom modu, dok aktivni napadač može odrediti identitet Alise i Boba u glavnom režimu.

4.3.2. IKE PRVA FAZA: SIMETRIČNI KLJUČ

U sledećoj verziji prve faze *IKE* protokola, razmatraćemo o opciji – simetrični ključ sa glavnim i agresivnim režimom rada. Kao i kod prethodne verzije, glavni režim se sastoji od šest poruka, gde je format formalno isti kao na slici (Slika 4.9), osim što se notacije tumače drugačije.

K_{AB} – simetrični ključ distribuiran unapred,

$$K = h(IC, RC, g^{ab} \bmod p, R_A, R_B, K_{AB}),$$

$$SKEYID = h(K, g^{ab} \bmod p),$$

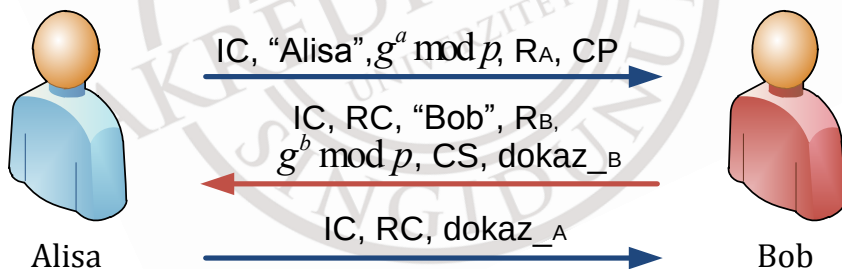
$$dokaz_A = h(SKEYID, g^a \bmod p, g^b \bmod p, IC, RC, CP, Alisa).$$

Opet ćemo navesti prednost glavnog režima u odnosu na agresivni, iz razloga što glavni režim obezbeđuje anonimnost.

Nailazimo odmah na probleme sa simetričnim ključem u ovoj verziji prve faze *IKE*. Pojasnićemo, Alisa u petoj poruci šalje svoj identitet šifrovan sa ključem K , ali Bob mora da koristi ključa K_{AB} da bi odredio ključ K . Dakle, imamo slučaj u kome Bob mora da zna ključ K_{AB} , pre nego što sazna sa kim razgovara. Pretpostavimo da Bob paralelno razgovara sa više korisnika, i da Alisa nije jedina osoba koja razgovara sa Bobom. Na koji način Bob može da zna koji ključ K_{AB} da koristi, ako to ne može da sazna na osnovu informacija iz protokola?

Programeri *IPSec*-a su prepoznali ovaj potencijalni problem. Njihovo rešenje je da se Bob osloni na *IP* adresu i tako odredi koji ključ K_{AB} da koristi. Dakle, Bob mora da koristi *IP* adresu sa dolaznih paketa, da bi znao sa kim razgovara. Na ovaj način, Alisin identitet je njena *IP* adresa.

Postoji nekoliko problema sa ovim pristupom. Prvo, Alisa mora posedovati statičku *IP* adresu, ali šta ukoliko je promeni. Pre svega, ovaj protokol sa šest poruka je veoma složen, a pri tome ne uspeva da sakrije identitet, osim ako statička *IP* adresa bude tajna. Sve ovo u glavnom režimu u verziji sa simetričnim ključevima izgleda besmisleno, umesto da se koristi jednostavniji i značajno efikasniji agresivni režim rada, koji opisujemo u nastavku odeljka.



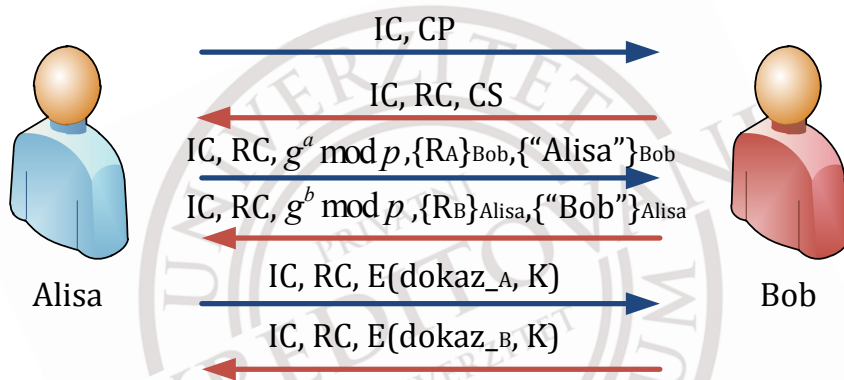
Slika 4.11 Simetrični ključ – agresivni režim rada

Agresivni režim rada sa simetričnim ključem (Slika 4.11) u *IPSec*-u sledi isti format kao i digitalni potpis u agresivnom režimu na slici (Slika 4.10). Kao i kod verzije digitalnog potpisa, glavna razlika od glavnog režima je da agresivni režim ne pokušava da sakrije identitet (ne želi da krije). Pošto simetrični ključ u glavnoj verziji ne uspeva da sakrije identitet, problem nedostatka anonimnosti u agresivnom režimu više nije ozbiljno ograničenje.

4.3.3. IKE PRVA FAZA: JAVNI KLJUČ ZA ŠIFROVANJE

U sledećoj verziji prve faze *IKE* protokola, razmatraćemo o opciji – javni ključ za šifrovanje sa glavnim i agresivnim režimom rada. Do sada smo videli verziju sa digitalnim potpisom. U glavnom modu za šifrovanje Alisa mora znati Bobov javni ključ unapred i obrnuto. Svakako, bilo bi logično da razmene sertifikate, ali to će otkriti identitet Alise i Boba. Ovo bi oduzelo jednu jedinu prednost glavnog moda sa šest poruka. U ovoj verziji postoji pretpostavka da Alisa i Bob imaju siguran način za pristup sertifikatu druge strane, bez slanja preko mreže.

Javni ključ za šifrovanje u glavnom režimu prikazan je na slici (Slika 4.12),



Slika 4.12 Javni ključ za šifrovanje – glavni režim rada

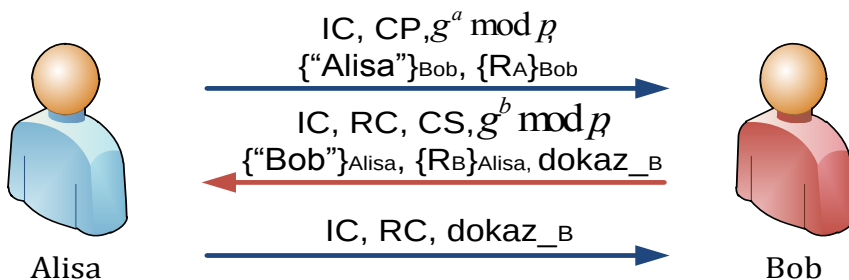
gde je notacija, kao i u prethodnim režimima, osim:

$$K = h(IC, RC, g^{ab} \bmod p, R_A, R_B),$$

$$SKEYID = h(R_A, R_B, g^{ab} \bmod p),$$

$$dokaz_A = h(SKEYID, g^a \bmod p, g^a \bmod p, IC, RC, CP, “Alisa”).$$

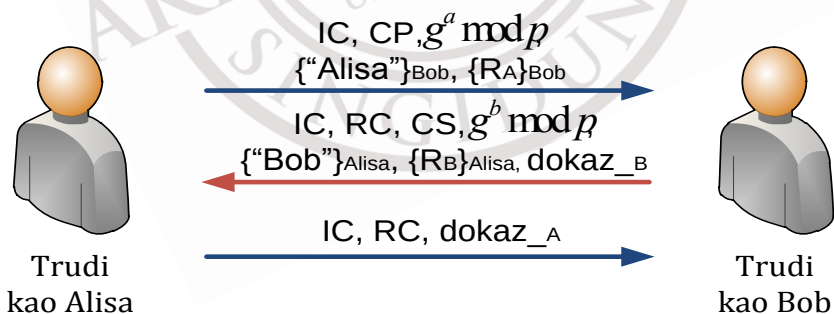
Primitićemo na slici (Slika 4.13), da je notacija kod agresivnog režima za šifrovanje sa javnim ključem dosta slična notaciji u glavnom režimu. Zanimljivo je, za razliku od drugih agresivnih režima, javni ključ za šifrovanje u agresivnom režimu omogućava Alisi i Bobu da ostanu anonimni. Imajući na umu ovaj slučaj, pitamo se, imali agresivni režim neku prednost u odnosu na glavni režim?



Slika 4.13 Javni ključ za šifrovanje – agresivni režim rada

Zbog sigurnosti, u nastavku razmotrićemo agresivni režim sa javnim ključem za šifrovanje. Pretpostavimo da trudi generiše DH eksponente a, b i parametre iza-zova R_A i R_B . Tada Trudi uspeva da izračuna sve preostale vrednosti koje se po-javljaju u protokolu $(K, \text{SKEYID}, \text{dokaz}_A, \text{dokaz}_B \text{ i } g^{ab} \bmod p)$ na slici (Slika 4.13). Razlog zbog kojeg Trudi uspeva ovo da uradi je zbog toga što je Alisin i Bobov javni ključ javan. Ovaj scenario napada važi i za glavni režim šifrovanja sa javnim ključem.

Na ovaj način Trudi može generisati poruke u razmeni koja izgleda kao da je va-žeća $IPSec$ komunikacija između Alise i Boba. Scenario napada čini se da važi za jednog posmatrača, uključujući Alisu i/ili Boba (Slika 4.14).



Slika 4.14 Trudi napada agresivni režim – šifrovanje sa javnim ključem

Činjenica da Trudi može da stvori lažni razgovor (lažnu konverzaciju) koji izgleda kao da je između Alise i Boba, predstavlja ozbiljan bezbednosni propust. Interes-antno je primetiti da se u ovom režimu bezbednosna funkcija može nazvati ime-

nom uverljive porecivosti. Protokol koji sadrži funkciju uverljive porecivosti (moguće odbijanje), omogućava Alisi i Bobu da poriču da se razgovor ikada dogodio, jer Trudi je mogla lažirati bilo koji razgovor. U nekim situacijama to može biti poželjna osobina, ali sa druge strane u nekim situacijama može predstavljati neki tip ranjivosti. Na primer, ako Alisa kupi nešto od Boba, ona može kasnije to poreći sve dok digitalno ne potpiše.

Bez obzira kojih od osam verzija se koristi u prvoj fazi *IKE* protokola, uspešan završetak ove faze rezultira sa:

- Uzajamnom autentifikacijom,
- Deljeni simetrični ključ,
- *IKE SA* (engl. *Security Association*);

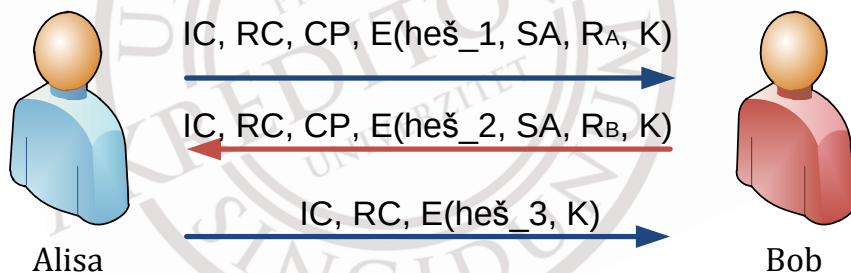
Prva faza u *IKE* protokolu je računarski skupa, posebno u slučaju korišćenja javnih ključeva, a glavni režimi zahtevaju šest razmenjenih poruka preko mreže. Programeri *IKE* protokola su pretpostavljali da će se *IKE* koristiti za mnoge druge stvari, a ne samo u *IPSec*-u, što predstavlja razumno objašnjenje za prekomerni broj funkcionalnosti u *IKE* protokolu, ali na njihovu žalost u praksi se ne koristi. Druga faza je značajno jeftinija i ona se realizuje nakon *IKE SA* (prve faze). Druga faza je specifična, jer je zahtevana za svaku različitu aplikaciju koja će koristiti *IKE-SA*.

Druga faza *IKE* protokola koristi se za uspostavljanje tzv. *IPSec-SA* (*IPSec* bezbedna asocijacija). U poređenju sa *SSL* protokolom, prva faza *IKE* protokola uporediva je sa *SSL* sesijom, dok je druga faza uporediva sa *SSL* konekcijom. Na ovaj način dizajneri i programeri *IKE* protokola su hteli da budu fleksibilniji, jer su pretpostavljali da će se protokol koristiti i za mnoge druge stvari, ali osim kod *IPSeca* u praksi se to nije dogodilo.

4.3.4. IKE DRUGA FAZA

Druga faza *IKE* protokola je dosta jednostavnija u poređenju sa drugom fazom. Pre započinjanja druge faze, neophodno je da bude kompletirana prva faza, u kojoj su: sesijski ključ K , *IPSec* kolačići (IC i RC) i *IKE-SA* poznati Alisi i Bobu. Ceo slučaj *IKE* protokola za drugu fazu, prikazan je na slici (Slika 4.15), gde važi:

- Predlog CP (engl. *Crypto proposal*) uključuje ESP ili AH . Tačnije, tada Alisa i Bob odlučuju da li će koristiti ESP ili AH .
- SA je identifikator za *IKE-SA* koji je uspostavljen u prvoj fazi.
- Numeracija heš vrednosti zavisice od $SKEYID$, R_A , R_B i *IKE-SA* iz prve faze.
- Ključevi koji su izvedeni $KEYMAT = h(SKEYID, R_A, R_B, "junk")$, smeće (engl. *junk*) je poznato svima uključujući i Trudi.
- Vrednost $SKEYID$ zavisi od metoda u prvoj fazi *IKE* protokola.
- Opciono, PFS može da bude implementiran koristeći efemerni DH protokol za razmenu ključa.



Slika 4.15 *IKE* druga faza

Vrednosti R_A i R_B sa slike (Slika 4.15) nisu isti kao oni sa iz prve faze *IKE* protokola. Kao rezultat, ključevi generisani u drugoj fazi su različiti od ključeva generisanih u prvoj fazi.

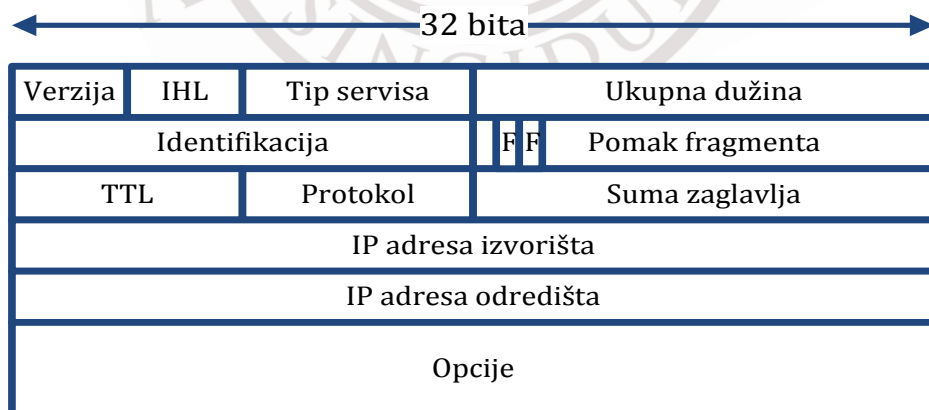
Nakon završetka prve faze *IKE* protokola, uspostavljen je *IKE-SA*, a nakon završetka druge faze *IKE* protokola, uspostavljen je *IPSec-SA*. Posle druge faze Alisa i Bob su autentifikovani, dele zajednički sesijski ključ za upotrebu u trenutnoj sesiji.

Podsetimo se da je u slučaju *SSL* protokola, nakon obavljene uzajamne autentifikacije i razmenjenog ključa sesije, protokol spreman za rad (razmenu šifrovanih podataka). *SSL* protokol radi sa podacima na aplikativnom sloju, tada je šifrovanje i zaštita integriteta urađena na standardan način. Kod *SSL* protokola, mrežni sloj je transparentan za Alisu i Boba, jer je *SSL* protokol smešten u jednom delu aplikativnog sloja (jedan deo aplikacije). Ova činjenica predstavlja prednost u radu sa podacima aplikativnog sloja.

Zaštita podataka u *IPSec*-u nije toliko jednostavna. Pod pretpostavkom da je u *IPSec*-u uspela autentifikacija i razmena sesijskog ključa, ostaje problem da se zaštite podaci u *IP* datogramima. Pre nego što nastavimo da se bavimo ovim problemom, treba da razmotrimo *IP* datagrame iz perspektive *IPSec*-a.

4.3.5. IP DATAGRAMI U IPSEC PROTOKOLU

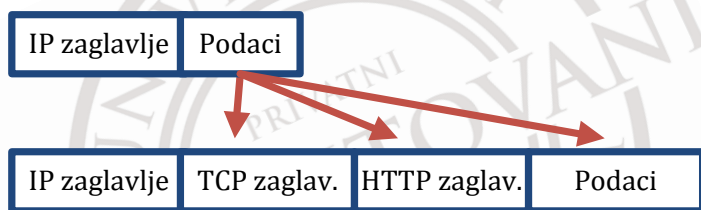
IP datagram se sastoji od zaglavlja i podataka. *IP* zaglavlje je ilustrovano na slici (Slika 4.16). Ukoliko je polje „opcije“ prazno (kao što je to obično), tada *IP* zaglavlje se sastoji od 20 bajtova. Za potrebe *IPSec*-a, jedna bitna stvar je da ruteri imaju pristup *IP* adresi odredišta u *IP* zaglavlju, da bi mogli da rutiraju pakete. Ostala polja *hedera* se takođe koriste u svrhu rutiranja paketa. Imajući u vidu da ruteri nemaju pristup sesijskom ključu, time ne postoji mogućnost za šifrovanje paketa.



Slika 4.16 *IP* zaglavlje

Druga bitna stvar je vezana za prosleđivanje paketa. Prosleđivanje paketa će izazvati promenu vrednosti nekih polja u *IP* zaglavlju. Na primer, *TTL* (engl. *Time-to-live*) polje predstavlja vrednost koja se umanjuje na svakom ruteru. Obzirom da ključ sesije nije poznat, integritet nijednog polja zaglavlja ne može da bude zaštićen. U diskusiji koja se odnosi na *IPSec*, polja zaglavlja koja se menjaju u prenosu nazivaju se promenljivim poljima.

Dalje, razmatramo sadržaj *IP* datagrama. Uzećemo za primer sesiju u toku *WEB* pregledanja. Aplikativni sloj protokola za ovu vrstu saobraćaja je *HTTP*, a transportni sloj je *TCP*. U ovom slučaju, *IP* enkapsulira *TCP* paket, koji enkapsulira *HTTP* paket, koji je prikazan na slici (Slika 4.17). Poenta je da iz perspektive *IP*-a, podaci uključuju više od aplikativnog sloja podataka. Konkretno u ovom primeru, podaci uključuju *TCP* i *HTTP* zaglavlje, kao i podatke aplikativnog sloja. Videćemo zašto je to relevantan ishod.



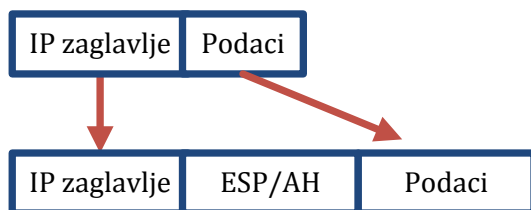
Slika 4.17 *IP* datagram

Kao što je ranije pomenuto, *IPSec* koristi *ESP* ili *AH* za zaštitu *IP* datagrama. Jedan od ova dva metoda će biti izabran za zaštitu *IP* datagrama (*ESP* zaglavlje ili *AH* zaglavlje). Izabrani tipovi zaglavlja govoriće primaocu da primljeni paket tretira kao *ESP* ili *AH* paket, ne kao standardni *IP* datagram.

4.3.6. TRANSPORT I REŽIMI TUNELOVANJA

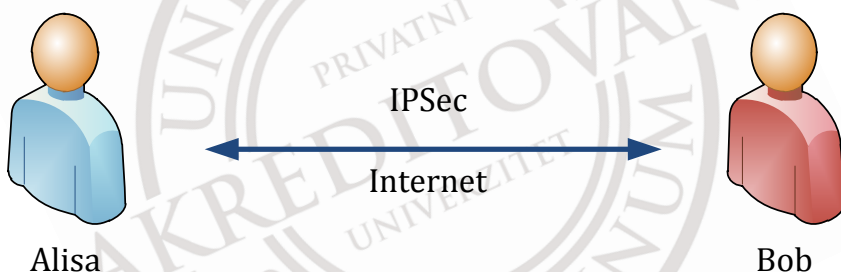
Ne zavisno od toga koji je metod izabran za upotrebu, *ESP* ili *AH*, *IPSec* je aktivirao transportni režim i režim tunelovanja. U transportnom režimu, kao što je prikazano na slici (Slika 4.18), novi tip zaglavlja - *ESP/AH*, nalazi se u sendviču između *IP* zaglavlja i podataka. Transportni režim je dosta efikasniji, iz razloga što dodaje manju količinu dodatnih informacija u zaglavlje. Bitna stvar je da u transportnom režimu, originalno *IP* zaglavlje ostaje netaknuto. Loša strana tran-

sportnog režima je što pasivni napadač može videti zaglavlje. Međutim, ako Trudi primeti da je *IPSec*-om zaštićen razgovor između Alise i Boba, u transportnom režimu na osnovu zaglavlja Trudi će otkriti da Alisa i Bob komuniciraju.



Slika 4.18 *IPSec* – transportni režim

Transportni režim je dizajniran prvenstveno za „*host-to-host*“ komunikaciju, to znači da Alisa i Bob razgovaraju direktno jedno sa drugim, koristeći *IPSec* (Slika 4.19).



Slika 4.19 *IPSec* – „*host-to-host*“

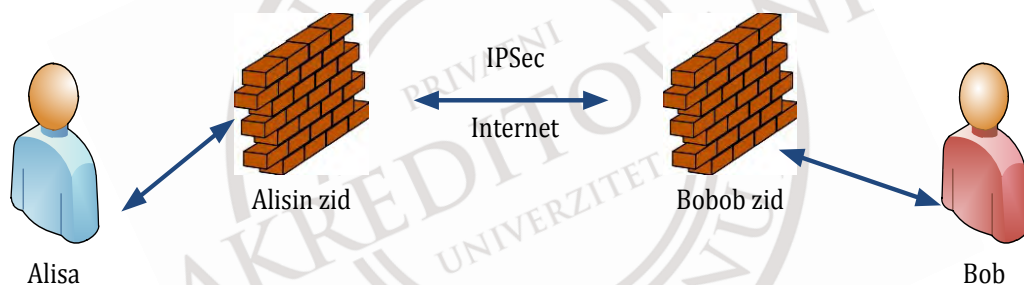
U režimu tunelovanja (Slika 4.20), ceo *IP* paket je enkapsuliran u novi *IP* paket. Jedina prednost ovog pristupa je da *IP* zaglavlje više nije vidljivo za napadača pod pretpostavkom da je šifrovano. Međutim, ako Alisa i Bob direktno komuniciraju, novo *IP* zaglavlje će biti isto kao enkapsulirano *IP* zaglavlje, iz tog razloga kriti originalno zaglavlje bilo bi besmisleno. *IPSec* je često korišćen za komunikaciju „*firewall-to-firewall*“. U ovom slučaju Alisin i Bobov zaštitni zid (engl. *Firewall*) komuniciraju preko *IPSec*-a, na ovaj način je izbegnuta direktna komunikacija između Alise i Boba. Ako pretpostavimo da Alisa i Bob komuniciraju preko svojih zaštitnih zidova koristeći režim tunelovanja, novo *IP* zaglavlje će otkriti da je paket poslat između Alisinog i Bobovog zaštitnog zida. Tačnije, ako je paket šifrovan

Trudi bi mogla da zna da Alisin i Bobov zaštitni zid komuniciraju, ali ona ne može da zna koji se nalazi iza *host*-a.



Slika 4.20 IPsec režim tunelovanja

Režim tunelovanja prvenstveno je dizajniran za komunikaciju „*firewall-to-firewall*“, na ovaj način sprečena je Trudi da sazna koji *host*-ovi komuniciraju.



Slika 4.21 Režim tunelovanja – „*firewall-to-firewall*“

Tehnički, transportni režim nije neophodan, jer smo mogli enkapsulirati originalni *IP* paket u novi *IPsec* paket. Čak i u komunikaciji „*host-to host*“. Za zaštitu saobraćaja u komunikaciju „*firewall-to-firewall*“, neophodno je koristiti režim tunelovanja, jer je bitno da se sačuva originalno *IP* zaglavlje, tako da zaštitni zid na određitu može dalje rutirati pakete do *host* odredišta. Na kraju zaključujemo da je transportni režim efikasniji, što ga čini boljom opcijom u komunikaciji „*host-to-host*“.

4.3.7. ESP I AH

Nakon što smo odlučili da li da koristimo transportni režim ili režim tunelovanja, tada dodatno moramo razmotriti i tip zaštite koji ćemo da koristimo za zaštitu *IP* datagrama. Izbori su poverljivost, integritet ili oba. Takođe, trebamo uzeti u obzir i zaštitu koju ćemo primeniti nad zaglavljem. U *IPSec*-u, jedini izbori su *ESP* ili *AH*. U nastavku ćemo razmotriti, koje tipove zaštite svaki od njih pruža?

AH (engl. *Authentication Header*) obezbeđuje samo integritet, ali ne i šifrovanje. *AH* zaštita integriteta odnosi se na sve iznad *IP* zaglavlja i na neka polja u njemu. Kao što smo malopre rekli, nije moguće štititi integritet svih polja u *IP* zaglavlju, iz razloga što su neka polja promenljiva (primer sa *TTL*-om).

ESP (engl. *Encapsulating Security Payload*) obezbeđuje integritet i poverljivost. Oba tipa zaštite su primenjena na sve izvan *IP* zaglavlja, to jest, na podatke iz perspektive *IP*-a. Nema zaštitu koja se primenjuje na *IP* zaglavlje.

Šifrovanje je potrebno u *ESP*-u. Međutim, postoji trik preko kojeg *ESP* može da se iskoristi samo za integritet. U *ESP*-u, Alisa i Bob pregovaraju za krypto algoritam koji će koristiti. Još jedna šifra mora da bud podržana, a to je šifra *NULL*, opisana u *RFC*-u 2410.

Ovde su nabrojani neki neobični izvodi iz *RFC*-a koji se odnose na šifru *NULL*.

- Šifra *NULL* je blokovska šifra, čije se poreklo gubi u antičkom vremenu,
- Ne postoje dokazi da je *NSA* inicirala objavljivanje ovog algoritma,
- Dokazi ukazuju da je razvijen u rimsko doba, kao izvozna verzija Cezarove šifre,
- Algoritam omogućava upotrebu ključeva različite dužine,
- Nije potreban *IV* (inicijalni vektor),
- Metod šifrovanja je definisan kao $NULL(P, K) = P$, za bilo koji otvoreni tekst *P* i bilo koji ključ *K*.

U *ESP*-u, ako je *NULL* šifra izabrana, tada se šifrovanje ne primenjuje, ali integritet podataka je zaštićen. Ovaj slučaj izgleda sumnjivo, slično kao i sa *AH*.

Pokušaćemo da odgovorimo na pitanje, zašto *AH* postoji?

Postoje tri razloga koja opravdavaju postojanje *AH*-a. Kao što je prethodno navedeno, *IP* zaglavlje ne može da bude šifrovano, već ruteri moraju da imaju pristup zaglavlju paketa. Međutim, *AH* pruža nešto veću zaštitu integriteta, nego *ESP* sa *NULL* šifrom.

Drugi razlog postojanja *AH* je što *ESP* šifruje sve izvan *IP* zaglavlja, pod uslovom da je izabrana šifra *nonNULL*. Ako je *ESP* korišćeno za šifrovanje paketa, zaštitni zid ne može da pristupi unutrašnjosti paketa. Možda iznenađujuće, *ESP* sa *NULL* šifrovanjem ne rešava ovaj problem, *ESP* ne štiti *IP* zaglavlje uopšte. Kada zaštitni zid detektuje *ESP* zaglavlje, tada će znati da se koristi *ESP*. Međutim, zaglavlje neće otkriti informaciju zaštitnom zidu da je korišćeno *NULL* šifrovanje, to je Ali-sin i Bobov dogovor koji nije uključen u zaglavlje. Dakle, kada zaštitni zid otkrije da je korišćen *ESP*, to ne znači da će otkriti da li je *TCP* zaglavlje šifrovano ili nije. Nasuprot tome, kada zaštitni zid otkrije da je korišćen *AH*, tada će odmah znati da ništa nije šifrovano.

Nijedan od navedenih razloga nije dovoljno dobar da opravda postojanje *AH*. Dizajneri *AH/ESP* mogli su napraviti neke manje modifikacije na protokolu i da tako prevaziđu ove nedostatke kod *ESP*-a. Sa druge strane, postoji uverljiv dokaz za postojanje *AH*. Na jednom sastanku gde je *IPSec* standard razvijen „neko iz Mikrosofta je održao strastven govor o tome kako je *AH* bio beskoristan“ i „svi prisutni su gledali oko sebe i rekli. On je u pravu i mi mrzimo *AH*. Ali ako on nervira Mikrosoft neka ostane, pošto mi mrzimo više Mikrosoft nego *AH*“. Dakle, sada možete i sami da pretpostavite ostatak priče.

Još jednom ćemo dati osnovne razlike između *AH* i *ESP*. *AH* obezbeđuje zaštitu integriteta, ne i poverljivost. Zaštita integriteta na sve izvan *IP* zaglavlja i na neka polja zaglavlja koja nisu promenljiva. *ESP* obezbeđuje integritet i poverljivost. Štiti sve izvan *IP* zaglavlja. Zaštita integriteta je obezbeđena upotrebom samo *NULL* šifre.

4.4. KERBEROS

U Grčkoj mitologiji, *Kerberos* je troglavi pas koji čuva ulaz u Had. U svetu informacione bezbednosti *Kerberos* je autentifikacioni protokol koji je zasnovan na simetričnom ključu i vremenskom pečatu. Nastao je na MIT-u (*Massachusetts Institute of Technology*), na radu Needham-a i Schroeder-a. *SSL* i *IPSec* protokoli su dizajnirani za korišćenje na Internetu, dok je *Kerberos* dizajniran za korišćenje u malom radnom okruženju, kao što je lokalna mreža *LAN* u okviru neke kompanije.

Pretpostavimo da imamo N korisnika u mreži, gde svaki par mora međusobno da se autentifikuje, jedno pred drugim. Ako bi se *Kerberos* protokol zasnivao na javnom ključu, svaki korisnik bi morao da poseduje par javnihi/privatnih ključeva, samim tim, bilo bi potrebno N parova ključa. Sa druge strane, ako *Kerberos* protokol obezbeđuje servis autentifikacije sa simetričnim ključevima, tada za N korisnika je potrebno oko N^2 ključeva i svi korisnici moraju unapred međusobno podeliti ključeve. Na osnovu ove činjenice, autentifikacija sa korišćenjem simetričnih ključeva u *Kerberos* protokolu neće biti razmatrana. Međutim, *Kerberos* protokol se zasniva na trećoj strani od poverenja (engl. *Trusted Third Party*), na ovaj način je zahtevano samo N simetričnih ključeva za N korisnika. Umesto međusobne podele simetričnih ključeva između svih korisnika protokola, svaki korisnik deli jedan ključ sa *KDC*-om. To znači da Alisa deli ključ K_A sa *KDC*-om, Bob deli ključ K_B sa *KDC*-om itd. *KDC* (engl. *Key Distribution Center*) ima ulogu posrednika između bilo koja dva korisnika, zapravo njegova uloga je da obezbedi bezbednu komunikaciju između korisnika, korišćenjem *Kerberos* simetričnog ključa.

Kerberos TTP je kritična bezbednosna komponenta u protokolu, od koje zavisi ukupna bezbednost sistema i iz tog razloga mora biti zaštićena od napada. Ovo je svakako bezbednosni problem, ali za razliku od *PKI* infrastrukture, nijedan javni ključ nije zahtevan. U suštini, *Kerberos TTP* igra sličnu ulogu kao vrhovni *CA* u *PKI* infrastrukturi. *Kerberos* je kao i *TTP*, centar za distribuciju ključeva, što znači da je ceo sistem ugrožen ako je on nezaštićen. Kao što smo već gore naveli, *KDC* deli simetrični ključ K_A sa Alisom i simetrični ključ K_B sa Bobom i td..

KDC Kerberos protokola poseduje glavni ključ K_{KDC} , koji je uglavnom poznat samo kao *KDC*. Iako ovo može da zvuči nelogično, da jedino *KDC* zna vrednost ključa

K_{KDC} , ali videćemo da ovaj ključ igra veoma važnu ulogu u *Kerberos* protokolu. Važna bezbednosna karakteristika *Kerberos* protokola je što ključ K_{KDC} omogućava *KDC*-u da ostane nepoznat. Na ovaj način je onemogućen *DoS* napad.

Kerberos se koristi za autentifikaciju i uspostavu sesijskog ključa, a koji se naknadno mogu koristiti za obezbeđenje poverljivosti i integriteta. To znači da je svaki simetrični kriptografski algoritam moguće koristiti sa *Kerberos*-om. Međutim, u praksi je čest slučaj da se koristi *DES* (engl. *Data Encryption Standard*).

U radu *Kerberos* kao protokol izdaje različite vrste tiketa. Razumevanje ovih tiketa je od ključnog značaja za razumevanje *Kerberos*-a. Tiket ili ulaznica (karta), sadrži ključeve i druge informacije koje su potrebne za pristup mrežnim resursima. Dalje u nastavku ćemo koristiti reč tiket kao sinonim za kartu ili propusnicu. *KDC* svakom korisniku izdaje jedan poseban tiket *TGT* (engl. *ticket-granting ticket*). *TGT* je generisan i izdat u inicijalnoj fazi, kada se korisnik sistema prvi put prijavio na sistem sa svojim pristupnim parametrima. Kasnije, *TGT* kao glavni tiket se koristi za izdavanje običnih tiketa, koji omogućavaju pristupe pojedinačnim mrežnim resursima. Na primer, pretpostavimo da Alisa želi da pristupi mrežnom štampaču i da joj je za to potrebno odobrenje, ali nije stvar samo u odobrenju, Alisa želi šifrovanu komunikaciju sa štampačem. U ovom slučaju *KDC* će odigrati važnu ulogu, tako što će podeliti identičan simetričan ključ, između Alise i štampača.

Svaki *TGT* sadrži ključ sesije, *ID* korisnika kom je izdat *TGT* i vreme trajanja. Zbog jednostavnosti zanemarimo vremenski pečat, ali bitno je napomenuti da *TGT* ne traju večno. Svaki *TGT* je šifrovan ključem K_{KDC} . Ne zaboravite da samo *KDC* zna ključ K_{KDC} . Kao rezultat tome, *TGT* može biti čitljiv samo *KDC*-u.

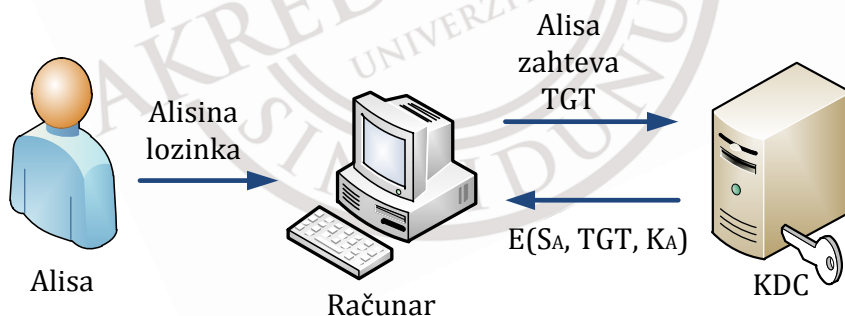
Postoji određen razlog, zašto *KDC* šifrue *TGT* sa ključem koji je poznat samo njemu? Druga alternativa *KDC*-a, bila bi da postoji baza podataka sa svim prijavljenim korisnicima i njihovim sesijskim ključevima, što nije dovoljno dobro rešenje. *KDC* šifrovanjem *TGT*-a pruža jednostavan, efektivan i bezbedan način za distribuciju ključeva. Na primer, Alisa pošalje svoj *TGT* *KDC*-u, tada *KDC* dešifrue *TGT* i tako dobije sve potrebne informacije o Alisi. U nastavku ćemo malo bolje objasniti upotrebu *TGT*-a, jer *TGT* predstavlja izuzetno pametan dizajn *Kerberos*-a.

4.4.1. KERBEROS INICIJALIZACIJA

Za razumevanje *Kerberos* protokola, neophodno je prvo razmotriti rad sistema za prijavljivanje na sistem u kom je implementiran *Kerberos* protokol, tačnije, proći ćemo kroz sve korake, kroz koje prolazi Alisa kada se prijavljuje na sistem u kome se *Kerberos* koristi za autentifikaciju. Slično kao i u većini sistema, Alisa unosi korisničko ime i lozinku. U *Kerberos*-u, Alisin računar obavlja derivaciju ključa K_A iz lozinke (upotrebom neke heš funkcije), a ključ K_A je ključ koji Alisa unapred deli sa *KDC*-om. Na osnovu ključa K_A Alisa dobija glavni tiket (*TGT*) od *KDC*-a. Alisa zatim može da koristi svoj *TGT* za bezbedan pristup mrežnim resursima.

Prijava na *Kerberos* je prikazan na slici (Slika 4.22), a koristili smo sledeću notaciju za razumevanje ove faze protokola.

- Ključ K_A je generisan na osnovu Alisine lozinke kao heš vrednost $K_A = h(\text{Alizina lozinka})$,
- S_A je sesijski ključ koji kreira *KDC*,
- Alisin računar koristi K_A za dobijanje S_A i *TGT*-a. Nakon čega zaboravlja K_A ,
- *TGT* je vrednost $TGT = E(„Alisa“, S_A; K_{KDC})$.



Slika 4.22 Prijava na *Kerberos*

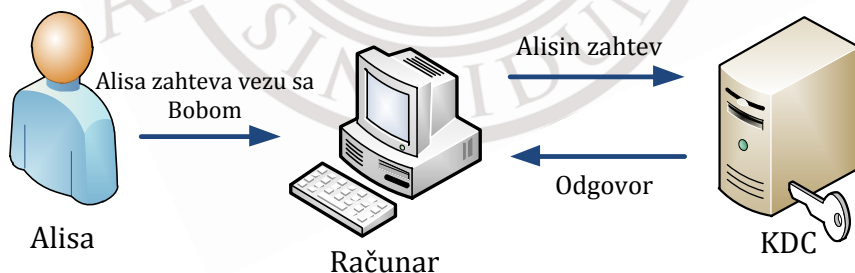
U ovom sistemu za prijavljivanje na *Kerberos*, bezbednost je transparentna za Alisu, dok *KDC* mora biti bezbedan i mora da mu se veruje.

4.4.2. KERBEROS TIKETI

Kompletan *Kerberos* protokol, zasnovan je na tiketima. Alisa je nakon uspešne prijave na *Kerberos*, dobila glavni tiket *TGT*, koji će kasnije da koristi za odobrenje pristupa mrežnim resursima. Na primer, pretpostavimo slučaj u kome Alisa želi da razgovara sa Bobom. Tada Alisin računar dostavlja svoj glavni tiket (*TGT*) *KDC*-u, zajedno sa autentifikatorom. Autentifikator je šifrovani vremenski pečat koji služi za sprečavanja napada zasnovanog na ponovnom slanju poruka. Nakon što je *KDC* proverio validnost autentifikatora, *KDC* odgovara sa drugim tiketom koji Alisa direktno koristi u bezbednoj komunikaciji sa Bobovim računarom. Proces izdavanja tiketa za komunikaciju sa Bobom (koji je Alisa inicijalizovala) prikazan je na slici (Slika 4.23), a koristili smo sledeću notaciju za razumevanje procesa.

- $ZAHTEV = (TGT, \text{autentifikator}),$
- $\text{Autentifikator} = E(\text{vremenski pečat}, S_A),$
- $ODGOVOR = E(\text{„Bob“}, K_{AB}, \text{tiket do Boba}; S_A),$
- $\text{Diket do Boba} = E(\text{„Alisa“}, K_{AB}; K_B).$

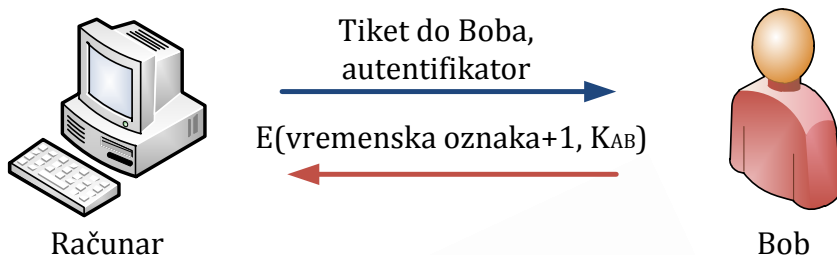
Na slici (Slika 4.23), *KDC* dobija zahtev od Alise, nakon čega sa ključem S_A proverava *TGT* i vremenski pečat. Posle provere, odgovara sa ključem K_{AB} , koji će se koristiti kao sesijski ključ za sesiju između Alise i Boba.



Slika 4.23 Alisa dobija tiket za komunikaciju sa Bobom

Kada je Alisa dobila „tiket do Boba“, tada ona može da započne bezbednu komunikaciju sa Bobom. Proces je prikazan na slici (Slika 4.24), gde je tiket do Boba, zaštićen kao i gore ($\text{autentifikator} = E(\text{vremenski pečat}, K_{AB})$).

Treba da imamo na umu, da Bob dešifruje „tiket do Boba“ sa njegovim ključem K_B , da bi dobio ključ K_{AB} . Ključ K_{AB} se koristi za zaštitu poverljivosti i integriteta u komunikaciji između Alise i Boba.



Slika 4.24 Alisa uspostavlja komunikaciju sa Bobom

Komunikacija između Alise i Boba je zaštićena od ponovnog slanja, sve to zahvaljujući vremenskom pečatu, na osnovu čega *Kerberos* smanjuje broj poruka koje moraju biti poslate. Kao što smo spomenuli u prethodnim poglavljima, jedina mana je što vremenski pečat postaje kritičan parametar bezbednosti. Glavni problem vremenskih pečata je vremenska sinhronizacija satova, ne možemo nikad očekivati perfektnu sinhronizaciju i iz tog razloga neophodna je vremenska tolerancija. U slučaju *Kerberos*-a, vremenska tolerancija može da bude i par minuta, što predstavljala večnost u savremenim računarskim mrežama.

4.4.3. BEZBEDNOST KERBEROS PROTOKOLA

U ovom odeljku, razmotrićemo neke bezbednosne elemente *Kerberos* protokola. Na primer, kada se Alisa uspešno prijavi na sistem, *KDC* Alisi šalje $E(S_A, TGT; K_A)$, gde je $TGT = E(\text{„Alisa“, } S_A; K_{KDC})$. Vidimo da je TGT već šifrovan sa ključem K_{KDC} , zašto se TGT šifrjuje ponovo za ključem K_A ? Ovo predstavlja manji propust u *Kerberos*-u, jer je to samo dodatni posao na koji se troše resursi, a ne pruža dodatnu bezbednost. Ako se desi da ključ K_{KDC} bude otkriven, ceo sistem će biti kompromitovan, iz ovog razloga ne postoji dodatna prednost ponovnog šifrovanja TGT -a, nakon što je već šifrovan sa K_{KDC} .

Možemo da primetimo na slici (Slika 4.23), da Alisa ostaje anonimna u ZAHTEVU. Ovo je dosta dobra bezbednosna osobina, činjenicom da je TGT šifrovan sa K_{KDC}

ključem, dok sa druge *KDC* ne mora da zna ko upućuje zahtev, pre nego što može da dešifruje *TGT*, jer su svi *TGT* tiketi šifrovani sa K_{KDC} . Problem anonimnosti može biti teško rešiv problem. Videli smo problem anonimnosti u *IPSec*-u, ali taj problem nije prisutan kod *Kerberos*a.

Primetimo da u *Kerberos*-u *KDC* prosleđuje Alisi „tiket do Boba“, nakon čega Alisa jednostavno prosleđuje tiket Bobu. Razlog zašto *KDC* nije uradio taj deo posla leži u efikasnosti *Kerberos* protokola. Međutim, ako tiket stigne do Boba pre nego što Alisa inicijalizuje komunikaciju, Bob će morati da ključ K_{AB} drži neko potrebno vreme u raspoloživom stanju.

Na kraju, kako *Kerberos* sprečava napad zasnovan na ponovnom slanju poruka? Prevencija od ovog tipa napada se oslanja na vremenske pečate, koji su sadržani u autentifikatoru. Ali i dalje postoji pitanje koje se odnosi na mogućnost postojanja ove vrste napada, zbog postojanja problema sa vremenskom sinhronizacijom i vremenske tolerancije koja je zadata u *Kerberos* protokolu.

Postoje i neke alternative dizajna *Kerberos* protokola. Na primer, da li bi *KDC* mogao da pamti sesijski ključ umesto što ga stavlja u *TGT*? Ukoliko bi postojala ovakva mogućnost, tada bi *TGT* iz dizajna *Kerberos*-a bio uklonjen. Alternativni pristup koji smo naveli, često se koristi u aplikacijama, ali ne i u *Kerberos*u.

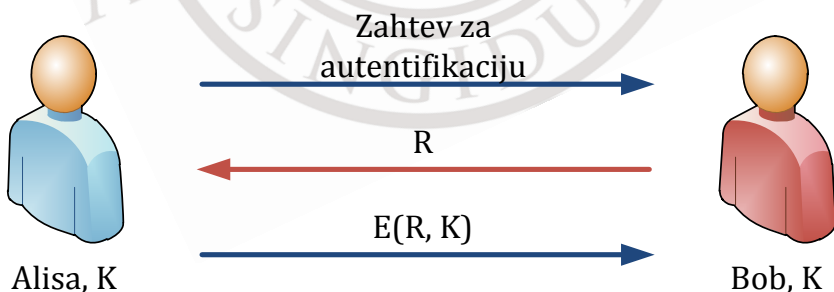
4.5. WEP

WEP (engl. *Wired Equivalent Privacy*) je bezbednosni protokol koji je dizajniran za zaštitu lokalnih (*LAN*) bežičnih mreža. Proklamovani cilj *WEP* protokola je da učini bežični *LAN* jednako bezbednim kao i žičani *LAN*.

Standard 802.11 propisuje bezbednosni protokol na nivou veze podataka. Protokol je nazvan *WEP*, čija je svrha da postigne jednaku bezbednost bežične *LAN* mreže, koja postoji već u žičanoj *LAN* mreži. Budući da žičani *LAN* ne implementira nikakve bezbednosne mehanizme, ovaj cilj se lako postiže. U nastavku videćemo kako je to urađeno kod *WEP*-a.

4.5.1. AUTENTIFIKACIJA U WEP PROTOKOLU

Pretpostavimo sledeći scenario u kome je Bob bežična pristupna tačka (engl. *wireless router*). Simetrični ključ K se deli između Boba (pristupne tačke) i svih korisnika. Ideja da se deli zajednički simetrični ključ, nije toliko dobra. U svakom slučaju, autentifikacija kod *WEP* protokola je jednostavan primer protokola sa izazov-odgovor, kao što je prikazano na slici (Slika 4.25), gde je Bob pristupna bežična tačka, Alisa korisnik i K je deljeni simetrični ključ koji se retko menja (ako ne i nikako).



Slika 4.25 *WEP* autentifikacija

Na koji način Bob autentifikuje Alisu? U prvoj poruci Alisa šalje zahtev za autentifikaciju. U drugoj poruci Bob šalje izazov R . Na kraju, u trećoj poruci Alisa šifruje izazov R sa deljenim ključem K . Bob verifikuje Alisu tako što dešifruje šifrat $E(R,$

K) i ukoliko je vrednost R dobijena nakon dešifrovanja jednaka poslatoj vrednosti R , Alisi je odobren pristup.

WEP poseduje mnoge bezbednosne problem, o kojim možda i ne treba previše raspravljati, ako imamo na umu da protokol nije dizajniran sa osnovama stvarnih bezbednosnih protokola.

4.5.2. ŠIFROVANJE U WEP PROTOKOLU

Posle uspešne autentifikacije, paketi koji se razmenjuju između korisnika bežične mreže su šifrovani sa $RC4$ sekvencijalnom šifrom. Svaki paket saobraćaja je šifrovan sa ključem $K_{IV} = (IV, K)$, gde IV predstavlja inicijalni vektor veličine 3 bajta, koji je poslat nezaštićeno do autentifikovanog korisnika, a ključ K je isti ključ koji je prethodno korišćen u autentifikaciji, prikazano na slici (Slika 4.26).



Slika 4.26 Šifrovanje kod WEP-a

Glavni cilj je da se paketi šifruju sa različitim ključevima, pošto ponovno korišćenje ključa kod $RC4$ šifarskog algoritma predstavlja lošu ideju. Napominjemo da je $RC4$ pseudo perfektna šifra, koja se smatra jakom šifrom uz pravilnu implementaciju. Međutim, postoji jedan mali propust, Trudi zna 3 bajta inicijalnog vektora IV , ali ne zna i ključ K . U ovom slučaju, ključ za šifrovanje se menja i nije poznat Trudi.

Inicijalni vektor IV je dužine samo 3 bajta, ključ K se retko menja, tako da je neminovno da će se ključ $K_{IV} = (IV, K)$ često ponavljati. Ova činjenica je poznata za Trudi, pošto je IV vidljiv, a ključ K se ne menja skoro nikako. Obzirom, da je $RC4$ sekvencijalna šifra, pa ponovno korišćenje ključa generisaće već korišćen radni

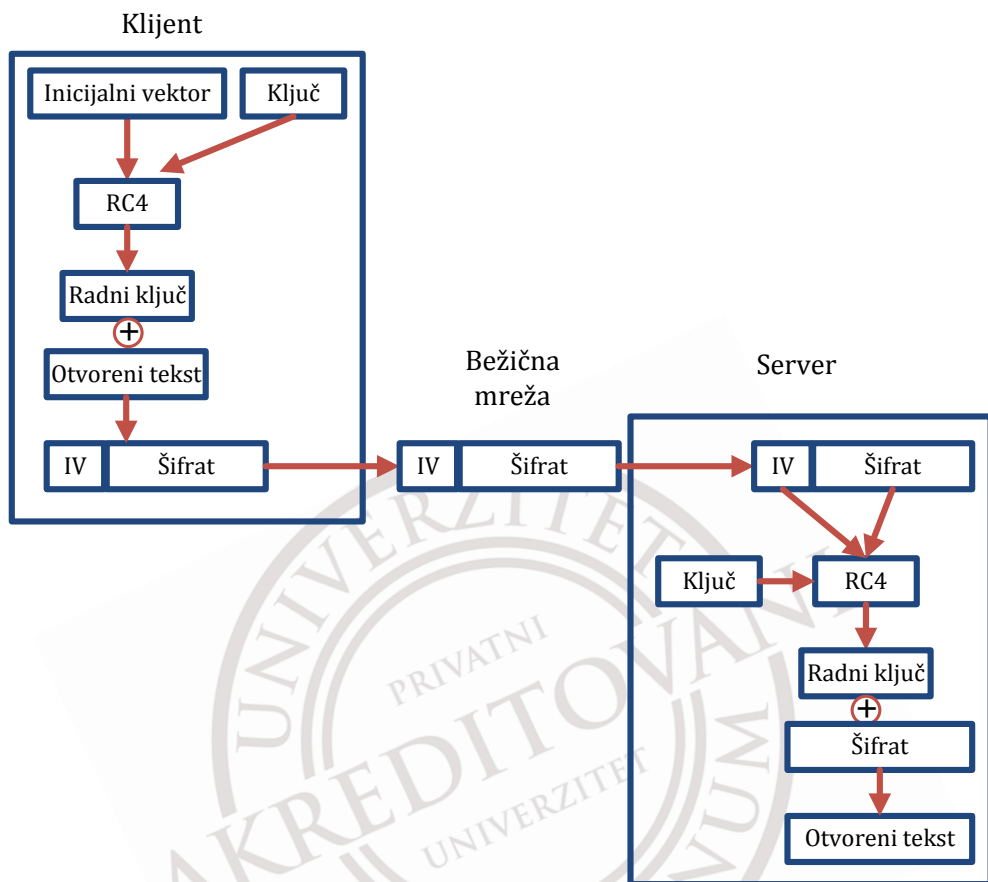
ključ, što predstavlja ozbiljan problem i veliku prednost na strani Trudi. Ponavljanjem istog IV , kriptanalitički posao za Trudi učiniće još lakšim.

Broj ponovljenih ključeva K koji se koriste za šifrovanje moguće je smanjiti redovnom promenom ključa K . Nažalost, ključ K se dugo koristi i retko menja. Promena ključeva predstavlja ručni proces koji je neizvodljiv za pristupne tačke, jer u WEP -u ne postoji urađena procedura koja bi vodila računa o stalnoj promeni ključa.

Ovaj napad od strane Trudi je potpuno realan, jer kad Trudi uhvati ponovljeni inicijalni vektor IV , tada može da pretpostavi i rekonstruiše radni ključ $RC4$ šifarskog algoritma. Zbog dužine inicijalnog vektora IV od samo 24 bita, ponavljanja radnog ključa su relativno česta. Imajući na umu da je korišćena pseudo perfektna šifra, ponovljeni radni ključ je ozbiljan prekršaj u implementaciji i dovodi do ozbiljnih bezbednosnih problema.

Pored ovog problema, postoji još jedan kriptanalitički napad, koji je moguće realizovati i pod pretpostavkom da je $RC4$ implementiran na pravilan način. Ovaj napad se temelji na otkrivanju ključa na osnovu postojanja srodnih ključeva. Videli smo da i pored suptilnih propusta u WEP protokolu postoje i druge vrste napada.

$RC4$ sekvencijalna šifra predstavlja pseudo perfektni šifru (engl. *One-Time pad*). $RC4$ u WEP -u koristi ključ veličine 40 bitova i 24 bita inicijalni vektor IV . Za pravilan i bezbedan rad $RC4$ algoritma, neophodno je odbaciti prvih 256 bajtova radnog ključa (engl. *Key stream*). Osnovni razloga je sprečavanje curenja informacija o unutrašnjem ključu K , na osnovu poznavanja velike količine šifrata. Međutim, implementacija $RC4$ algoritma u WEP -u ne podrazumeva odbacivanje prvih 256 bajtova radnog ključa. U jednoj sesiji od nekoliko hiljada paketa, ponavlja se inicijalni vektor IV , dok se ključ K skoro nikad ne menja. Sve ove činjenice predstavljaju odličnu polaznu tačku za kriptanalitičara.



Slika 4.27 Šifrovanje u WEP protokolu

4.5.3. PROBLEM INTEGRITETA U WEP PROTOKOLU

WEP ima brojne bezbednosne probleme, ali jedan od najupečatljivijih je da koristi CRC (engl. *Cyclic Redundancy Check*) za proveru kriptografskog integriteta. Ovaj metod je preuzet iz oblasti kodovanja za cikličnu proveru integriteta kod zaštitnih kodova u šumnim komunikacionim kanalima. Podsetimo se da kriptografska provera integriteta ima zadatak da otkrije maliciozno ponašanje, a ne samo greške u šumnim komunikacionim kanalima. CRC metod koliko je dobar za otkrivanje grešaka, toliko nije dobar za proveru kriptografskog integriteta, pošto sofisticiran napadač može da promeni podatke i CRC vrednosti, tako da, na prijemnoj

strani ne bude detektovan napad. Zaštita od ove vrste napada zahteva upotrebu drugih kriptografskih tehnika, kao što su *MAC*, *HMAC* ili digitalni potpis.

Ovaj problem provere integriteta je još pogoršan činjenicom da su podaci šifrovani sekvencijalnom šifrom. Zbog upotrebe sekvencijalne šifre, *WEP* šifrovanje je linearno i zbog toga dozvoljava Trudi da direktno promeni šifrat i izračuna nove *CRC* vrednosti, tako da prijemnik neće detektovati promene. Za ovu vrstu napada Trudi ne mora da zna ključ ili otvoreni tekst da bi uspeła da napravi izmenu u podacima. Prema ovom scenariju, Trudi neće znati kakvu je promenu u podacima napravila, ali poenta je da podaci budu oštećeni na način da ni Alisa ni Bobo ne mogu detektovati.

Problemi se još više mogu pogoršati ukoliko se desi da Trudi sazna neke delove otvorenog teksta, tada će Trudi ciljno napraviti promenu u poruci. Na primer, pretpostavimo da Trudi zna *IP* adresu odredišta datog šifrovanog *WEP* paketa. Tada bez poznavanja ključa, Trudi može promeniti *IP* adresu odredišta u adresu po njenom izboru (na primer, njenu *IP* adresu) i *CRC* vrednosti za proveru integriteta, tako da njeni pokušaji ne budu otkriveni na pristupnoj tački. *WEP* saobraćaj je šifrovan samo od korisnika do pristupne tačke i obrnuto, tako da šifrovani paket sa promenjenom *IP* adresom stiže do pristupne tačke, tu biva dešifrovan, a zatim i prosleđen do Trudi na zadatu (zadatu od Trudi) *IP* adresu. Ovaj napad je omogućen zbog nedostatka stvarne provere integriteta. Suština je da *WEP* proveru integriteta ne pruža elemente kriptografske provere integriteta. Svi ovi veliki problemi nastaju zbog narušavanja integriteta.

U *WEP* protokolu postoji mnogo problema, koji ga zajedno čine bezbednosno ranjivim. Na primer, ako Trudi može da pošalje poruku preko bežične mreže i da presretne šifrat, tada ona zna otvoreni tekst i odgovarajući šifrat koji će joj omogućiti da sazna radni ključ koji se koristio za šifrovanje. Ovaj isti radni ključ će se koristiti za šifrovanje svih poruka koje koriste isti inicijalni vektor *IV*, pod uslovom da se ključ *K* duže vremena nije menjao, što je vrlo verovatno. Da li Trudi potencijalno može da sazna otvoreni tekst šifrovane i poslate poruke preko bežične mreže? Možda, Trudi može da pošalje e-poruku Alisi i da nju pita da je prosledi drugoj osobi. Ako Alisa uradi sve po scenariju koji je postavila Trudi, tada Trudi može da presretne šifrat poruke za koji poseduje odgovarajući šifrat i tako otkrije radni ključ koji je iskorišćen za šifrovanje. Nakon toga, Trudi može da dešifruje svaki paket šifrata koji je nastao preko istog inicijalnog vektora *IV*. Sa dru-

ge strane, ako Trudi može ovaj scenario da ponovi više puta, tada može da dešifruje poruke za mnoge različite inicijalne vektore.

Razmotrimo bolje ovaj kriptanalitički napad. *WEP* podaci se šifruju sa algoritmom *RC4*. Ključ paketa je inicijalni vektor *IV* i dugotrajni ključ *K*. Inicijalni vektor je 3-bajtni sufiks koji se dodaje na ključ *K*, tako da je ključ paketa (*IV*, *K*). Napomenimo da se inicijalni vektor šalje otvoreno, dok se novi inicijalni vektor šalje novim paketom. Sada vidimo da Trudi uvek zna inicijalni vektor i šifrat, ali kako Trudi može da pronađe ključ *K*? Ukoliko označimo *RC4* bajtove ključa sa $K_0, K_1, K_2, K_3, K_4, K_5$, gde je $IV = (K_0, K_1, K_2)$, što Trudi zna, ali želi da pronađe $K = (K_3, K_4, K_5)$. Ukoliko Trudi ima dovoljno inicijalnih vektora, moći će da pronađe ključ, bez obzira na dužinu ključa. Preduslov je da Trudi zna prvi bajt niza ključeva za šifrovanje, ili napad na osnovu poznatog otvorenog teksta. Ovaj napad se može osujetiti ako se odbaci prvih 256 bajtova radnog ključa za šifrovanje. Na osnovu preporuke za sprečavanje ove vrste napada, zaključujemo da nisu poštovana sva pravila za implementaciju *RC4* šifarskog algoritma.

Pored lozinke koja je zahtevana za autentifikaciju, postoji i parametar *SSID* (engl. *Service Set Identifier*) koji pristupna tačka emituje u svom dometu. *SSID* predstavlja sličan parametar kao i korisničko ime koje korisnik treba da koristi u autentifikaciji. Jedna od *WEP* bezbednosnih funkcija omogućava konfigurisanje pristupne tačke, na takav način da ne emituje *SSID*, već da korisnik mora ručno da unese naziv (deluje kao lozinka, koju korisnici moraju da znaju da bi se autentifikovali). Međutim, korisnici pošalju *SSID* da bi kontaktirali pristupnu tačku, tada Trudi samo treba da presretne jedan paket i da otkrije odgovarajući *SSID*. U praksi postoje alati koji će naterati korisnike da se nasilu odjave sa pristupne tačke, a zatim ponovo autentifikuju na istoj uz ponovno slanje *SSID* naziva mreže. Vidimo da ni *SSID* ne predstavlja konačno rešenje, jer sve dok postoji bar jedan korisnik na mreži, to će biti jednostavan proces u kom Trudi lako saznaje *SSID*. Svakako, ova mogućnost definitivno ne treba da bude bezbednosna opcija.

Teško je, a možda i nemoguće videti u *WEP*-u nešto drugo osim bezbednosne katastrofe. Međutim, i pored svih svojih bezbednosnih problema, u nekim okolnostima moguće je napraviti od *WEP*-a umereno bezbedan protokol u praksi. Na primer, pored lozinke i nepoznatog *SSID*, moguće je uključiti i opciju koja se odnosi na filtriranje saobraćaja na osnovu *MAC* adrese (fizičke adrese). Na ovaj način

bi iziskivali dodatni napor na strani napadača koji se mora uložiti na prevazilaženje ove prepreke.

Na kraju, treba da imamo na umu da postoje i druge bezbednosne alternative *WEP* protokolu. Na primer, *WPA* (engl. *WiFi Protected Access*) je znatno jači, ali on je dizajniran da koristi isti hardver kao i *WEP*, i iz tog razloga su zahtevani određeni bezbednosni kompromisi. Do danas postoji nekoliko tipova napada na *WPA*. Osim *WPA*, tu je i *WPA2* koji je nešto jači od *WPA*, ali zahtevan je snažniji hardver. Kao i za *WPA*, postoje i mogućnosti napada na *WPA2*, ali ukoliko su izabrane izuzetno jake lozinke, ovi bezbednosni protokoli postaju praktično bezbedni.

4.5.4. OSNOVNE ZA BEZBEDNO KORIŠĆENJE BEŽIČNIH MREŽA

Krenućemo od nekih osnovnih karakteristika javnih *WiFi* bežičnih mreža. Da bismo bolje shvatili probleme koji postoje u ovom domenu, navešćemo primer sa slobodnim „besplatnim“ bežičnim mrežama. Na primer, jedan aerodrom u Vašingtonu obezbedio je svojim putnicima slobodan i besplatan pristup bežičnoj mreži sa izlazom na Internet. Radi lakšeg pružanja *IT* usluga, zanemareni su zahtevni bezbednosni mehanizmi. Na ovaj način lični podaci skoro svih putnika su se našli u etru (u signalu bežične mreže) potpuno nezaštićeni. Procene su bile da je približno 97% putnika bilo u potpunosti ranjivo.

Nedostatak bezbednosti na bežičnim mrežama je zajednički problem svih korisnika istih. Logično je pretpostaviti da svako može da pristupi podacima koji su emitovani u etru, pregleda ih, promeni i pošalje dalje. Sa druge strane, dozvoljen je anoniman pristup mreži bilo kom korisniku. *RF* tehnologija omogućava bilo kome da snima i obrađuje signal koji je emitovan ili da emituje signal. Na ovaj način nikada ne možemo da budemo sigurni da baš osoba pored nas ne pokušava da pristupi našim podacima.

Danas u svetu postoji veliki broj lažnih bežičnih mreža, čiji je glavni cilj da namame korisnike na korišćenje. Često u nazivu ove mreže postoji „Besplatan internet“ i sl.

Pre povezivanja računara na nepoznate bežične mreže, kod kojih je tešku utvrditi legitimitet, neophodno je prekonfigurisati lični računar, u cilju sprečavanja

sistemskeg kompromisa. To podrazumeva proveru zaštitnog zida, antivirusa (provera ažurnosti definicije za otkrivanje virusa) i drugih programskih zakrpa koje mogu da dovedu do ozbiljnih problema. Pored ovih osnovnih konfiguracija, preporučuje se svim korisnicima da šifruju važne podatke ili da isključe programe za razmenu podataka. Na ovaj način moguće je izbeći neovlašćen pristup ličnim podacima. Tipičan primer su servisi za čuvanje podataka na Internetu (*dropbox*, *skydrive*, itd), koji u momentu kada detektuju povezanost sa Internet mrežom započinju sinhronizaciju podataka. Pored ovih preporuka, neophodno je onemogućiti ličnom računaru automatsko povezivanje na mrežu. U ovom slučaju od korisnika se očekuje da redovno proveravaju status bežičnog adaptera. Preporuka je da adapter bude isključen ukoliko nije potrebno koristiti mrežne resurse.

Druge preporuke se odnose na korisničke naloge u okviru operativnog sistema. Preporučuje se upotreba korisničkog naloga bez posebnih privilegija (neadministratorski nalog), na osnovu kojih bi bilo moguće napraviti neke neželjene promene u operativnom sistemu.

Ukoliko nije apsolutno neophodno, preporuka je da se izbegava rad sa servisima za elektronsko bankarstvo, elektronsku poštu i druge važne servise. U slučaju da je pristup ovim servisima neizbežan, bitno je da proveravamo na strani Internet pregledača da je konekcija bezbedna (*HTTPS*), tačnije da koristimo *SSL/TLS* bezbednosni protokol preko koga smo se prijavili na servis i sve podatke razmenili u šifrovanoj formi. Pored ove preporuke, preporučuje se korišćenje i *VPN* protokola, ukoliko postoji kao opcija u momentu povezivanja na bežičnu mrežu. napominjemo da *VPN* protokol obezbeđuje šifrovanje podataka u posebno „tunelovanoj“ komunikaciji.

Ostavljanje ličnih računara bez nadzora, takođe predstavlja ozbiljnu pretnju. U ovim situacijama moguće su neželjene modifikacije na operativnom sistemu ili još gore, krađa računara koja je uobičajena pojava. Krađa računara danas predstavlja veliki problem. Sve je postalo mobilno (prenosivi računari, pametni telefoni, *IP* štampači, *IP* kamere), tako da svi ovi uređaji ostavljeni bez nadzora mogu da prouzrokuju ozbiljne bezbednosne probleme.

4.5.5. SAVETI ZA BEZBEDNO KONFIGURISANJE BEŽIČNIH UREĐAJA

U ovom odeljku diskutovaćemo o nekim najosnovnijim podešavanjima pristupnih tačaka za izgradnju sopstvene bežične mreže. Najnovija istraživanja pokazala su da veliki broj korisnika koji sami postavljaju ove uređaje, ne poznaju dovoljno materiju koja se odnosi na sprovođenje nekih bezbednosnih mera i iz tog razloga ovi uređaju ostaju na najosnovnijim fabričkim podešavanjima. Slede koraci kroz koje je neophodno prći:

1. Krenućemo od vrste protokola koji će se koristiti za pristup i zaštitu u bežičnoj mreži. Preporuka je da se koristi protokol *WPA2-PSK*. Ovaj protokol koristi *AES* kriptografski algoritam za šifrovanje i implementira bezbedne protokole za razmenu ključeva. Svakako, *WEP* kao opciju nije preporučeno koristiti osim zbog velikih bezbednosnih problema.
2. Svi uređaju za pristupne tačke poseduju neka fabrička podešavanja, koja se upravo odnose na korisničko ime i lozinku („admin“ i „12345“). Ukoliko korisnik ne promeni ove početne parametre, postoji mogućnost da napadač potencijalno promeni i druge parametre pristupne tačke koji se odnose na aktivirane bezbednosne opcije (napadač može postaviti *WEP* kao protokol za autentifikaciju i sl.). Početni parametri su javni i zavise od proizvođača opreme.
3. Nije preporučljivo koristiti lake lozinke. Zahtevana je upotreba jakih lozinki, koje kombinuju slova, brojeve i specijalne karaktere sa minimalnom dužinom od 10 karaktera. U svim drugim varijantama, mogući su hibridni napadi zasnovani na rečnicima i žargonskom govoru. Osim jake lozinke, očekivana je promena lozinke bar na mesečnom nivou.
4. Ukoliko je bežična mreža postavljena za ličnu upotrebu, preporuka je da naziv mreže bude bez bilo kakvog posebnog značenja ili asocijativnog značenja, na osnovu koga vlasnik može da pretpostavi ko je vlasnik bežične mreže.
5. Ukoliko je bežična mreža postavljena za ličnu upotrebu, a u slučaju putovanja na duži vremenski period (godišnji odmor), preporučuje se gašenje bežične mreže. Ukoliko se radi o sofisticiranom napadaču, ovo može omogućiti snimanje velike količine saobraćaja i sprovođenje drugih radnji za uspešan napad (vremenski zahtevan).

6. Ukoliko nije potreban naziv mreže – *SSID*, u tom slučaju mrežu ne koristi veliki broj korisnika, preporučuje se isključivanje opcije za emitovanje *SSID*-a.
7. Smanjiti prostiranje (širenje) radio talasa izvan objekta u kome je postavljena pristupna tačka. Korišćenjem usmerenih antena može se usmeriti širenje unutar sredine u kojoj se koristi bežična mreža. Ovim se ne dobija samo dobra optimizacija, već i smanjenje mogućnosti da napadač locira mrežu.
8. Ukoliko nije otežavajuće za korisnika ili administratora mreže, preporučuje se korišćenje *MAC* adrese. Na ovaj način uključen je filter koji neće dozvoliti povezivanje neautorizovanim uređajima. Treba imati na umu da neki uređaji dozvoljavaju promenu *MAC* adrese i da je ovo samo još jedna zahtevna prepreka postavljena pred napadača.
9. Ukoliko mreža ne raspolaže sa većim brojem korisnika, preporučuje se isključivanje opcije *DHCP*. *DHCP* servis obezbeđuje svim učesnicima dinamičke *IP* adrese vodi računa o mogućnosti za postojanje duplih *IP* adresa u mreži. U ovom slučaju, očekuje se da na računaru korisnika bude postavljena statička *IP* adresa.
10. Pored ovih osnovnih preporuka, postoje mogućnosti za izgradnju nešto složenijih bežičnih mreža, koje predviđaju upotrebu *VLAN*-ova. Za ovaj poduhvat, neophodno je poznavati bolje savremene računarske mreže. Ovaj scenario je obično poželjan kada u mreži postoji veliki broj računara, kada se bežična mreža konfiguriše kao poseban *VLAN*.
11. Kao poslednje, preporučuje se organizovanje stručnih seminara, na kojima će članovi organizacija steći elementarna znanja i veštine o bezbednosnim protokolima i bezbednosnoj politici organizacije. Na ovaj način će biti spremi na prave reakcije u kriznim situacijama, pa čak i kome da se obrate u slučaju eventualnih incidenata.

4.6. GSM

Mnogi bežični protokoli, kao što je *WEP*, imaju loše rezultata po pitanju bezbednosti. U ovom odeljku ukratko ćemo diskutovati o bezbednosti *GSM* mobilnih telefona. *GSM* (engl. *Global System for Mobile Communications*) prikazuje neke jedinstvene bezbednosne probleme koji se javljaju u bežičnom okruženju. Predstavlja odličan primer za greške koje nastaju u fazi projektovanja, koje je kasnije teško ispraviti. Pre nego što se počnemo baviti detaljima *GSM* bezbednosti, navesti ćemo neke osnovne informacije o razvoju tehnologije mobilnih telefona.

Pre 1980. godine mobilni telefoni su bili skupi, potpuno nebezbedni i bili su fizički dosta veliki. Prvi telefoni su bili analogni, ne digitalni, a bilo je nekoliko standarda ali nijedan se nije bavio sa bezbednosti.

Najveći bezbednosni problemi sa ranim mobilnim telefonima su postojanje mogućnosti za kloniranje. Ovi mobilni telefoni prilikom slanja poziva šalju i svoj identitet, preko koga su se naplaćivali razgovori, jer je tako bilo moguće utvrditi ko je poslao poziv. Pošto je identitet javno, nezaštićeno poslat preko bežične mreže, svako može da kopira i da napravi kopiju telefona. Ovo je omogućilo napadačima da besplatno telefoniraju. Kloniranje telefona je postao unosan posao, preko lažnih baznih stanica koje su se jednostavno pravile.

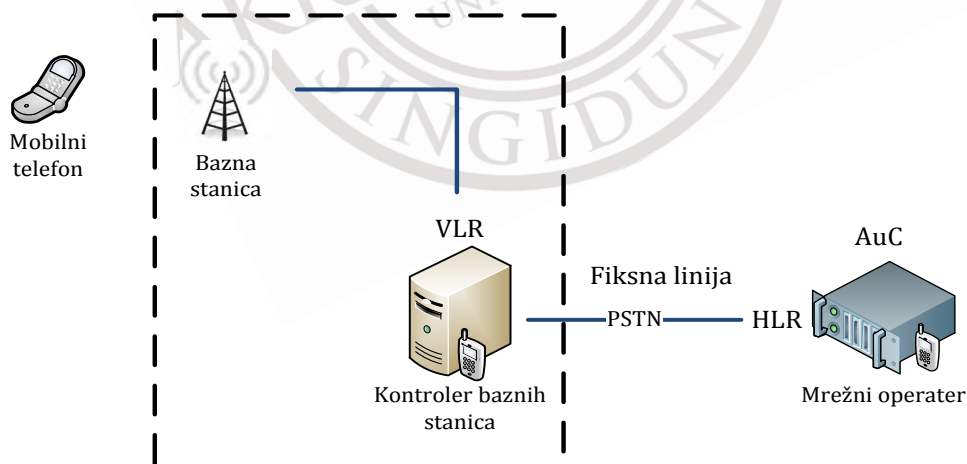
U tom haotičnom okruženju pojavila se *GSM* mreža, koja je uvedena 1982, a 1986 postala globalni sistem za mobilne komunikacije. Osnivanje *GSM* obeležava zvanični početak druge generacije tehnologije mobilnih telefona. Kasnije ćemo reći nešto više o bezbednosti *GSM*.

Međutim, danas postoji i treća generacija mobilnih komunikacija ili *3GPP* (engl. *Generation Partnership Project*). Nakon bezbednosti *GSM* protokola koja je interesantan školski primer, pomenućemo neke bezbednosne aspekte *3GPP*-a.

4.6.1. ARHITEKTURA I BEZBEDNOST GSM PROTOKOLA

Opšta arhitektura GSM-a je prikazana na slici (Slika 4.28), u razumevanju arhitekture koristićemo sledeću terminologiju.

- Mobilni je mobilni telefon;
- Pristupna tačka je najbliža bazna stanica kojoj telefon pristupa preko bežične mreže;
- Posećena mreža je mreža koja je sačinjena od više baznih stanica i kontrolera baznih stanica, koji deluju kao čvorište za povezivanje baznih stanica sa ostatkom GSM mreže.
- Javna telefonska mreža ili *PSTN*, predstavlja obični telefonski sistem. *PSTN* se ponekad naziva i "fiksna telefonija" da bi ga razlikovali od bežične mreže.
- Mreža operatera (domaćina) je mreža u kojoj je registrovan mobilni telefon. Svaki mobilni telefon je povezan sa jedinstvenim operaterom. Operaterova mreža sadrži lokalni registar ili *HLR* (engl. *Home Location Register*), koji vodi računa o trenutnim lokacijama svih mobilnih telefona koji su navedeni u *HLR*. Autentifikacioni centar ili *AuC* (engl. *Authentication Center*), održava informacije presudne za obračun svih mobilnih telefona koji pripadaju odgovarajućem HLR-u.



Slika 4.28 GSM arhitektura

Svaki *GSM* mobilni telefon sadrži modul pretplatničkog identiteta ili *SIM*, koja predstavlja otpornu pametnu karticu (engl. *Smartcard*). *SIM* kartica sadrži internacionalni mobilni pretplatnički *ID* ili *IMSI* (engl. *International Mobile Subscriber ID*), koji se koristi za identifikaciju mobilnog. *SIM* kartica u sebi sadrži 128 bitni ključ koji je poznat samo mobilnom uređaju i operateru.

Svrha upotrebe pametnih kartica za *SIM* je da obezbedi jeftinu formu hardvera, otpornu na neovlašćen pristup. *SIM* kartica obezbeđuje dvo-faktorsku autentifikaciju, oslanjajući se na „nešto što imate“ i „nešto što znate“ u obliku *PIN* kod od četiri cifre. *PIN* kod je naišao na otpor u upotrebi i obično se ne upotrebljava.

Podsetićemo se ukratko, posećena mreža je mreža u kojoj je mobilni telefon trenutno lociran. Bazna stanica je jedna ćelija mobilnog sistema, u kome kontroler baznih stanica upravlja sa više baznih stanica. *VLR* poseduje informacije o svim mobilnom telefonima koji se trenutno nalaze u mreži na baznoj stanici odgovarajućeg kontrolera.

Operater sadrži najvažnije informacije o mobilnim uređajima, kao što je *IMSI* i 128 bitni ključ. Uloga *IMSI* i ključa je slična ulozi korisničkog imena i lozinke, koje mobilni telefon koristi kada treba da uputi telefonski poziv. *HLR* prati trenutne lokacije svih registrovanih mobilnih uređaja, dok *AuC* sadrži bazu *IMSI*-ova i ključeva svih registrovanih mobilnih uređaja.

U nastavku ovog odeljka diskutovaćemo ukratko o *GSM* bezbednosnoj arhitekturi. Primarni ciljevi koji se odnose na bezbednost, propisani od strane dizajnera bili su:

1. Napraviti *GSM* podjednako bezbedan kao obični telefon – *PSTN*;
2. Sprečiti kloniranje mobilnih telefona;

GSM nije dizajniran da se odupre aktivnom napadu. U to vreme aktivni napadi su bili neizvodljivi i tako se smatralo, jer je potrebna oprema bila skupa. Međutim, danas je cena takve opreme jednaka ceni mobilnog telefona, tako da je aktivni napad ne samo moguć, nego i jednostavan. Dizajneri *GSM* su smatrali da je najbitnije rešiti probleme koji su se odnosili na probleme sa obračunom potrošnje i druge slične napada istog nivoa.

GSM protokol pokušava da se bavi sa tri bezbednosna pitanja: anonimnost, autentifikacija i poverljivost. U *GSM*-u pitanje anonimnosti je trebalo da spreči presretanje saobraćaja od identifikovanih korisnika (problem sa *ID*). Anonimnost nije naročito bila važna za telefonske kompanije, osim u meri u kojoj je to važno za kupca.

Autentifikacija sa druge strane je od najvećeg značaja za telefonske kompanije, iz razloga što je neophodno obezbediti tačnu potvrdu identiteta za pravilan obračun. Problem kloniranja koji je postojao može da se posmatra kao jedan nedostatak autentifikacije. Kao i kod anonimnosti, poverljivost poziva preko bežične mreže je vrlo važna klijentima, iz tog razloga ovo postaje važno i za telefonske kompanije.

U razmatranju *GSM* protokola, u kratkim crtama ćemo diskutovati o dizajnu protokola koji obezbeđuje anonimnost, autentifikaciju i poverljivost.

Prvo anonimnost, *IMSI* se koristi za inicijalnu identifikaciju korisnika koji poziva (pozivač) i šalje se otvoreno na početku poziva. Zatim se korisniku dodeljuje slučajno generisani *TMSI* (engl. *Temporary Mobile Subscriber ID*) koji na dalje služi za identifikovanje pozivača. *TMSI* se često menja i šifruje svaki put kada se šalje. Ne postoji jaka forma anonimnosti. Ako napadač uhvati početak poziva, anonimnost u tom slučaju ne postoji, a ako propusti početak, anonimnost je praktično dobro zaštićena. U većini primena ova tehnika je verovatno dovoljna, ali dizajneri nisu previše vodili računa o anonimnosti.

Drugo autentifikacija, u *GSM* protokolu autentifikacija nije uzajamna. Korisnik mobilnog telefona se autentifikuje pred baznom stanicom, jer je to najbitnije za telefonske kompanije zbog naplate. Ovo može biti mesto napada, u kome napadač može da iskoristi lažne bazne stanice. Nećemo detaljno obrađivati notaciju autentifikacije u *GSM* protokolu, ali navešćemo da je korišćen dizajn protokola „izazov-odgovor“.

I na kraju, servis poverljivosti je obezbeđen upotrebom sekvencijalne šifre. Stepen greške procenjuje se na oko 1/1000. Greška je suviše visoka za blokovske šifre. Drugi razlog zašto se ne koriste blokovske šifre je u bolja hardverska implementacija sekvencijalnih šifara.

Bitno je napomenuti da se saobraćaj šifruje samo između mobilnog uređaja i bazne stanice, ali se ne šifruje između bazne stanice i kontrolera bazne stanice. Od sekvencijalnih šifara, najveću zastupljenost je imala šifra A5/1. Ovu šifru moguće je probiti za manje od dve sekunde na bazi otvorenog teksta.

Pored navedenih bezbednosnih problem, postoje i problemi sa *SIM* karticama. Najpoznatiji napadi na kartice su:

- Optička indukcija greške (engl. *Optical Fault Induction*), napad omogućava napadači izvlačenje 128 bitnog ključa;
- Napad particionisanjem (engl. *Partitioning Attacks*), koristeći vremensku zavisnost trošenja energije, moguće je izvući ključ sa samo 8 adekvatno izabраних otvorenih tekstova;

Uz fizičko posedovanje *SIM* kartice, napadač može izvući ključ za samo nekoliko sekundi.

Jedan od možda najlakših scenarija napada je lažna bazna stanica, preko koje je moguće iskoristiti dve ranjivosti:

- Šifrovanje nije automatizovani proces, to znači da bazna stanica određuje da li će biti šifrovanja ili neće, bez znanja korisnika mobilnog uređaja.
- Bazna stanica nije autentifikovana od strane korisnika mobilnog uređaja, tako da ovo potvrđuje još jednom jednostavnost ovog napada.

U slučaju ovog napada, račun troškova ide lažnoj baznoj stanici. Lažna bazna stanica može sprovoditi napad izabranog otvorenog teksta bez posedovanja *SIM* kartice. Osim ovih navedenih napada na *GSM* protokol, moguć je i *DoS* napad, ometanjem signala i ovo je uvek prisutno u bežičnoj komunikaciji. Zatim, postoji mogućnost i za reemitovanje ili ponovno slanje poruka. *GSM* protokol nema zaštitu od napada izazvanog ponovnim slanjem poruka.

Na kraju ovog odeljka možemo da zaključimo da je *GSM* protokol dostigao svoje ciljeve (eliminiseo kloniranje, učinio pristupnu tačku bezbednom, kao i *PSTN*) i da je umereno bezbedan. Glavne ranjivosti *GSM* su slaba šifra, problem *SIM* kartice, lažna bazna stanica i ponovno slanje poruka. Što se tiče *PSTN* ranjivosti, moguće je prisluškivanje, različiti aktivni i pasivni napadi.

4.6.2. TREĆA GENERACIJA PROTOKOLA – 3GPP

Bezbednost treće generacije mobilnih telefona bila je predvođena sa *3GPP*. Grupa programera koja je radila na razvoju *3GPP*-a, vodila je računa više o bezbednosti nego programeri *GSM*-a. *3GPP* bezbednosni model je izgrađen na bezbednosnim ranjivostima *GSM*-a. *3GPP* programeri su pažljivo zakrpili sve od poznatih ranjivosti *GSM*-a. Na primer, *3GPP* uključuje uzajamnu autentifikaciju i zaštitu integriteta (kao što je komanda započni šifrovanje) između bazne stanice i mobilnog uređaja. Ovo poboljšanje eliminiše napad umetanjem lažnih baznih stanica. Takođe, ključevi za šifrovanje se ne mogu ponovo koristiti. Ovime je sprečeno ponovno emitovanje parametara. Slabi kriptografski algoritmi (*A5/1*, *A5/2* i *COMP128*) su zamenjeni sa jakim algoritmom po nazivu *Kasumi*, koji je prošao rigorozne provere. Pored toga, šifrovanje je produženo sa mobilnog pa sve do kontrolera bazne stanice.

Istorija mobilnih telefona, od prve generacije kroz *GSM* i sada *3GPP*, lepo govori o evoluciji bezbednosti koja se često javlja i u drugim sistemima. To je jedan krug, u kome napadači razvijaju nove napade, branioci odgovaraju novim zaštitama, koje opet postaju izazovi za napadače. U idealnom slučaju, koji je u praksi skoro nemoguć, potrebno je pre razvoja nekog sistema sprovesti rigorozne analize sa aspekta bezbednosti i tako izbeći sve probleme kasnije. Međutim, kao što smo rekli, teško je predvideti budućnost, smer tehnološkog razvoja da bi se svi problemi u startu izbegli. Na primer, napad lažnom baznom stanicom je bio nemoguć na početku razvoja *GSM*, ali danas je to moguće. Međutim, koliko god *3GPP* bio u prednosti u odnosu na *GSM* bezbednost, trka u razvoju novih mehanizama bezbednosti se nastavlja.

5. BIOMETRIJA

Tradicionalni sistemi za proveru identiteta zasnovani su na nečemu što znamo - na primer lozinkama - ili na nečemu što posedujemo - *smart* karticama, *tokeni*-ma, mobilnim telefonima... Ovi uređaji ne mogu garantovati da se radi o legitimnim korisnicima, jer ne postoji jaka veza između autentifikatora i servisa za autentifikaciju. Problem nastaje u slučaju njihovog kompromitovanja (krađa, gubljenje, kopiranje i sl.).

Problem je rešen uvođenjem još jednog atributa „nečeg što jesmo“. Biometrija ili bio-informacija se nameće kao moguće rešenje za obezbeđenje čvrste veze između autentifikatora i sistema za autentifikaciju.

Reč „biometrija“ vodi poreklo od grčke imenice „bios“ – život i glagola metreo – meriti. Biometrija je opšti termin za opis i merenje fizičkih karakteristika koje mogu biti korišćene za autentifikaciju.

Biometrijski sistemi su bazirani na fizičkim ili bihejvioralnim karakteristikama ljudskih bića kao što je lice, glas, otisak prsta, iris i drugo. Biometrijski podaci imaju potencijalnu prednost da budu jedinstveni identifikatori jedne osobe. U zavisnosti od vrste biometrijskog izvora, mogu da sadrže dovoljnu ili nedovoljnu količinu informacija za određenu primenu. Za estimaciju maksimalne količine informacija neophodno je dobro poznavati osobine biometrijskih podataka okarakterisane prema zadatom tipu biometrijskog izvora, kao i tehnologije za precizno očitavanje i ekstraktovanje informacija. Obzirom na osobine koje poseduju biometrijski podaci biometrija je postala ozbiljan kandidat za zamenu tradicionalnih metoda na polju autentifikacije i autorizacije pojedinaca.

Kasnije je nastala ideja o generisanju kriptoloških ključeva na osnovu biometrijskih izvora. Hardverska i softverska rešenja za informacionu bezbednost, koja učestvuju na direktan ili indirektan način u skladištenju, obradi i prenosu podataka, moraju da koriste adekvatne kriptografske mehanizme koji obezbeđuju računarsku ili praktičnu sigurnost koja podrazumeva sigurnost u odnosu na protivnika koji ima specifične ograničene vremenske i računarske resurse. Snaga ovih kriptografskih mehanizama je određena snagom kriptološkog ključa. Danas mnoge zemlje razmatraju ili već koriste biometrijske podatke za podizanje nivoa bezbednosti u cilju zaštite pojedinca od krađe identiteta ili lažnog predstavljanja.

5.1. VRSTE BIOMETRIJSKIH PODATAKA I NJIHOVA PODELA

U ovom odeljku navešćemo skoro sve poznate vrste biometrije i njihovu podelu s aspekta trajnosti, namene, dimenzionalnosti i načina očitavanja.

Najpoznatije biometrije koje se koriste u savremenim servisima za autentifikaciju i druge kriptografske svrhe su:

- Lice;
- Otisak prsta;
- Otisak dlana;
- Vene;
- Retina;
- Iris;
- Glas;



Slika 5.1 Biometrija lica

Za biometriju lica koristi se slika i video kao mediji za prikupljanje biometrijskih karakteristika. Postoji više različitih algoritama za ekstrakciju informacionog sadržaja iz biometrijskih uzoraka. Pored 2D biometrije lica (Slika 5.1), danas je popularna i 3D biometrija lica, koja uključuje i novu paletu algoritama za prepoznavanje.

Otisak prsta predstavlja najstariju metodu koja je korišćena za prepoznavanje i autentifikaciju. Informacioni sadržaji su ekstraktovani preko brazda na površini kože, u odnosu na koje se pozicioniraju tačke (minucije), koje poseduju osobine jedinstvenosti (Slika 5.2).



Slika 5.2 Biometrija otiska prsta

Otisak prsta se danas najviše upotrebljava u forenzičke svrhe, izdavanje biometrijskih ličnih dokumenata, daktiloskopija, kao i svakodnevna upotreba u uređajima za autentifikaciju. Danas većina laptop računara sadrži biometrijske čitače za otisak prsta, kao i pametni mobilni telefoni (*iphone 5s*).



Slika 5.3 Biometrija dlana

Veliku upotrebu danas ima i otisak dlana (Slika 5.3), ali ga karakteriše niska pouzdanost. Niska pouzdanost nastaje zbog male količine informacionog sadržaja i zbog velike varijabilnosti. Mala količina informacionog sadržaja utiče direktno na

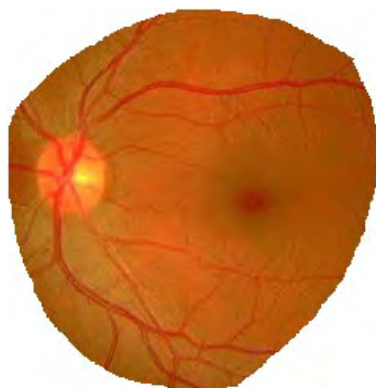
osobine jedinstvenosti i tako stvara mogućnost za postojanje identičnih biometrijskih obrazac kod više različitih ljudi.

Razvoj novih softverskih i hardverskih tehnologija omogućio je i razvoj i eksploataciju novih biometrijskih izvora. Tako je nastao jedan pouzdan i precizan biometrijski izvor na osnovu ljudskih vena (Slika 5.4). Od uređaja za skeniranje ili pribavljanje ove vrste biometrije se koriste skeneri sa LED i monohromatskim diodama. Dobijeni biometrijski obrazac je predstavljen sa strukturom crnih linija koje se razlikuju po debljini.



Slika 5.4 Biometrija vena

Sledeći biometrijski izvor je pozicioniran na retini ljudskog oka. Skeniranjem mrežnjače dobijamo raspored krvnih sudova u oku (Slika 5.5), što ujedno predstavlja i biometrijski obrazac preko koga se ekstrahuje informacioni sadržaj. Retina nije isto što i skeniranje irisa oka. Takođe, kao i kod dlana, niska preciznost karakteriše ovaj biometrijski podatak.



Slika 5.5 Biometrija retine

Iris biometrija predstavlja vrlo značajan biometrijski izvor za naše kriptografske potrebe, zbog veoma bogatog informacionog sadržaja koji se može koristiti pored autentifikacije i za generisanje kriptoloških ključeva. Iris u oku je predstavljen obojenom šarom, prikazano na slici (Slika 5.6) kao region između dve kružnice. Servisi zasnovani na biometriji irisa obezbeđuju visoku preciznost i pouzdanost. Tehnologija koja se koristi za procesiranje biometrijskih podataka kod irisa i dalje ima visoku cenu i iz tog razloga nije dostupna za široku upotrebu.



Slika 5.6 Biometrija irisa

Biometrija glasa je takođe popularan biometrijski izvor koji se može koristiti za izdvajanje određenih karakteristika (Slika 5.7) koje se kasnije mogu upotrebljavati u servisima za autentifikaciju. Biometrija glasa nije toliko pouzdana kao biometrija irisa. Postoji velika varijabilnost kod glasa kao biometrijskog podataka, koja može biti izazvana raznim šumovima proizvedenim uticajima okoline i druge zavisnosti koje mogu biti uvedene. Na primer, prehlada i druge mutacije glasa.

Praksa je pokazala da je biometriju glasa najbolje koristiti u kombinaciji sa drugim biometrijama. Na primer, kombinacija irisa i glasa.



Slika 5.7 Biometrija glasa

U ovom delu govorićemo o nekim osnovnim podelama kada je reč o samom načinu upotrebe biometrijskih podataka u autentifikacionim servisima. Prva podela odnosi se na aspekt trajnosti biometrijskih podataka. Sa ovog aspekta biometrija može da bude opoziva ili neopoziva. Opoziva upotreba biometrije omogućava neograničenu ponovnu upotrebu biometrijskih obrazaca sa istih biometrijskih izvora. Ova je postignuto razvojem novih algoritama koji uglavnom potiču iz nove oblasti poznatije kao biometrijska kriptografija. U ovom slučaju biometrijski obrasci dobijeni preko transformacija ovih algoritama, ne odaju originalne biometrijske podatke, a u servisima u kojima se koriste poseduju identične biometrijske osobine sa svim karakteristikama koje odgovaraju nekom pojedincu.

Suprotno ovome, neopoziva biometrija predstavlja upotrebu originalnih biometrijskih podataka u servisima za autentifikaciju. U ovom slučaju, kompromitovanjem biometrije ne bismo više imali mogućnost da koristimo isti biometrijski izvor u servisu za autentifikaciju. Biometrijski izvor ne može da se menja, on traje ceo život.

Sa aspekta dimenzionalnosti možemo da napravimo podelu na:

- Monomodalne;
- Multimodalne;

Monomodalana biometrija pretpostavlja korišćenje samo jednog tipa biometrije. Primer za monomodalnu biometriju je upotreba otiska prsta za autentifikaciju ili irisa.

Multimodalana biometrija pretpostavlja upotrebu dve ili više različitih vrsta biometrija. Potreba za multimodalnom biometrijom je nastala zbog pojedinačnih nedostataka svih vrsta biometrija. Na ovaj način se prevazilazi većina nedostataka. U praksi se obično spajaju dva obrasca ili više. Multimodalna biometrija može biti opoziva ili neopoziva.

Sa aspekta primene biometrijskih podataka, biometrijski podaci mogu biti korišćeni u poslovne i čisto bezbednosne svrhe. Pod poslovnim svrhama podrazumevamo primenu u bankama (savremeni bankomati, šalteri), elektronska trgovina, kontrola pristupa u nekim poslovnim okruženjima. Pod bezbednosnim svrhama podrazumevamo primenu u okruženjima gde je nivo bezbednosti koji je zahtevan izuzetno visok. Primer za to su nuklearna postrojenja, energetske kompleksi i vladine institucije.

I poslednji aspekt o kome ćemo navesti je podela prema načinu prikupljanja biometrijskih podataka, u zavisnosti od tehnologije:

- Audio (glas);
- Vizuelna (fotografija, snimci);
- Termička (termogram);
- Mikrobiološka (DNK);
- Grafološka (potpis);

U nastavku ovog odeljka izvešćemo nekoliko zaključaka koji mogu da budu od velike koristi za razumevanje trenutnog stanja ove oblasti.

Biometrijske sisteme za autentifikaciju treba proučavati u kontekstu njihovih društvenih implikacija, a ne samo kroz pitanja tehničke izvodljivosti i promenljivosti. To podrazumeva multidisciplinarni pristup koji pre svega obuhvata etičke, informatičke, pravne i sociološke discipline. Kriptografija, kao naučna disciplina je dala odgovore na zahtev za privatnosti u nekom aspektu korišćenja biometrijskih podataka. Na žalost, odgovori nisu sveobuhvatni. Distantna biometrija će morati biti regulisana zakonski, kao i uključivanje drugih, novih tehnologija.

5.2. BIOMETRIJSKI SERVISI ZA AUTENTIFIKACIJU

Konvencionalna kriptografija za šifrovanje koristi kriptološke ključeve. Ključ predstavlja binarnu sekvencu tačno određene dužine, obično 128, 192, 256 bitova ili više. Ovi ključevi mogu biti simetrični, javni ili privatni, i predstavljaju suštinski deo svakog kriptografskog sistema. Na primer, infrastruktura sa javnim ključevima - *PKI*. Ključevi koji se koriste u javnoj kriptografiji su velike dužine, obično 1024 ili 2048 bitova. Ljudi ne mogu da pamte ovako duge ključeve, kao što je to slučaj sa tradicionalnim lozinkama. Ovakvi ključevi često su zaštićeni lozinkama ili *PIN*-om koji se pamti. Upravljanje lozinkama je najslabija tačka svakog kripto sistema iz razloga što lozinka može biti ukradena, izgubljena ili pogođena primenom metoda za potpunu pretragu (engl. *Brute force*).

Biometrijski sistem za prepoznavanje uvek proizvodi jedan odgovor „DA“ ili „NE“, a to je samo jedan bit informacije. Dakle, očigledna je uloga biometrije u konvencionalnim kriptosistemima, a to je uloga upravljanja lozinkama. U procesu prepoznavanja, nakon faze verifikacije ukoliko je odgovor „DA“, sistem otključava lozinku ili ključ. Ključ mora da se čuva na sigurnom mestu ili uređaju od poverenja.

Interakcija između biometrije i kriptografije predstavlja dve potencijalne komplementarne tehnologije. Postoje različiti biometrijski izvori koji sadrže jedinstvene informacije u vidu ličnih karakteristika jedne osobe. Na ovoj pretpostavci može biti izgrađen napredni sistem za autentifikaciju pojedinca sa visokim stepenom sigurnosti. Na primer, čvrstom kombinacijom biometrije i kriptografije moguće je potencijalno ostvariti jaku vezu između digitalnog potpisa i osobe koja ga je sačinila sa visokim stepenom sigurnosti.

Međutim, postoje neizostavni tehnološki izazovi na koje je potrebno odgovoriti, a to su tačnost, pouzdanost, sigurnost podataka, prihvatljivost, cena, interoperabilnost, kao i izazovi vezani za obezbeđenje efikasne zaštite privatnosti. Sve ovo predstavlja uobičajenu ranjivost odnosno nedostatak biometrijskih sistema sa aspekta društvene prihvatljivosti. Biometrijske tehnologije stavljene u kontekst kriptografskih mehanizama, predstavljaju grupu povezanih tehnologija preko kojih je moguće na potpuno siguran način generisati kriptološki ključ na osnovu biometrijskih podataka.

Autentifikacija ili provera legitimnosti korisnika je sastavni deo opšte bezbednosti svih informacionih sistema. Tradicionalno, autorizacija korisnika znači uvođenje korisničkog imena i lozinke, a to je tehnika koja je u upotrebi već decenijama. Napravljene su mnoge inkrementalne promene na ovom polju, a izdvajamo samo osnovne. Lozinke se više ne šalju u otvorenoj formi preko mreže i postavljen je zahtev se generisanje jačih lozinki, ali se i dalje, osnovni pristup, u suštini, nije promenio. Slabosti ovog pristupa su dobro poznate i zbog njih su prisutni problemi na svakodnevnom nivou.

Za većinu poslovnih okruženja potencijalne pretnje uključuju:

- napad na privatnost, u kojem pojedinci neovlašćeno pristupaju tuđim privatnim podacima;
- napad na poslovne tajne, način na koji pojedinci kompromituju neku organizaciju, tako što joj nanose ogromne finansijske gubitke;
- napad sa ciljem zloupotrebe, u kojima pojedinac neovlašćeno raspolaže sa tuđim podacima, tj. lažno se predstavlja (krađa identiteta);

Sa druge strane, kriptografski mehanizmi koji obezbeđuju servis poverljivosti, integriteta i neporecivosti zahtevaju kriptološke ključeve većih dužina zbog kontinualnog tehnološkog razvoja. Drugi problemi nastaju usled odabira sigurnog mesta za čuvanje ključeva i načina za distribuciju. Ovakve ključeve nije moguće zapamtiti i neophodno je koristiti različite hardverske *tokene* za skladištenje kriptoloških ključeva. Takođe, slabosti ovog pristupa za skladištenje ključeva su dobro poznate, ukoliko hardverski medijum bude kompromitovan na neki od ovih načina.

Biometrija je ponudila nove i bolje pristupe za autentifikaciju korisnika, kao i tehnike za obezbeđenje mnogih servisa savremene informacione bezbednosti. Obzirom da su tradicionalne lozinke najslabije karike u sistemu bezbednosti, biometrija predstavlja novu potencijalnu tehnologiju koja treba da bude brzo usvojena u cilju rešavanja problema na svim nivoima bezbednosti.

Autentifikacija na bazi biometrije obezbeđuje pogodnu i bezbednu proveru identiteta korisnika kako u lokalnom mrežnom okruženju, tako i preko Veba. Ukoliko je zahtevan viši nivo bezbednosti, na mreži je moguće koristiti biometriju samostalno ili u kombinaciji sa drugim akreditivima. Biometrijske sisteme je značajno

teže prevariti nego dosadašnje tradicionalne sisteme na bazi lozinki. Imajući u vidu raznolikost biometrijski izvora, moguće je izvršiti njihovu podelu prema kvalitetu, u odnosu na količinu informacija koje sadrže. U zavisnosti od količine informacija, moguće je generisati biometrijske ključeve za kriptografske potrebe. Osim primene za generisanje ključeva, biometrija nudi rešenja za čuvanje i skladištenje kriptoloških ključeva, kao i njihovu distribuciju.

Razvojem biometrijskih sistema i njihovom prvom tradicionalnom primenom, prepoznati su i prvi nedostaci. Nedostaci mogu biti različito okarakterisani i možemo da ih podelimo u dve osnovne kategorije. Prvu kategoriju čine svi nedostaci koji se odnose na lošu zaštitu privatnosti biometrijskih podataka, a koji su u direktnoj vezi sa osnovnim osobinama biometrijskih podataka (jedinственost, nezamenljivost, sadrže šum). Drugu kategoriju čine nedostaci koji su vezani za bezbednost sistema, kod kojih se biometrijski podaci koriste u svrhu autentifikacije.

Tradicionalni model primene biometrije irisa je praktično neprihvatljiv kada je u pitanju zaštita privatnosti i nije u skladu sa drugim aspektima bezbednosti. Iako biometrijski obrasci mogu biti šifrovani, to nije dovoljno dobro rešenje za bezbednost biometrijskih podataka. Jer, ukoliko se dogodi da baza podataka bude kompromitovana, biometrijski podaci će biti izgubljeni zauvek. Sa druge strane, biometrijski obrasci se ne nalaze uvek u šifrovanoj formi, zbog nemogućnosti obavljanja faze prepoznavanja u kojoj se vrši provera stepena poklapanja dva biometrijska obrasca. U momentu provere poklapanja, biometrijski podaci moraju da budu prisutni u dešifrovanoj formi.

Ukoliko je napad u ovoj fazi uspešno realizovan, napadač će posedovati odgovarajuću originalnu biometriju. Ponovljenim napadom, pristup sistemu je zagarantovan. Nastala situacija može da postane još teža, ukoliko je vlasnik izgubljene biometrije koristio biometriju za pristup u više različitih i nepovezanih servisa. Ovo predstavlja ozbiljan bezbednosni problem, a takođe može biti problem koji nosi određene pravne konsekvence.

Između biometrijskih podataka postoji velika varijabilnost, nezavisno od tipa biometrijskog izvora. Varijabilnost biometrijskih podataka nastaje skoro u svim fazama obrade biometrijskih podataka. Od momenta očitavanja, pa sve do faze za generisanje biometrijskih obrazaca. Biometrijski podaci poseduju šum zbog kojeg nije moguće dva puta očitati potpuno identičan biometrijski podatak, sa istog

biometrijskog izvora. Na primer, tehnika za prepoznavanje identiteta korisnika na osnovu biometrije lica sklona je visokom stepenu varijabilnosti zbog različitih spoljnih uticaja - osvetljenja i ugla pomeranja korisnika. Ovo je jedan od razloga zbog koga smo zamoljeni da ne koristimo sliku sa osmehom u ličnim dokumentima. Slično ovome, brojni faktori utiču na neefikasno izdvajanje konzistentne informacije i iz uzoraka biometrije prsta. Na osnovu analize osobina za različite tipove biometrija, utvrđeno je da iris oka sadrži najveću količinu informacija i najmanju varijabilnost, a sa druge strane odlikuje ga i visok stepen pouzdanosti i konzistentnosti.

Kao posledica varijabilnosti, sveže generisani biometrijski obrasci mogu biti u potpunoj suprotnosti sa uskladištenim referentnim biometrijskim obrascima. Kod biometrijskih sistema nije moguće postići tačnost poklapanja dve biometrije od 100%. Kada biometrijski sistem nije u stanju da potvrdi visok stepen sličnosti u fazi prepoznavanja, prinuđen je da odbaci legitimnog korisnika. Ovakav događaj naziva se „lažno odbacivanje“ (engl. *False Rejected Rate*) od strane sistema u fazi prepoznavanja. Ukoliko se dogodi ovakav slučaj, korisnik je prinuđen da ponovi postupak iz početka.

Biometrijski sistemi za prepoznavanje mogu biti dizajnirani tako da se stopa lažnog odbacivanja smanji i da prepoznavanje bude uspešno, što će omogućiti pravilno funkcionisanje sistema i obezbediti njegovu društvenu prihvatljivost. Standardne metode za poboljšanje rada sistema za prepoznavanje su dodatno kontrolisanje uslova u kojima se očitavaju izvori biometrijskih podataka, kao i optimizacija matematičkih algoritama. Jedan od načina da se to uradi, jeste da se smanji prag ili granica za prihvatanje - *FRR*. Postoje problemi sa ovim pristupom jer direktno utičemo na stopu „lažnog prihvatanja“ (engl. *False Acceptance Rate*), a taj događaj bi značio da je sistem napravio grešku kod identifikacije i prihvatio pogrešnu osobu na bazi tuđeg referentnog biometrijskog obrasca.

Imajući u vidu da je moguće smanjenje jednog parametra na račun drugog i obrnuto, neophodno je napraviti kompromis između njih, tako da sistem bude prilagođen okruženju. Neka okruženja dozvoljavaju visok *FRR*, dok druga mogu tolerisati visok *FAR*.

Vrednosti parametara *FAR* i *FRR* koje su navedene od strane prodavca sistema za prepoznavanje, na osnovu biometrijskih podataka, često su nepouz dane. Iz tog

razloga, neophodno je konsultovati nezavisne izvore informacija, kao što su javna takmičenja na polju biometrijskih istraživanja u organizaciji američkog Nacionalnog instituta za standarde (*NIST*). Za većinu biometrijskih sistema, vrednost *FRR* kreće od 0.1 % do 20 %, što znači da će legitimni korisnik biti odbijen najmanje jednom od 1000 puta. *FAR* kreće od jednog prihvaćenog u 100 (aplikacije niskog stepena sigurnosti) i jednog prihvaćenog u 10.000.000 (aplikacije visokog stepena sigurnosti). Drugi izazov kod biometrijskih sistema je brzina prepoznavanja. Sistem mora da bude sposoban da napravi preciznu odluku u realnom vremenu. Sa druge strane, najbitnija sposobnost biometrijskih sistema koju bi trebalo da poseduju je otpornost na učestale napade.



5.3. BIOMETRIJSKI SISTEMI ZA GENERISANJE KLJUČEVA

Tehnološki razvoj Interneta i globalnih komunikacionih mreža stavio je u prvi plan pitanje sigurnosti i integritet prenesenih i memorisanih informacija. U istu kategoriju spada i pitanje pouzdanih metoda autentifikacije učesnika globalne mreže. Mehanizmi zaštite koji se baziraju na principu računarske složenosti potrebne za njihovo probijanje, sve više otvaraju prostor ka informaciono-teorijskim kriterijumima sigurnosti koji jasno definišu potrebne i dovoljne uslove za takozvanu bezuslovnu sigurnost. Sistemi sa ovim svojstvom su invarijantni na računarsku moć protivnika. Teorijski rezultati u poslednjih desetak godina ostvaruju solidnu osnovu za praktičnu realizaciju pojedinih segmenata bezbednosnih servisa, npr. tajnosti koji bi u dobroj meri posedovali ovo poželjno svojstvo.

Polazna tačka istraživanja su teorijske osnove i Šenonov koncept savršenih šifarskih sistema. Teorijsko informaciona analiza biometrije, kao svojevrsnog informacionog izvora, davala bi konkretna rešenja za sintezu kriptografskog sistema sa teorijski garantovanim performansama. Performanse biometrijskih kriptosistema zasnivaju se na nominovanoj sigurnosti koja zahteva pažljiv i kompletan opis operacionog scenarija u kome se egzaktno proučava:

- Od kakvih napada kriptografski sistem treba da obezbedi zaštitu?
- Šta je poznato napadaču?
- Šta je poznato korisnicima sistema?
- Koje su fizičke pretpostavke koje bliže određuju šta napadač i korisnici mogu da urade?

Problem istraživanja predstavlja kompleksan način obrade biometrijskih podataka. Biometrijski podaci sadrže šum koji znatno povećava varijabilnost podataka i tako utiče na informacioni kvalitet jednog biometrijskog uzorka. Problemi ovakve vrste mogu da se prevaziđu upotrebom odgovarajućih tehnika za obradu signala i kodova za ispravljanje grešaka. Atraktivne osobine jedinstvenosti stavljaju biometriju na prvo mesto, ali sa druge strane pojavljuju se i brojne slabosti. Za razliku od lozinki, jednom izgubljena ili kompromitovana biometrija ne može ponovo da se koristi, niti zameni sa nekom drugom biometrijskom informacijom. Na osnovu ovih činjenica može se zaključiti da je biometrija ograničen resurs.

Biometrijski sistemi moraju da odgovore na problem skladištenja i sigurne komunikacije između aplikacija u kojima se biometrija koristi. Imajući u vidu navedene slabosti i zahtevane uslove korišćenja, potrebno je analizirati različite scenarije generisanja kriptoloških ključeva iz biometrijskih uzoraka.

Postoje različiti biometrijski izvori koji sadrže jedinstvene informacije o ličnim karakteristikama jedne osobe. Iris kao biometrijski podatak sadrži dovoljnu količinu informacija za razvoj jedne klase sistema za generisanje kriptoloških ključeva, dovoljnih dužina za potrebe današnjih kriptografskih mehanizama, sa visokim stepenom bezbednosti.

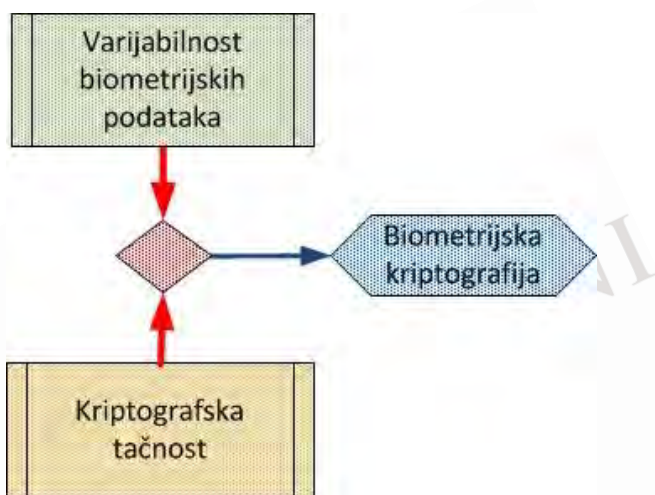
Zaključke koje možemo da izvedemo:

1. Biometrijski podaci su jedinstveni i predstavljaju dobru polaznu osnovu za sintezu optimizovanog sistema za ekstrakciju kriptoloških ključeva visokog kvaliteta;
2. Uvođenjem informacionih mera, entropije, lokalne entropije i uzajamne informacije, moguće je identifikovati segmente u biometriji irisa koji su najpogodniji za proces generisanja kriptoloških ključeva;
3. Optimizacijom parametara odgovarajuće transformacione funkcije, očekuje se veća entropija i manje uzajamne informacije u transformacionom domenu, čime su postavljeni okviri za sintezu sistema za ekstrakciju čisto slučajnih nizova iz biometrije irisa;
4. Biometrija iz istih biometrijskih izvora se ne reprezentuje uvek na isti način zbog prisustva šuma u biometrijskim podacima, te je neophodno projektovati tolerantnu šemu za nastale greške;
5. Biometrijski izvor i biometrijske podatke moguće je posmatrati i okarakterisati kao komunikacioni kanal sa šumom, što uvodi u upotrebu široku paletu tehnika za obradu signala iz oblasti digitalnih komunikacija;

5.3.1. BIOMETRIJSKA KRIPTOGRAFIJA

Originalni koncept „biometrijske kriptografije“ je primenjen nad otiscima prstiju 1994. god. Pionir u ovoj oblasti bio je dr. Džordž Tomko (*dr. George Tomko*), osnivač (*Mytec technologies*) Toronto, Kanada. Od tada mnoge istraživačke grupe su učestvovala u razvoju ove oblasti kao i drugih srodnih tehnologija. Pored naziva

biometrijska kriptografija (engl. *Biometric Encryption*), korišćeni su i drugi nazivi za ovu tehnologiju, kao što su: biometrijski kripto sistemi (engl. *biometric cryptosystem*), privatni obrasci (engl. *private template*), biometrijsko zaključavanje (engl. *biometric locking*), sigurna skica (engl. *secure sketch*), biometrijsko vezivanje ključeva (engl. *fuzzy commitment scheme, fuzzy vault*), biometrijsko generisanje ključeva (engl. *biometric key generation*), virtuelni PIN (engl. *virtual PIN*), biometrijski potpis (engl. *biometric signature*) i biometrijsko hešovanje (engl. *bioHashing*).



Slika 5.8 Izvor biometrijske kriptografije

Biometrijska kriptografija može da se definiše, u osnovi, kao proces koji koristi PIN, lozinku ili kriptološki ključ u kombinaciji sa biometrijskim podacima, na takav način da originalni biometrijski podaci, niti ključ ne mogu biti otkriveni ili regenerisani na osnovu referentnog podatka koji je predviđen za skladištenje. Ovo bi značilo da je moguće sa posebno dizajniranim algoritmima ponoviti ili regenerisati originalni ključ sa novim biometrijskim obrascem bez skladištenja prvog generisanog biometrijskog obrasca u početnoj fazi generisanja biometrijskog ključa. Dva biometrijska obrasca ne moraju da budu identična. Važno je da oba obrasca potiču od istog biometrijskog izvora da bi bilo moguće regenerisati ključ. Korišćenjem ove tehnike moguće je napraviti određen kompromis između biometrijske varijabilnosti i zahtevane kriptografske preciznosti (Slika 5.8).

Biometrijska kriptografija i srodne tehnologije su stvorile interesovanje glavnih akademskih istraživačkih centara specijalizovanih za biometriju poput državnog Univerziteta Mičigen, Univerziteta u Virdžiniji, Univerziteta Karnegi Melon u Kembridžu (Velika Britanija) i Univerziteta u Bolonji (Italija). Među sadašnjim liderima u industriji nalaze se *IBM (T.J. Watson Research Center)*, (*RSA Laboratories*), (*Lucent Technologies*), (*Sandia National Laboratories*) i (*Philips Research*).

Primenom tehnologije za biometrijsku kriptografiju postignut je ogroman potencijal za poboljšanje privatnosti i informacione bezbednosti. Ključne prednosti, kao i značaj ove tehnologije su navedene u nastavku.

Kod biometrijskih sistema strogo je zabranjeno čuvanje biometrijskih obrazaca u bazama podataka. Ovo je regulisano zakonima za zaštitu privatnosti kod upotrebe biometrijskih sistema. Zahtevana je minimizacija podataka, preko koje se smanjuje količina ličnih podataka. Ovo je postignuto generisanjem nezavisnih referentnih podataka koji ne odaju originalne biometrijske podatke. Bezbednosni problemi više su prisutni na strani baza podataka za skladištenje biometrije, zbog straha od zloupotrebe (krađa, presretanje, zamene i drugo).

Biometrijska kriptografija omogućava korisnicima višestruku upotrebu biometrijskih obrazaca. Ukoliko je jedan nalog kompromitovan, značajno su smanjene šanse za kompromitovanje drugih naloga za pristup drugim servisima. Sa druge strane, obezbeđena je mogućnost ponovnog generisanja na osnovu originalne biometrije, kao i povlačenje referentnih podataka iz upotrebe. Tradicionalni biometrijski sistemi ne poseduju navedene mogućnosti.

Povećana je bezbednost kod servisa autentifikacije, tako što je ostvarena čvrsta veza između autentifikatora (korisnika) i korisničkog naloga za pristup određenom servisu. Obezbeđena je zaštita lozinki i ključeva kreiranjem referentnih podataka. U momentu predstavljanja lozinke ili ključa, zahtevana je originalna biometrija i referentni podatak. Napadač nema mogućnost da dobije ključ na osnovu referentnog podatka, kao ni informaciju o biometriji korisnika servisa.

Biometrijska kriptografija povećava bezbednost ličnih podataka i komunikacija. Korisnici sistema za biometrijsku kriptografiju mogu da iskoriste pogodnost i jednostavnost date tehnologije za kriptografsku zaštitu ličnih podataka. Obzirom

da je priroda izvora ključa lična i na strani pojedinca, ova činjenica predstavlja moćan alat za široku primenu kriptografske zaštite.

Biometrijskom kriptografijom se stiče javno poverenje koje je neophodno za uspeh svakog biometrijskog sistema. Politika upravljanja podacima i procedure mogu da idu daleko onoliko koliko se neguje poverenje u javnosti. Biometrijski sistem mora da obezbedi elemente privatnosti, poverenja i bezbednosti. Ovo su ključni elementi koji utiču na njegovu prihvatljivost. To znači da biometrijski podaci moraju da budu stavljeni pod isključivu kontrolom pojedinca, kao i da je obezbeđen visok nivo zaštite privatnosti i podataka.

5.3.2. RAZVOJ SISTEMA ZASNOVANIH NA BIOMETRIJSKOJ KRIPTOGRAFIJI

Praktično sve vrste biometrija (otisak prsta, iris, lice, dinamika kucanja, glas, svojeručni potpis i druge) su testirane preko tehnike za generisanje ključa, na osnovu biometrije (zaključavanje ključa biometrijskim obrascem) ili tehnikom koja obezbeđuje generisanje ključa iz biometrijskih podataka (primena ekstraktorskih funkcija). Najbolji rezultat, takoreći najperspektivniji rezultat postignut je sa iris biometrijom sa *FRR* parametrom od 0,47% i *FAR* parametrom od 0% za generisanje kriptološkog ključa dužine 140 bitova. Ove greške su neznatno veće kod konvencionalnih biometrijskih sistema za prepoznavanje. Upotreba otiska prsta je takođe moguća u pogledu tačnosti za biometrijsku kriptografiju sa *FRR* parametrom većim od 10%, ali za razliku od irisa postoji primetna degradacija tačnosti biometrijskog sistema za otiske prstiju.

Treća biometrija, posle irisa i otiska prsta, jeste lice. Poslednjih godina napravljena su primetna poboljšanja kod biometrijskih sistema za prepoznavanje, na osnovu lica sa aspekta performansi sistema. Očekivani *FRR* parametar je 3,5%, parametar *FAR* je 0. Ovim sistemom moguće je generisati ključ dužine 56 bitova. Postignut je dovoljno dobar rezultat koji omogućava izbacivanje tradicionalnih lozinki iz upotrebe.

Nije poznato da li drugi biometrijski izvori poseduju dovoljnu količinu informacija za generisanje ključa minimalne dužine od 128 bitova. U ovom slučaju, entropija je mera koja se koristi za postavljanje teorijskih okvira za dužinu kriptoloških

ključeva. Entropiju možemo definisati kao neredundantnu informaciju koja je sadržana u biometrijskim izvorima. Ova mera je od velike važnosti jer su na njoj zasnovani kriptografski principi koji garantuju nivo bezbednosti kriptografskih mehanizama. Teorijski sada možemo da kažemo da dužina ključa ne sme da prelazi ukupnu količinu informacija koju poseduje biometrijski izvor, a predstavljeno je preko entropije, gde se za jedinicu informacije koristi 1 bit.

Radovi koji su objavljivani od 2001. godine daju opštu teorijsku osnovu za tehnologije biometrijske kriptografije, sa kriptografske tačke gledišta. U njima se dokazuje da sistem može biti tako dizajniran da bude otporan na kriptoanalitičke metode, čak i na metod potpune pretrage. U ovom slučaju napadač mora da isproba sve moguće kombinacije, kako bi uspeo da otkrije ključ ili biometrijski obrazac, čime bi sistem bio bezbedan u odnosu na dostupnu tehnologiju. U ovom dokazu se pretpostavlja, isto kao kod konvencionalne kriptografije, da je algoritam javan, a da napadač kod sebe može posedovati biometrijski obrazac koji nije odgovarajući sa nijednim referentnim podatkom u bazi podataka.

Međutim, napadač bi mogao da pokuša da izvede sofisticiranije napade, tako što bi iskoristio nasledne slabosti. Nasledne slabosti možemo tumačiti kao uzajamnu informaciju ili zavisnost koja postoji između dva biometrijska podataka ili između dva referentna biometrijska podatka koja u sebi sadrže zaključan ključ i originalni biometrijski obrazac. Istraživanje na polju informacione analize je u velikoj meri zanemareno. Ako bi ovakav napad bio uspešan, efikasna sigurnost sistema sa 140 bitova, bila bi smanjena na 70 ili 50 bitova. U cilju određivanja efikasnije sigurnosti sistema, smatramo da je neophodno sprovesti detaljnu informacionu analizu nad podacima koji učestvuju u šemi za tehnologije biometrijske kriptografije.

5.3.3. GENERISANJE KLJUČEVA IZ BIOMETRIJE

U ovom delu rada napravićemo pregled prvih tehnika za generisanje kriptoloških ključeva iz biometrijskih podataka. Tehnika obezbeđuje zaštitu privatnosti biometrijskih podataka, opoziv, kao i mogućnost ponovnog generisanja javnih biometrijskih podataka za primenu kod sistema za autentifikaciju, kriptografsku zaštitu podataka, digitalno potpisivanje i druge kriptografske aplikacije. Sigur-

nost kod ovih aplikacija obezbeđuju bešumni, slučajni, uniformni nizovi u ulozi kriptoloških ključeva.

Kriptografija se tradicionalno oslanja na ravnomerno raspoređene i precizno ponovljive slučajne nizove u ulozi tajne ili kriptološkog ključa. Realnost međutim otežava generisanje, čuvanje i pouzdano preuzimanje takvih slučajnih nizova. Uglavnom ti nizovi nisu sa uniformnom ili ravnomernom raspodelom, a još teže su precizno ponovljivi, kada se to zahteva. Na primer, nizovi koji proizlaze iz obrađene zenice oka ili irisa, nisu sa uniformnom distribucijom, niti se precizno očitavaju svaki put kada se iznova generiše obrazac irisa.

Da bi ilustrovali upotrebu slučajnih nizova za autentifikaciju, na jednostavnom primeru ćemo razmotriti upotrebu lozinke za svrhu autentifikacije. Korisnik želi sa svojom lozinkom L da pristupi svom korisničkom nalogu. Servis koji autentifikuje korisnika, poseduje informaciju $y = f(L)$. Kada korisnik priloži lozinku L , servis računa $f(L) = y'$. Ukoliko su vrednosti y i y' jednake, proces autentifikacije biće uspešan. U ovom slučaju pretpostavićemo da je ovo siguran način za verifikaciju korisnika. Sigurnost sistema je zasnovana na neinvertibilnosti funkcije $f(L)$. Ovakve funkcije nazivaju se jednosmerne funkcije ili jednosmerne funkcije (engl. *one-way functions*).

Nažalost, ovo rešenje poseduje nekoliko problema kada se koristi lozinka L u realnom životu. Prvo, definicija jednosmernih funkcija podrazumeva da je L generisano na slučajan način sa uniformnom distribucijom. U našem slučaju, biometrijski podaci u ulozi lozinke su daleko od uniformne distribucije. Drugo, tradicionalna lozinka je precizno ponovljiva svaki put kada se koristi za autentifikaciju, dok to nije slučaj sa biometrijskim podacima. Sa druge strane, tradicionalna upotreba lozinke obezbeđuje relativno nizak nivo sigurnosti, jer je čovek u stanju da zapamti relativno kratke lozinke. Visok nivo sigurnosti moguće je jedino obezbediti sa upotrebom biometrijskih lozinke. Ove lozinke mogu biti generisane na osnovu biometrijskih podataka kao što je biometrija prsta, irisa, glasa, geometrija dlana ili još bolje kombinacijom više biometrijskih izvora podataka. Biometrijski podaci sadrže neuporedivo veću količinu informacija nego tradicionalne lozinke koje su predviđene za pamćenje. Osnovni problem biometrijskih podataka je varijabilnost koja postoji u signalima, nakon očitavanja biometrijskih podataka iz dva identična biometrijska izvora. Drugim rečima, potrebna je mogućnost da se tole-

riše ograničen broj grešaka, zadržavajući sigurnost na visokom nivou, za razliku od nivoa sigurnosti koji je postignut upotrebom kratkih lozinki.

Autentifikacija lozinkama, o kojoj smo već diskutovali, je jedan jednostavan primer kriptografske aplikacije gde se postavljaju pitanja uniformnosti i tolerancije na grešku kod biometrijskih podataka. Ostali primeri primene uključuju mnoge kriptografske aplikacije, algoritme za šifrovanje i dešifrovanje, digitalni potpis ili identifikaciju, gde kriptološki ključ koji se koristi potiče ili proizilazi iz neuniformnih signala sa šumom.

Važan i opšti problem je proces konvertovanja neuniformnih biometrijskih podataka sa šumom u čisto slučajne uniformne nizove sa maksimalnom entropijom. Entropiju koju navodimo, odnosi se na entropiju binarnih informacionih izvora koju definišemo kao meru neodređenosti nekog sistema ili kao prosečnu količinu informacije koja je sadržana u jednom bitu. Opšta ideja je zasnovana na dva koraka. Ekstraktujuća funkcija konvertuje biometrijske podatke u slučajne nizove sa uniformnom distribucijom koje je moguće koristiti u različitim kriptografskim aplikacijama za zaštitu podataka. U poslednjem koraku funkcija generiše javnu informaciju (engl. *Secure sketch*) koja se koristi za rekonstrukciju potpuno istih privatnih (tajnih) nizova u prisustvu biometrijskih obrazaca, dovoljno blizu aproksimacije originalnih biometrijskih podataka.

Predložena je funkciju pod nazivom „*Fuzzy extractors*”. Funkcija ima osnovni zadatak da pretvara neuniformni slučajni podatak minimalne entropije u slučajni podatak sa uniformnom distribucijom i visokom entropijom.

Zatim predloženo su šeme koje obezbeđuje generisanje više ključeva za primenu u različitim aplikacijama. Modifikovana je postojeća „*Fuzzy extractor*” šema, tako što je korišćena fiksna i jedinstvena permutacija nad obrascem irisa u fazi generisanja ključa. Kompromitovanjem jednog ključa koji je generisan iz biometrije jednog pojedinca, neće dovesti u pitanje ostale ključeve koji su izvedeni iz biometrije od istog pojedinca. U revidiranom dizajnu predložene šeme, ostaje pretpostavka da originalni biometrijski podaci ostaju tajna ili da neće biti kompromitovani.

Takođe, drugi teorijski radovi se bave ekstraktovanjem ključa iz biometrijskih podataka sa šumom. U datom predlogu, autori primenjuju kodove za ispravljanje

grešaka za ulazni signal, a zatim i *heš* funkcije. Dokazano je da je količina curenja informacija o ulaznim podacima zanemarljiva u odnosu na analizu izlaznih podataka. Ova vrsta pristupa može biti korisna samo ako se biometrijski podaci sa šumom čuvaju u tajnosti. Međutim, problem biometrijskih podataka je što ih ljudi ostavljaju svuda oko sebe ili mogu biti ukradeni. U ovom slučaju, biometrijski podatak u rukama napadača otkrio bi mnogo o entropiji ključa.

Kasnije su identifikovane potencijalne ranjivosti kod postojećih biometrijskih sistema na bazi *Fuzzy* ekstraktora. Predstavili su šemu za zaštitu glavnog biometrijskog obrasca, kao i načine kako da se obezbedi zaštita biometrijskih obrazaca u odnosu na glavne karakteristike *Fuzzy* ekstraktor šeme za dati iris obrazac.

Definicije koje smo naveli do sada su formalne, kao i efikasne tehnike za pretvaranje biometrijskih podataka u kvalitetnu informaciju koja bi obezbedila pouzdanu i bezbednu autentifikaciju na osnovu biometrijskih podataka, kao i primenu kod bilo koje kriptografske aplikacije. Opisana tehnika nije ograničena samo na primenu nad biometrijskim podacima, već može biti upotrebljena i za druge podatke koji su namenjeni za generisanje kriptoloških ključeva. Na osnovu bezbednosnih analiza koje su sprovedene u više preglednih radova, potencijalno je moguća dokazana sigurnost za predloženu šemu, samo ukoliko postoji pretpostavka da originalni biometrijski podaci ostaju tajna ili da neće biti ukradeni ili kompromitovani. U svim drugim slučajevima, napadač bi mogao da ima neke informacije o ključu, a to dalje ukazuje na postojanu mogućnost curenja informacija iz javnih podataka koji su predloženi ovom šemom.

5.3.4. GENERISANJE KLJUČEVA NA OSNOVU BIOMETRIJE

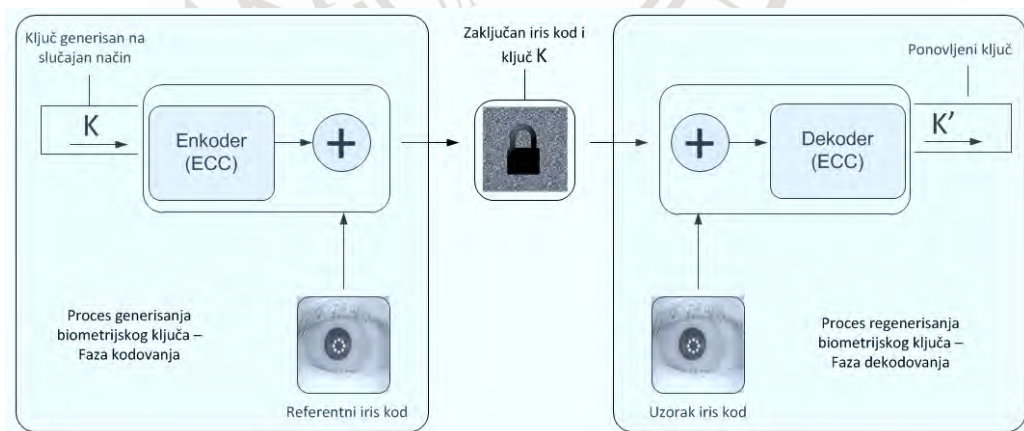
U ovom odeljku napravljen je pregled tehnika za generisanje kriptoloških ključeva na osnovu biometrijskih podataka. Za razliku od prethodne tehnike koja je navedena, kriptološki ključevi se generišu iz biometrijskih podataka. Ova nova tehnika takođe obezbeđuje zaštitu privatnosti biometrijskih podataka, opoziv, kao i mogućnost ponovnog generisanja kriptoloških ključeva za autentifikaciju, kriptografsku zaštitu podataka, digitalno potpisivanje i druge kriptografske aplikacije. Neki autori radova su pokušali da unutar biometrijskih podataka ugrade jedinstvene i ponovljive binarne nizove koji dalje imaju ulogu kriptološkog ključa. Ova tehnika omogućava ponovno regenerisanje ključa koji je u fazi upisa ugrađen

u referentni podatak. Ostvareni doprinos preko ove tehnike je od izuzetnog značaja, iz razloga što je kriptografija konvencijalna nauka i zahteva istu tačnost koja postoji kod kriptoloških mehanizama.

Biometrijsko šifrovanje je adekvatan naziv ovog metoda koji predstavlja proces u kome se čvrsto vezuje kriptološki ključ za biometrijski obrazac (podatak). Suštinski, ključ je šifrovan sa biometrijskim podatkom primenom logičke operacije za sabiranje (engl. *XOR*), a rezultat je biometrijski kodovani ključ koji predstavlja javnu informaciju ili pomoćni podatak. Formom pomoćnog podatka obezbeđena je zaštita privatnosti, kao i sigurnost ugrađenih kriptoloških ključeva. Pomoćni podaci mogu da budu sačuvani na nekom memorijskom prostoru, bez bezbednosnih rizika.

Kriptološki ključ moguće je ponoviti ili regenerisati ponovljenom operacijom (*XOR*), na osnovu pomoćnog podatka sa odgovarajućim predloženim biometrijskim obrascem koji je generisan u fazi verifikacije (engl. *Decommitted*).

Proces šifrovanja i dešifrovanja je prirodno konfuzan, iz razloga što je biometrijski podatak svaki put različit, za razliku od konvencijalnih metoda u kriptografiji. Imajući u vidu varijabilnosti u biometrijskim podacima, veliki je tehnološki izazov da ključ bude svaki put precizno ponovljen ili identičan. Na slici (Slika 5.9) predstavljena je generička šema visokog nivoa za generisanje biometrijskih ključeva.



Slika 5.9 Šema za generisanje biometrijskog ključa

Posle procesa verifikacije ili oporavka ključa, ključ se može koristiti kod bilo kog tipa kriptografskih aplikacija, gde se ključ koristi kao lozinka ili može da služi za generisanje simetričnih ili asimetričnih ključeva. Bitno je istaći da biometrijsko šifrovanje nije samo po sebi kriptografski algoritam. Uloga biometrijskog šifrovanja je da zameni ili da osigura bezbednost kod postojećih šema za autentifikaciju, koje su bazirane na tradicionalnim lozinkama.

Biometrijsko šifrovanje ne treba mešati sa sistemima za šifrovanje biometrijskih podataka ili sa zaštitom biometrijskih obrazaca kriptografskim metodama za potrebe skladištenja, ili sa načinima za skladištenje kriptoloških ključeva na *smart* karticama ili drugim memorijskim *tokenima*, preko kojih je ključ oslobođen nakon uspešne verifikacije.

Međutim, metod za biometrijsko šifrovanje nalazi se u familijarnom odnosu sa metodom poznatim pod nazivom (engl. *Cancelable Biometrics*). Ovaj metod predstavlja prvi metod koji obezbeđuje opoziv biometrijskog obrasca, odnosno izdavanje novog ukoliko je postojeći kompromitovan ili je potreban novi za upotrebu u drugim aplikacijama. Priroda biometrijskih sistema nije takva da originalni biometrijski podaci mogu biti promenjeni sa drugim biometrijskim podacima. Na primer, ukoliko neko snimi biometriju našeg prsta, lica ili irisa, ne postoji mogućnost generisanja nove biometrije.

Postoje dva osnovna pristupa za generisanje kriptoloških ključeva. U prvom slučaju, imamo potpuno nezavisno generisan ključ koji se čvrsto vezuje sa biometrijskim obrascem (engl. *Data binding*), a u drugom slučaju, kada ekstraktujemo ključ iz biometrijskog obrasca (engl. *Fuzzy extractor*). Kod oba pristupa su prisutni pomoćni podaci koji moraju biti negde skladišteni i od njih ovaj sistem zavisi.

Pomoćni podatak omogućava regenerisanje kriptološkog ključa u fazi verifikacije. Faza verifikacije podrazumeva primenu logičke operacije *XOR* između tog generisanog biometrijskog obrasca i pomoćnog podatka. Veličina prostora ključeva na pomoćnom podatku zavisi od stepena varijabilnosti biometrijskih obrazaca koji na ovaj način utiču na kapacitet kodova za ispravljanje grešaka i na ukupnu količinu neuzajmne informacije poređenjem različitih biometrijskih obrazaca.

U režimu vezivanja biometrijskog obrasca sa ključem, ključ je slučajno i nezavisno generisan tako da ni korisnik niti bilo ko drugi zna nešto o ključu. Nezavi-

snost ključa od biometrijskog podatka omogućava izmenu ukoliko je potrebno. Nakon generisanja biometrijskog podatka, algoritam na siguran način vezuje biometriju sa ključem i tako generiše biometrijski šifrovan ključ. Dobijeni pomoćni podaci obezbeđuju zaštitu privatnosti i mogu biti sačuvani u bazi podataka ili lokalno na *smart* karticama, računarima, *tokenu* ili mobilnom telefonu. Na kraju kompletne procedure (kada je generisan pomoćni podatak), ključ i biometrijski obrazac su uništeni na siguran način.

Osnovni metod je tako dizajniran da bude prihvatljiv za određenu količinu šuma kod ulaznih biometrijskih podataka. Ukoliko neko na nelegitiman način pokuša da regeneriše ključ, tako što koristi različit biometrijski obrazac od originalnog, algoritam neće biti u mogućnosti da ponovi isti ključ. Mnoge šeme za biometrijsko šifrovanje čuvaju *heš* vrednosti ključeva na mestima gde se dati ključevi skladište.

Nakon uspešne verifikacije, algoritam za dobijeni ključ računa *heš* vrednost na osnovu koje se proverava identičnost dobijenog ključa u isto vreme. U praksi, aplikacije koriste *heš* vrednosti za derivaciju ključeva. U ovom slučaju to nije moguće jer se originalna *heš* vrednost čuva na *tokenu*. Sa ovakvom arhitekturom obezbeđenja, napadač ne može da dobije originalni ključ izvan domena metoda za biometrijsko šifrovanje. U praktičnoj primeni biometrijska slika ne treba da bude poslata preko komunikacionog kanala do servera, već je verifikaciju bitno realizovati lokalno.

Neki autori predlažu novu šemu poznatu pod nazivom „*Fuzzy commitment scheme*”. Ova šema predstavlja metod za prikrivanje (engl. *Concealing*) biometrijskih podataka i šemu za uvezivanje podataka (engl. *Binding*). U konvencionalnoj šemi za otključavanje ovog tipa nastalog podatka neophodan je jedinstven identifikator, sličan kao što je kriptološki ključ kod algoritma za dešifrovanje. Karakteristike predložene šeme su vrlo primenjive kod aplikacija kao što su biometrijski sistemi za autentifikaciju, kod kojih biometrijski podaci sadrže šum. Šema je tolerantna na nastale greške, sposobna da zaštiti biometrijske podatke slično kao kriptografski mehanizmi zaštite, ili kao jednosmerne funkcije koje se koriste za zaštitu alfanumeričkih lozinki.

Neki autori predlažu sistem baziran na otisku prsta. Oni su prvi koji su komercijalizovali ovu tehnologiju u proizvod (www.biocrypt.com). Fazna informacija se

ekstraktuje sa slike otiska prsta, koristeći Furijeovu transformaciju i kodove za ispravljanje grešaka, da bi smanjili varijabilnost u biometrijskom signalu. Umesto da generišu ključ iz biometrijskih podataka, oni uvode metod biometrijskog zaključavanja. Zapravo, unapred određeni slučajni ključ se zaključava sa dobijenom faznom informacijom (biometrijski obrazac). Dobijeni rezultat moguće je jedino otključati sa originalnom biometrijom. U ovom radu prikazana je obećavajuća ideja o biometrijskom zaključavanju jer je ključ sada moguće definisati nasumično i nezavisno od sistema. Performanse predloženog sistema nisu date.

Neki autori u svom radu koriste svojeručni potpis. Definisali su 43 karakteristike koje mogu da ekstraktuju iz takve dinamične informacije, kao što su brzina, pritisak, nadmorska visina i azimut (pravac određen uglom u horizontalnoj ravni). Na osnovu svih pribavljenih vrednosti navedenih parametara, generiše se jedan konkatentni niz iz koga se funkcijom ekstraktuje informacija i rezultat je jedan binarni niz. Na ovaj način generisan je ključ sa entropijom od 40 bitova sa stopom lažnog odbacivanja *FRR* od 28% i stopom lažnog prihvatanja *FAR* negde oko 1,2%.

Neki autori kombinuju slične tehnike koje su gore navedene, projektuju sistem baziran na biometriji lica. Usvajaju metod biometrijskog zaključavanja. Uspeli su da regenerišu ključ sa entropijom od 80 bitova sa stopom lažnog odbacivanja *FRR* od 0,93%. Dobijene vrednosti parametara *FRR* predstavljaju najpribližnije očekivane vrednosti za praktičnu primenu sistema. Sistem je testiran na slikama lica. Slike su dobijene preko kontinualnog video signala, a ne na osnovu slika iz baze podataka. Postoje određene sumnje kod evaluacije ovog rada, iz razloga što u kontinualnom video signalu postoji nešto manja varijacija, nego što je u slikama iz baze podataka.

Neki autori predlažu šemu pod nazivom virtuelni *PIN*. Korišćen je Gabor filter za ekstrakciju informacionih sadržaja. Autori predlažu korišćenje (engl. *Low Density Parity Check*) zaštitnih kodova za ispravljanje grešaka. Evaluacija predloženog rešenja je urađena na neutvrđenoj bazi podataka.

Veoma sličan, ali više praktičan pristup je realizovan na biometriji otiska prsta, gde je za ekstrakciju informacionih sadržaja korišćen fazni Gaborov filtr. Neki autori izdvajaju konzistentne i pouzdane bitove informacija iz biometrije prsta koristeći *BCH* kodove za ispravljanje nastalih grešaka. Sprovedenom evaluacijom

u radu dobijaju sledeće rezultate, vrednost parametra *FRR* od 5,4% do 9,9% za ključ dužine 49 bitova i 85 bitova. Međutim, parametar *FAR* od 3,2% do 2,5% je relativno visoka vrednost u odnosu na postignutu dužinu ključa.

Neki autori su predstavili šemu za biometrijsku kriptografiju na osnovu biometrije lica. Generička šema je zasnovana na šemi čvrstog vezivanja biometrije sa nezavisno generisanim ključem. Sa ciljem poboljšanja tačnosti algoritma, autori ekstraktuju pouzdane i konzistentne bitove informacija iz biometrijskih uzoraka i primenjuju *BCH* kodove za ispravljanje grešaka. Rezultat koji su dobili relativno je dobar sa *FRR* parametrom od 3,5% za standardizovanu bazu podataka sa niskim i srednjim nivoom varijabilnosti kod slika i parametrom *FAR* od 0% u oba slučaja. Algoritam je kasnije implementiran u *Philips* sistem koji je nazvan "*privIDTM*".

Neki autori su predstavili bimodalni biometrijski sistem za generisanje kriptološkog ključa na osnovu biometrije glasa i signala elektrokardiograma - *EKG*. Jedinstveni informacioni sadržaj iz oba biometrijska izvora je ekstraktovan preko transformacione funkcije. Rad je zasnovan na jedinstvenom i kvazi stacionarnom ponašanju *EKG* signala i govornog signala koji predstavlja bihejvioralnu osobinu pojedinca. Sprovedenom evaluacijom u radu dobijeni su sledeći rezultati: vrednost parametra *FAR* od 1,27%, i vrednost parametra *FRR* od 10,62%.

Navedeni primeri predloženih šema generišu ključeve relativno manjih dužina i većina njih ima visoku stopu lažnog odbacivanja *FAR*, što se negativno odražava na društvenu prihvatljivost nekih rešenja. Na osnovu uvida u postignute rezultate, neki autori predlažu generičku šemu za generisanje ključeva na osnovu biometrije irisa preko koje su postigli dobre performanse koje obezbeđuju praktičnu primenu njihovog rešenja.

Iz tog razloga, u nastavku ćemo detaljno proći kroz kompletnu šemu algoritma predloženu u njihovom radu. Pre dizajniranja šeme za ispravljanje grešaka, prvo je urađena karakterizacija prisutnih grešaka u iris podatku. Nakon urađene analize, dobili su rezultate na osnovu kojih su izabrali adekvatne zaštitne kodove i optimizovali iste u odnosu na maksimalni dozvoljeni kapacitet za ispravljanje grešaka. Njihov algoritam prvo izdvaja 256 bajtova fazne informacije upotrebom 2D Gabor filtera. Uočeno je da postoje različiti tipovi grešaka u iris podatku. Klasifikacija je napravljena prema dva osnovna tipa grešaka. Prva klasa grešaka, pred-

stavlja pozadinske slučajne greške izazvane od strane *CCD* senzora kamere ili distorzije irisa koja je prouzrokovana promenom osvetljenja. Kako god, nastale greške nije moguće korigovati postojećim algoritmima za obradu signala. Druga klasa grešaka je u formi paketskih grešaka i nastaje zbog lošeg detektovanja trepavica, kapaka i refleksije. Osnovne ideje za primenu tehnika za kodovanje, predložene su u nekim ranijim radovima koje su korišćene za ispravljanje grešaka. Međutim, navedene tehnike ne rade dobro i na iris podatku, jer višestruko skeniranje ne smanjuje količinu greške. Utvrđeno je da na grupi slika od 70 korisnika bez korišćenja maske za pojedinačno skeniranje, stopa greške u proseku iznosi 13,69%, a nakon tri skeniranja stopa greške je smanjena na 10,68% i na 9,36% posle pet skeniranja. Da bi se izborili sa ovim tipom grešaka, autori u radu predlažu upotrebu konkatentnih kodova za ispravljanje grešaka. Za prvu klasu grešaka primenjuju Hadamardove kodove, a zatim na drugu klasu grešaka (paketske greške) primenjuju Rid-Solomon kodove. Kao spoljašnji sloj, koriste se Hadamardovi kodovi za ispravljanje slučajnih grešaka u binarnom podatku irisa, a za unutrašnji sloj Rid-Solomon kodovi za ispravljanje paketskih grešaka na blokovskom nivou.

U predloženoj šemi sa dva faktora ključ zavisi od kombinacije biometrije i *tokena*. Pretpostavlja se da napadač, ukoliko uspe da dođe u posed *tokena*, može imati potpuno znanje o podacima na njemu. Početni dizajn imao je za cilj da pokaže da ukoliko jedan faktor šeme bude kompromitovan, napadač neće imati mogućnost da regeneriše ključ. Kasnije u radu je pokazana mogućnost da se šema produži sa trećim faktorom, dodavanjem lozinke. Šema predstavlja mogućnost premošćivanja nekompatibilnosti koja postoji između varijabilnih biometrijskih podataka i konvencionalne kriptografije.

U prvoj fazi, generiše se nezavisno biometrijski ključ k kao slučajna binarna sekvenca. Ključ k poseduje sve osobine kriptoloških ključeva. Ključ k je tačno zadate dužine. U sledećoj fazi ključ k se koduje konkatentnim kodovima, čija je dužina na kraju faze kodovanja 2048 bitova. Kodovani ključ sa konkatentnim kodovima naziva se „pseudoiris kod“. Zatim kodovani ključ k ili pseudoiris kod se čvrsto vezuje logičkom operacijom XOR za biometriju irisa i tako dobijeni rezultat predstavlja pomoćni podatak koji se skladišti na nekom hardverskom *tokenu* zajedno sa heš vrednošću ključa k .

Nakon kompletnog procesa za upis ili generisanje biometrijskog ključa, neophodno je uništiti ključ na siguran način. Faza dekodovanja je potpuno inverzna fazi kodovanja. Korisnik podmeće originalnu biometriju irisa da bi otključao pseudoiris kod iz pomoćnog podatka, preko ponovljene logičke operacije XOR. Dalje sledi faza dekodovanja sa istim konkatentnim kodovima, samo u suprotnom redosledu od kodovanja. Da bismo potvrdili uspešnost čitave operacije, za dobijeni rezultat k' računa se heš vrednost preko koje se utvrđuje sličnost sa heš vrednošću koja se nalazi na *tokenu*.

Cilj koji je postignut, zasniva se na detaljnoj analizi obrasca greške u obrascu irisa. Iris kodovi (obrasci) od jednog oka obično se razlikuju od 10 – 20 % bitova, saopšteno od autora. Sa druge strane, razlika između dva irisa kod različitih osoba ili dva irisa iste osobe, iznosi 40 – 60 % bitova. Hadamardov kod je izabran za ispravljanje 25 % pogrešnih bitova, koji precizno razdvaja ispravljanje grešaka na biometrijskom uzorku istog i različitog oka.

Neki autori za spoljašnji sloj koriste Hadamardove kodove za ispravljanje slučajnih grešaka u biometrijskom obrascu irisa, a za unutrašnji sloj Rid-Solomon kodovi za ispravljanje paketskih grešaka na blokovskom nivou. Napravljene su određene izmene u šemi. Radi povećanja kapaciteta kodova za ispravljanje grešaka, uvedeni su redundantni bitovi (nule), sa uniformnom distribucijom, čime je dužina iris koda povećana za 40%. Uveden je metod mešanja iris obrasca za permutaciju koja je kontrolisana lozinkom, što je dalje uticalo na povećanje Hamingovog rastojanja između različitih irisa, kao i smanjenje rastojanja između istih irisa. Drugi doprinosi su izraženi preko povećanja entropije iris obrasca. Postignuta je dužina ključa od 186 bitova sa stopom lažnog odbacivanja FRR od 0,76% i stopom lažnog prihvatanja FAR od 0.096%. Sa aspekta bezbednosti, zaključani iris kod ne otkriva biometrijsku informaciju u slučaju kompromitovanja kriptološkog ključa, *smart* kartice i lozinke. Obezbeđena je mogućnost opoziva i mogućnost ponovnog generisanja biometrijskog ključa.

5.4. JEDAN ALGORITAM ZA GENERISANJE KRIPTOLOŠKIH KLJUČEVA NA OSNOVU BIOMETRIJE

U ovom odeljku data su uvodna razmatranja vezana za različite aspekte razvoja novog sistema za generisanje kriptoloških ključeva na osnovu biometrije irisa, kao i kompletan proces njegovog razvoja i integracije u standardne biometrijske sisteme. U poglavlju su date i komponente tradicionalnog biometrijskog sistema za prepoznavanje na osnovu irisa u kog će naš sistem biti integrisan, kao i izbor nosećih tehnologija napravljen na osnovu analize trenutnog stanja na polju biometrijske kriptografije i bezbednosti.

Na početku istraživanja, u ovom radu, imali smo utisak da su dostignuti maksimumi kod postojećih sistema za generisanje ključeva na osnovu biometrije, kao i da su dostignuti određeni nivoi stabilnosti i bezbednosti, koja je neophodna za njihovo korišćenje sa aspekta društvene prihvatljivosti. Međutim, nakon određenih testiranja aktuelnih rešenja, javila se sumnja da je teorijski maksimum ipak iznad postignutih praktičnih rezultata.

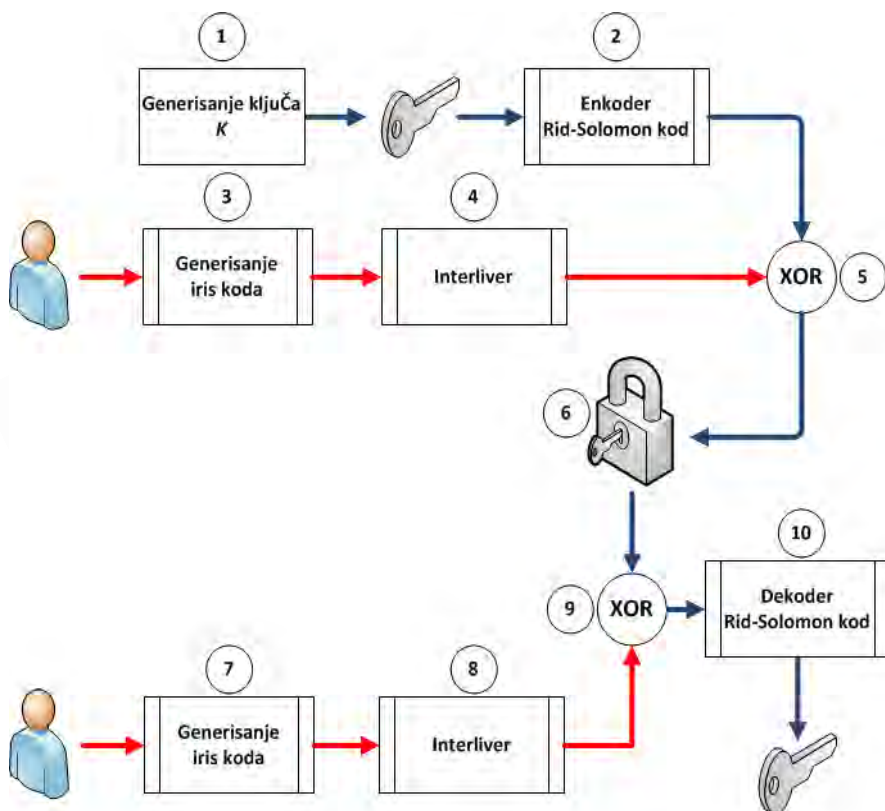
Daljim radom, potvrđene su sumnje i postavljeni su čvrsti ciljevi istraživanja da se podigne granica efikasnosti blizu teorijske granice. Nakon uvida u rezultate teorijsko-informacione analize, postavljeni su novi teorijski okviri sistema za sintezu kriptoloških ključeva, na osnovu biometrijskih podataka.

Osnovna motivacija ovog istraživanja, bila je potreba da se omogući razvoj profesionalne klase sistema za generisanje ključeva velikih dužina, tako da zadovolji potrebe savremenih kripto sistema, korišćenjem postojećih komponentata za kodovanje biometrijskih izvora koji obuhvataju kompletan proces, od izbora biometrije, preko slike do biometrijskih obrazaca.

U skladu sa tim, kao osnovni cilj postavljen je razvoj sopstvene klase sistema za generisanje kriptoloških ključeva na osnovu biometrije irisa. Za uspešno ostvarivanje ovog cilja bilo je neophodno sprovesti razne kontrole, kao i uraditi rigorozne informacione analize nad svim komponentama sistema u skladu sa kriptografskim pravilima i principima koje je bilo bitno ispoštovati. Kompleksnost savremenih kripto sistema, kao i potreba za kriptološkim ključevima većih dužina, učinile su rad na ovoj ideji izuzetno složenim i zahtevnim.

5.4.1. GENERIČKA ŠEMA ALGORITMA

Za sintezu jednog kompleksnog sistema neophodno je napraviti generičku šemu sa detaljnim opisima svih komponenti koje na direktan ili indirektan način učestvuju u svojstvu gradivnih komponenti ovog novog predloženog rešenja (Slika 5.10).



Slika 5.10 Generička šema predloženog rešenja

Na slici je predstavljena generička šema predloženog rešenja sa svim svojim pod-sistemima. Kompletan sistem sastoji se od dva podсистema: podсистem za kodoвање iris biometrijskog izvora koji je zasnovan na algoritmima tradicionalnih biometrijskih sistema i podсистemu za prenos poruka preko biometrijskog kanala sa šumom. U nastavku sledi detaljno objašnjenje pojedinačnih uloga svih navede-

nih komponenti koje su sadržane u ovom dijagramu procesa. Komponente su numerisane brojevima od 1 do 10.

Komponenta 1 - predstavlja proces u kom se generiše kriptološki ključ zadate veličine. Preporučeno je da ključ bude generisan na slučajan način preko informacionih izvora koje je moguće pronaći u prirodnim okruženjima. U drugom slučaju koji nije toliko popularan, moguće je ključ generisati i nekim pseudoslučajnim generatorom. Ovakav način generisanja ključa može da naruši bezbednost jednog simetričnog kripto sistema.

Komponenta 2 - predstavlja proces zaštitnog kodovanja za korekciju grešaka u kome se koriste Rid-Solomon kodovi. U ovom procesu kriptološki ključ K je kodovan Rid-Solomon koderom. Uloga ovog procesa je od suštinske važnosti za sistem, zapravo tehnika preuzeta iz polja komunikacija, na osnovu koje je nastala i čitava ideja o potpuno jednom novom naučnom istraživačkom polju pod nazivom "biometrijska kriptografija".

Komponenta 3 - predstavlja proces generisanja iris koda koji pripada podsistemu za kodovanje iris biometrijskog izvora. U našem slučaju specifičan proces koji u sebi sadrži dva podprocesa. Prvi podproces se odnosi na standardnu proceduru za generisanje biometrijskog obrasca koji je opisan u poglavlju 3. Drugim rečima, možemo da kažemo da je ovo jedan složen proces za formiranje iris informacionog izvora na osnovu koga je kasnije urađena sinteza kompletnog rešenja o kome je reč. Drugi podproces predstavlja još jedan složen proces koji uvodi informacione mere i na osnovu rezultata dobijenih preko teorijsko-informacione analize koduje informacioni izvor u cilju izdvajanja najkonzistentnijih informacija.

Napomenućemo da je ovo kritična tačka u ovom sistemu, gde se dobijen loš rezultat prenosi domino efektom na preostale komponente. Zapravo, performanse čitavog sistema zavise od kvaliteta procesa kodovanja iris informacionog izvora. Iz tog razloga sprovedi smo detaljnu i rigoroznu teorijsko-informacionu analizu o kojoj ćemo kasnije govoriti u ovom poglavlju.

Komponenta 4 - predstavlja još jednu tehniku preuzetu iz teorije komunikacija. Interliver ima značajnu ulogu u sistemu. Koristi se za raspršivanje paketskih grešaka i smanjenje uzajamne informacije između različitih iris. Uticaj interlivera na uzajamne informacije. U predloženom rešenju koristili smo slučajni interliver

(engl. *Random interliver*). Tehniku interlivinga primenićemo nad kodovanim iris kodom.

Komponenta 5 - predstavlja logičku operaciju “XOR” u kojoj se bodovan kriptološki ključ čvrsto vezuje za originalni iris kod nad kojim je primenjena tehnika za interliving. Imajući u vidu da su oba podatka slučajna, dobijamo sistem koji po svim svojim osobinama, dosta podseća na “One-time pad” perfektni tajni kriptosistem.

Komponenta 6 - predstavlja podatak koji je rezultat “XOR” operacije. Dobijeni podatak u sebi čuva zaključanu originalnu biometriju i slučajno generisani ključ. Na osnovu ovog podatka nije moguće otkriti originalnu biometriju ili ključ. Ovaj podatak zadovoljava formu podatka za skladištenje sa aspekta zaštite privatnosti biometrijskih podataka.

Komponenta 7 - predstavlja proces u kome se započinje sa procedurom u kojoj regularni korisnik želi da na osnovu originalne iris biometrije regeneriše ključ koji je zaključan čvrstom vezom originalne iris biometrije i ključa. Ovaj proces je identičan procesima u komponenti 3.

Komponenta 8 - predstavlja proces koji je identičan procesu u komponenti 4. Tehnika interlivinga je primenjena i nad originalnom iris biimetrijom koja služi za regenerisanje ključa K . Napominjemo da u oba slučaja interliver radi samo u jednom smeru bez inverznog režima. Tačnije, u ovom ekvivalentnom kanalu ne postoji potreba za invertibilnosti.

Komponente 9 i 10 - predstavljaju dva poslednja procesa u dijagramu procesa, preko kojih se regeneriše ključ koji je zaključan čvrstom vezom u komponenti 5 na dijagramu. Zatim, ponovo se primenjuje logička operacija “XOR” nad kodovanim iris kodom i podatkom koji u sebi čuva ključ. Zatim se primenjuje Rid-Solomon dekodeer koji koriguje sve nastale greške. Ukoliko je dobijeni rezultat posle dekodera jednak ključu koji je generisan u procesu (1), to znači da je kompletna procedura realizovana uspešno i da smo napravili sistem koji ima mogućnost da na osnovu istog iris biometrijskog podataka generiše kriptološke ključeve.

5.4.2. POSTAVKA EKSPERIMENTALNOG OKRUŽENJA

Pored detaljno izložene generičke šeme potrebno je obezbediti i kvalitetno eksperimentalno-razvojno okruženje koje je standardizovano za oblast u kojoj je predmet istraživanja, kao i u odnosu na koga se može kasnije uraditi evaluacija predloženog sistema sa već postojećim sistemima slične namene. Osnovni cilj standardizacije u ovom slučaju je da nam omogući preciznije sagledavanje veličine doprinosa u ovom istraživačkom radu.

Eksperimentalno okruženje sastoji se iz dve komplementarne celine:

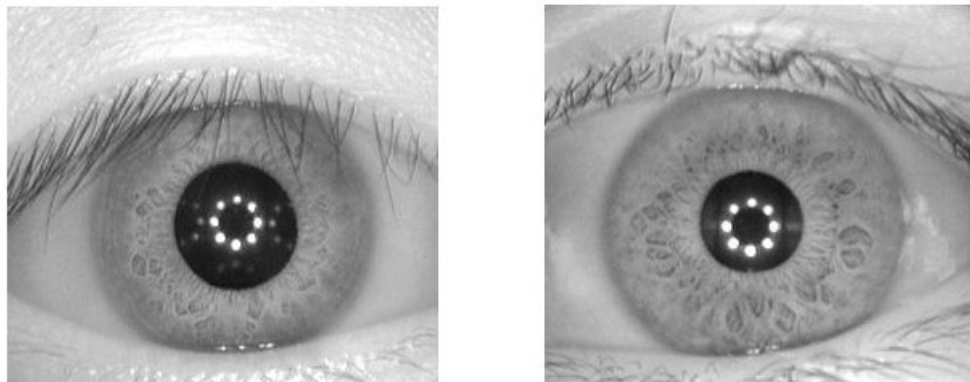
- programskog razvojnog okruženja;
- baze podataka sa eksperimentalnim podacima.

Za programsko-razvojno okruženje u ovom istraživačkom radu je izabran Matlab® programski paket. Matlab je nastao kao skraćenica za "MATrix LABoratory" ("laboratorija za matrice"). Izumeo ga je 1970-ih Kliv Moler (Cleve Moler), šef katedre za informatiku na Univerzitetu "Novi Meksiko". Omogućava pristup brzog razvoja aplikacija (eng. *RAD-rapid application development*) u cilju brzog generisanja eksperimentalnih rezultata. Matlab® je RAD okruženje i obezbeđuje odlično radno okruženje sa alatima za obradu podataka, vizualizaciju podataka i standardizovane algoritme koji se primenjuju u svim visoko-tehnološkim poljima. Pored mnogobrojnih algoritama nudi programiranje na visokom nivou.

Eksperimentalne podatke koje smo koristili, dobili smo besplatno iz „CASIA“ baze podataka. „CASIA“ - baza podataka sadrži slike irisa, a tvorci ove baze su kineska istraživačka grupa sa Instituta za biometrijska istraživanja. Više verzija baze podataka je besplatno ponuđeno međunarodnoj zajednici za potrebe biometrijskih istraživanja. Više od 3000 korisnika iz 70 zemalja preuzelo je „CASIA“ bazu podataka sa slikama irisa i mnogo odličnih istraživački radova koji su priznati od međunarodne naučne zajednice su takođe nastali na osnovu slika ove baze podataka.

Od 1990-tih zabeležen je visok rast interesovanja na polju tehnologija namenjenih za prepoznavanja pojedinca na osnovu biometrije. Osnovni problem ili izazov je upotrebljivost i skalabilnost. Upotrebljivost je najveće usko grlo kod prepoznavanja na osnovu biometrije irisa. Prvi problem je realizovati jednostavnu (eng.

user friendly) hardversku infrastrukturu za autentifikaciju korisnika. Drugi problem je široka primena ovih sistema koja zahteva visok stepen integracije, indeksiranje i skladištenje biometrijskih podataka u bazama podataka. Sve ovo vodi do problema skalabilnosti kod sistema za prepoznavanja korisnika na osnovu biometrije irisa. Do danas se pojavila i četvrta verzija baze podataka "CASIA-Iris V4" koja je korišćena za potrebe eksperimentalnog rada na ovoj disertaciji (Slika 5.11).



Slika 5.11 Primeri slika irisa iz „CASIA-Iris V4” baze podataka

"CASIA-Iris V4" baza podataka u sebi sadrži ukupno 54.601. sliku irisa sa više od 1800. originalnih i 1000 virtuelnih subjekata. Sve slike irisa su 8-bitne u „JPEG” formatu, prikupljene akvizicijom specijalnih kamera sa infra-crvenim osvetljenjem. Bazu podataka može da koristi svako za potrebe istraživanja i edukativne svrhe.

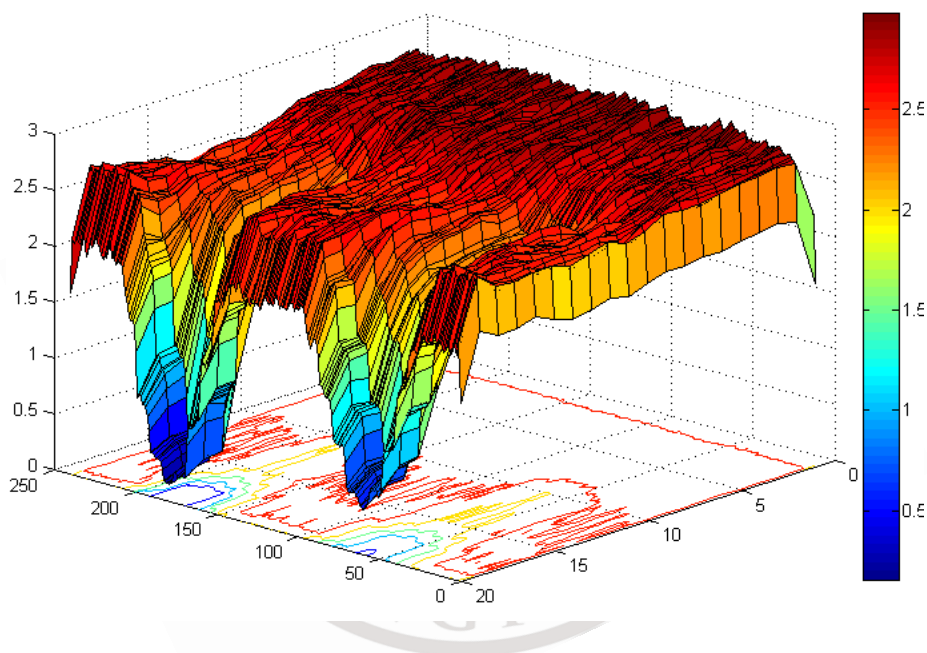
5.4.3. INFORMACIONA ANALIZA TEKSTURE IRISA

Pravljenje 3D modela lokalne entropijske vrednosti je od velikog značaja za razumevanje informacionog kvaliteta površine irisa. Stručan naziv za ovaj prikaz rezultata je 3D kolor mapa (eng. *Heatmap*).

Prvi model predstavlja rigorozniju analizu jer je korišćena veličina prozora [3 x 3] i može da se tretira kao model na osnovu minimalnih entropijskih vrednosti,

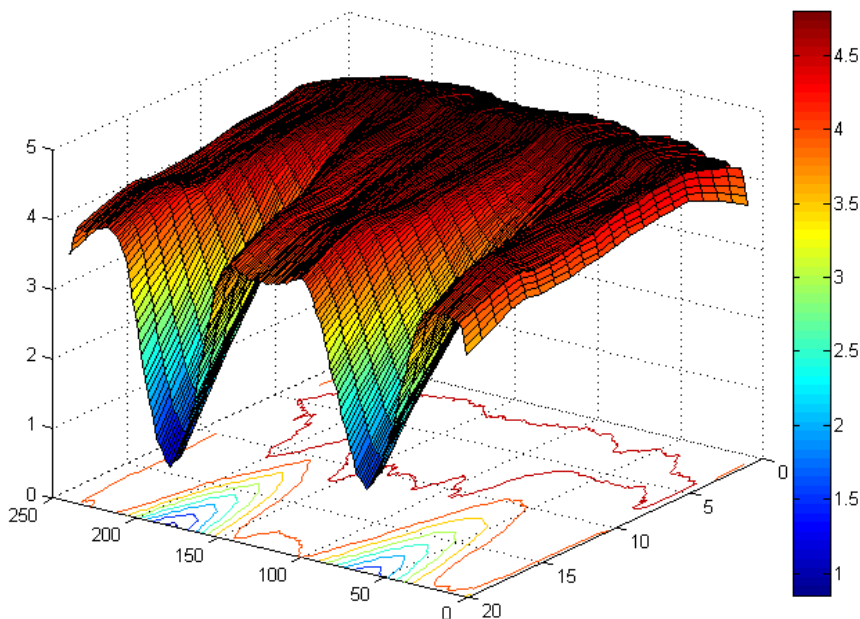
dok drugi model je manje rigorozan i modelovan na osnovu maksimalne entropije koja je zabeležena na teksturi slike irisa.

Na 3D entropijskom plotu (Slika 5.12), vidimo da prvi kružni segment irisa do zenice poseduje veću lokalnu entropiju od drugog kružnog segmneta irisa koji se graniči sa beonjačom. Posmatrajmo levu stranu na Y osi i videćemo da lokalna entropija nakon vrednosti 10 na osi Z naglo opada. Ovoj momenat je bio polazna osnova za dalju informacionu analizu texture irisa i njihovih međusobnih odnosa.



Slika 5.12 3D informacioni model lokalne entropije

Iako je prvi model dosta precizniji kada je upitanju lokalna entropija, drugi model (Slika 5.13) je dobijen na osnovu veličine prozora $[9 \times 9]$ za određivanje lokalne entropiju. Smatramo da ovaj model daje konačnu sliku o kvalitetu prvog segmenta u odnosu na kvalitet drugog segmenta. Na osnovu ovog modela možemo precizno da odredimo prostorne okvire prvog segmenta koji treba biti podvrgnut daljim informacionim analizama.

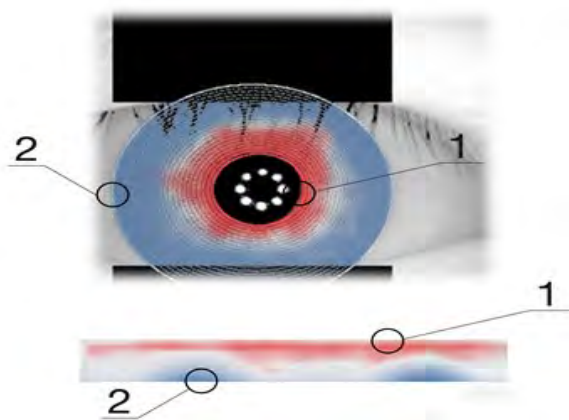


Slika 5.13 3D informacijski model lokalne entropije

Na 3D entropijskom plotu (Slika 5.13), vidimo da je prethodna konstatacija tačna i da prvi kružni segment irisa do zenice poseduje veću lokalnu entropiju, što se jasno vidi na levoj strani na Y osi. Ovaj 3D model je dosta ilustrativan iz razloga što sada jasno vidimo segment irisa koji je značajan za nas. Ovu konstataciju potvrđujemo sa konturom koja se jasno ocrta u dvo-dimenzionalnom prostoru (X, Z). Kontura označena jakim crvenom bojom ocrta informaciono najkvalitetniji segment irisa, koji će kasnije biti ekstraktovan i korišćen u informacionoj analizi u cilju postavljanja teorijskih okvira ovog sistema za generisanje kriptoloških ključeva. Sa desne strane plotu na osnovu toplotne skale možemo da se uverimo da su u tom segmentu zabeležene maksimalne vrednosti.

Ovo saznanje je polazna osnova za nastavak informacione analize tekture irisa i njihovih međusobnih odnosa. U narednim analizama posebno su tretirani segmenti na osnovu podele koju smo do sada napravili (Slika 5.14). Prvi segment irisa predstavlja informativno najkvalitetniji segment, dok je u drugom delu zabeležen pad kvaliteta posmatran kroz rezultate dobijene preko lokalne entropije. Na kvalitet drugog segmenta dobrim delom utiče automatska faza

segmentacije koja ne ispunjava uslov od 100% tačnosti. Iz tog razloga smatramo da ovaj segment ne može da predstavlja materijal za generisanje ključeva.



Slika 5.14 Vrednosti lokalne entropije po segmentima

Estimacijom entropije, lokalne entropije i uzajamne informacije, identifikovani su segmenti irisa koji su najpogodniji za ove potrebe. Izvršena je optimizacija parametara odgovarajuće *vejvlet* transformacije u cilju dobijanja što veće entropije i što niže uzajamne informacije u transformacionom domenu. Koristimo sledeću notaciju:

$H(K)$ - entropija ključa ili veličina ključa;

$I(Y; Y')$ informacija između irisa iste osobe;

$I(X; Y)$ - informacija između irisa različitih osoba;

$H(X)$ - entropija iris koda;

$H(X, Y)$ - entropija dva iris koda različitih osoba;

$H(Y, Y')$ - entropija dva iris koda iste osobe;

$H(K)_{max}$ maksimalna veličina ključa.

$$H(IRIS\ X) = H(IRIS\ Y) = H(IRIS\ Y') = 3940;$$

$$I(X;Y) = 511;$$

$$I(Y;Y') = 997;$$

$$H(X,Y) = 7281;$$

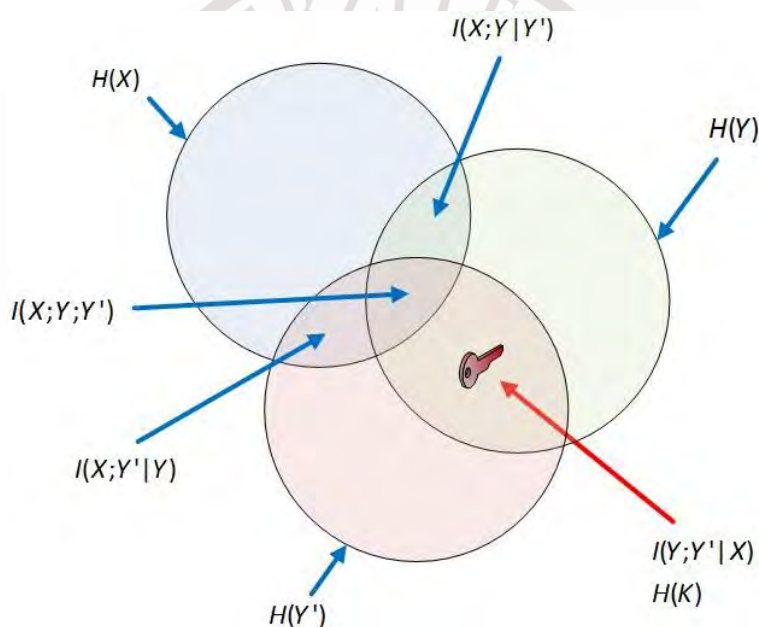
$$H(Y,Y') = 6709;$$

$$I(Y;Y' | X) = 788;$$

$$H(K) = I(Y;Y' | X) = 788;$$

$$I(X;Y;Y') = I(Y;Y') - I(Y,Y' | X) = 997 - 788 = 209;$$

Maksimalna entropija ključa iznosi $H(K) = 788$ bitova, čime su postavljeni okviri za sintezu sistema za ekstrakciju čisto slučajnih nizova iz iris biometrije.



Slika 5.15 Grafička prezentacija prostora biometrijskog ključa

Maksimalna veličina kriptološkog ključa je određena izrazom:

$$H(K)_{\max} = I(Y;Y' | X);$$

Na slici (Slika 5.15) je predstavljena grafičku prezentaciju pozicije biometrijskog ključa. Dijagram na slici sadrži tri slučajne promenljive X, Y i Y' . Važno je napomenuti da je uzajamna informacija $I(X; Y; Y')$ simetrična ukoliko su ove tri promenljive jednako nezavisne. Imajući u vidu da u ovom dijagramu postoji veća zavisnost između promenljive Y i Y' time je uzajamna informacija $I(Y; Y')$ veća. Na osnovu ove činjenice i informacija $I(Y; Y'|X)$ je veća. U ovom slučaju pojedinačne uzajamne informacije $I(X; Y)$ i $I(X; Y')$ su se smanjile, dok se zajednička informacija $I(X; Y|Y')$ i $I(Y; Y'|X)$ povećala. Na dijagramu koji sledi pokušali smo da prikažemo vrednosti u zadatoj proporciji.

5.4.5. IZBOR ADEKVATNOG ZAŠTITNOG KODA

Na početku izbora adekvatnog zaštitnog koda, potrebno je napraviti analizu grešaka u procesu projektovanja sistema koji je otporan na nastale greške. Kod ovakvih sistema greške mogu da budu uzrok otkaza.

Grešku možemo tretirati kao meru za odstupanje od tačnosti. Na primer, ukoliko je vrednost greške izuzetno visoka u sistemu za generisanje ključa na osnovu dva biometrijska podatka, onda to može da utiče na smanjenje količine uzajamne informacije između biometrijskih podataka što dovodi do otkaza sistema ili u drugom slučaju prouzrokuje pogrešan rezultat koji je u ovoj klasi sistema nepopustljiv. Dakle, vidimo da čak i ako postoji greška, ne mora da se ispoljava preko otkaza sistema, već može da daje loše rezultate.

Karakteristike grešaka možemo posmatrati sa sledeća tri aspekta:

- uzrok;
- vrednost;
- trajanje.

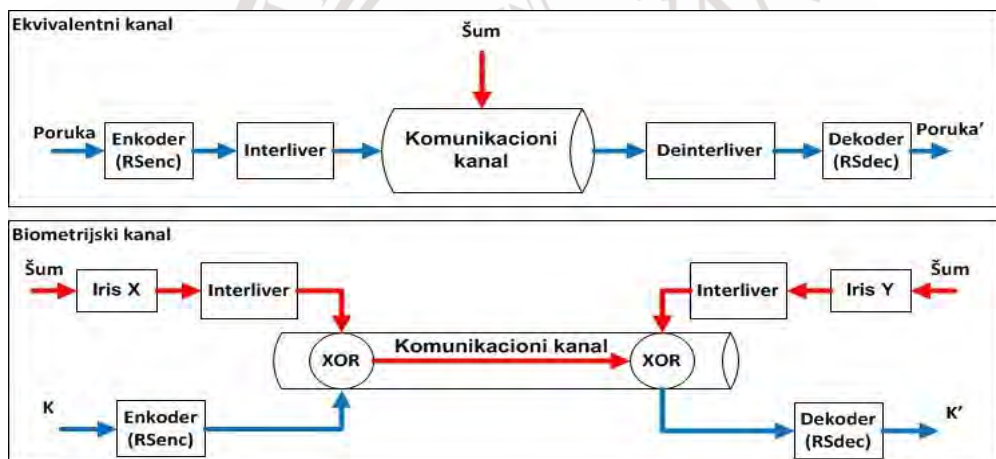
Uzrok greške može da nastane zbog problema u realizaciji na hardverskoj ili softverskoj platformi zbog lošeg izbora funkcionalnih komponenti.

Vrednost grešaka generalno može da bude određena ili neodređena. Vrednost greške je određena ukoliko se ta vrednost ne menja bez spoljašnjeg uticaja. Greška koja ima neodređenu vrednost, njena vrednost se menja u različitim vremen-
skim trenucima.

Trajanje grešaka može da bude stalno, prolazno ili trenutno. U našem slučaju imamo stalne greške za koje smo merenjem odredili približne vrednosti koje su stalne i ispoljavaju se sve dok ne preduzmemo odgovarajuće zaštitne mere ili mere korekcije.

Pored ova tri navedena aspekta bitno je navesti i rasprostranjenost grešaka koja može biti okarakterisana kao lokana ili globalna. Rasprostranjenost grešaka u iris biometrijskom kodu može da bude lokalna i globalna.

Analiza ekvivalentnog kanala podrazumeva pronalaženje nekog klasičnog komunikacionog kanala iz teorije komunikacija koji utvrđuje uslove pod kojima je moguć pouzdan prenos informacija, a odgovara po svim svojim karakteristikama našem kanalu, ali sa različitim sadržajem. Potrebno je utvrditi maksimalnu brzinu pouzdanog prenosa po kanalu sa šumom uz upotrebu kodova za ispravljanje grešaka i maksimalnu količinu grešaka koja nastaje kada se informacija prenese većom brzinom od maksimalne.



Slika 5.16 Analiza ekvivalentnog kanala

Sada je jasno da ekvivalentni kanal predstavlja isti kanal koji je opisan na dva različita načina. Na slici (Slika 5.16), sadrži analizu dva ekvivalentna kanala. Gornji kanal na slici predstavlja ekvivalentni kanal koji se često može sresti u klasičnim komunikacionim kanalima. Šema kanala sadrži enkoder, dekodeer, interliver, deinterliver i kanal sa šumom. Poruka koja se prenosi ovim kanalom, izložena je uticaju šuma koji se ispoljava u vidu paketskih grešaka u sadržaju poruke. Obzi-

rom da se radi o većim paketskim greškama na predajnoj strani, primenjen je Rid-Solomonov kod i interliver čiji je zadatak da rasprši simbole kodovane poruke, a zatim se poruka šalje preko kanala. U toku prenosa poruka je izložena uticaju šuma koji utiskuje u sadržaj poruke paketske greške. Kada poruka stigne na prijemnu stranu, primenjuje se deinterliver koji simbole kodovane poruke vraća na iste indeksne pozicije koje su bile nakon kodovanja na predajnoj strani. Paketske greške koje su nastale sada su razbijene i ujednačeno raspoređene preko celog sadržaja poruke. U poslednjoj fazi, primenom Rid-Solomon dekodera korijugu se sve nastale greške.

Donji kanal na slici predstavlja biometrijski kanal sa prisustvom šuma. Šema kanala sadrži enkoder, dekoder, interliver i komunikacioni kanal. U ovom kanalu poruka je ključ K koji se prenosi preko šumnog kanala koji je indukovano sa dva irisa. Šum koji je prisutan u kanalu, ispoljava se preko paketskih grešaka. U cilju postizanja visokih performansi na strani dekodera, primenjujemo interliver nad oba irisa (jedan na predajnoj, a drugi na prijemnoj strani) koja zajedno indukuju komunikacioni kanal sa šumom. Zatim, ključ K kodujemo sa Rid-Solomonovim enkoderom i šaljemo kroz takav komunikacioni kanal nad kojim sada imamo kontrolu za određen opseg vrednosti paketskih grešaka. Poruka na prijemu ili ključ K se dekoduje Rid-Solomonovim dekoderom i dobijena poruka predstavlja ključ K' koji je jednak ključu K na predajnoj strani.

Možemo sad da zaključimo da smo analizom ekvivalentnog kanala sami modelovali ovaj novi kanal, preko koga ostvarujemo prenos poruka sa maksimalnim kapacitetom. Ovaj kanal ima osobine binarnog simetričnog kanala sa šumom i na ovaj način smo potvrdili Šenonovu teoremu, koja je bila veliko iznenađenje u njegovom radu, u kome se tvrdi da ako izaberemo odgovarajući način kodovanja informacije za zadati kanal, može se postići po želji mala greška dekodovanja, odnosno prenosa informacija. U poglavlju 3. dato je više detalja vezanih za ovu teoremu.

Imajući u vidu da projektovani sistem pripada biometrijskoj kriptografiji, glavni izazov je integritet podataka. Greške koje nastaju nije moguće u potpunosti eliminisati, ali ih je moguće znatno smanjiti. U zavisnosti od stepena integracije, verovatnoća nastanka greške je veća ili manja. Sa aspekta projektovanja sistema, odnosno za postizanje visoke pouzdanosti u radu sistema koriste se tri osnovna pristupa:

- izbegavanje grešaka;
- ispravljanje grešaka;
- smanjenje grešaka;

Izbegavanje grešaka podrazumeva sprečavanje nastanka grešaka nastalih na hardverskoj ili softverskoj platformi. Ovakve tehnike se odnose na izbor kvalitetnog hardvera (iris kamera) koji učestvuju u procesu akvizicije slike irisa, kao i adekvatan izbor algoritama koji učestvuju u obradi signala (kodovanje irisa). Izbegavanje grešaka podrazumeva i faze u kojima se vrše testiranja gde se preispituju pojedine komponente sistema.

Ispravljanje grešaka je tehnika koja ne sprečava nastanak greške. Ova tehnika uspešno detektuje i ispravlja nastale greške. Možemo da kažemo da ova tehnika ima mogućnost transformacione invertibilnosti nad podatkom sa greškom, u cilju dobijanja istog podatka bez greške. Jedna od važnijih komponenti ovog sistema su zaštitni kodovi koje primenjujemo nad podatkom (ključ K), koji je u toku prenosa izložen greškama. Na ovaj način je omogućen prenos u kritičnim situacijama za zadati stepen tolerancije.

U projektovanju sistema korišćeni je Rid-Solomon kod. Ovaj kod ispravlja greške na nivou simbola, a ne na nivou bitova, pogodni su za ispravljanje koncentrisanih paketskih (engl. *burst*) grešaka. Oni imaju široku primenu u sistemima digitalnih komunikacija i sistemima za čuvanje podataka. Rid-Solomon kodovi su podgrupa *BCH* kodova i klasa linearnih, nebinarnih cikličnih kodova. Rid-Solomon kod je blok kod koji se predstavlja kao $RS(n, k, t)$ preko polja Galoa $GF(2^n)$.

Rid-Solomon kod uvodi veliku redundantnu informaciju (preko polinomske strukture) i tako postiže visoke performanse za detekciju i ispravljanje grešaka. Da bi se ova cena platila neophodno je koristiti samo konzistentnu informaciju (jedinствене karakteristike). Iz ovog razloga su urađene rigorozne informacione analize nad teksturom irisa, sa ciljem izbora upravo takvih segmenata koji će da sadrže većinom konzistentnu informaciju.

Smanjenje grešaka je uglavnom jedna od tehnika koja utiče na smanjenje nastalih grešaka koje nije moguće ispraviti. U našem slučaju izabrali smo za ovu vrstu tehnike interliver. Interliveri koriste metodu preplitanja vrednosti u iris kodu. Metod za preplitanje može da bude raznovrsan. Mi koristimo slučaju permutaciju

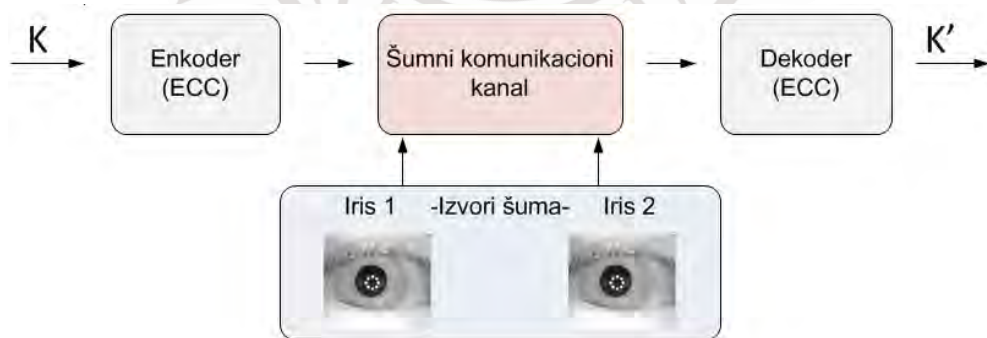
koja je zadata sa nekom inicijalnom vrednošću koja predstavlja početno stanje pesudogeneratora. Ovakvi interliveri uvode element slučajnosti u neki dizajn koda bez povećanja kompleksnosti, pretpostavljajući korišćenje iterativnog dekodovanja dva interlivovana koda.

5.4.6. MOTIV ZA UVOĐENJE ZAŠTITNOG KODA I INTERLIVERA

Primena zaštitnih kodova i interlivera nad irisom je stavila biometriju u paralelu sa klasičnim komunikacionim kanalima. Jedan od naših ciljeva je bio da pronađemo ekvivalentni kanal koji ima zajedničke osobine sa biometrijskim komunikacionim kanalom. Pronalazak ekvivalentnog kanala, davao bi garantovano dobre performanse celokupnog sistema koji je krajnji cilj.

Na slici (Slika 5.17) predstavlja deo sistema u kome je biometrija poistovećena sa klasičnim komunikacionim kanalom sa prisustvom šuma. U ovom primeru dva irisa indukuju biometrijski komunikacioni kanal preko koga imamo cilj da prenesemo ključ K . Vrednosti greške u ovom kanalu variraju u zavisnosti od toga da li dva irisa pripadaju jednoj osobi ili su od različitih osoba. U ovom apstraktnom modelu biometrijskog kanala, naš zadatak je da ključ K prenesemo preko kanala bez grešaka. Tačnije, cilj je projektovati komunikacioni kanal čiji je maksimalni kapacitet definisan izrazom:

$$C = \max I(K; K') = 1$$



Slika 5.17 Biometrijski komunikacioni kanal sa šumom

Razlozi za nastanak ovakvog motiva obrazložen je kroz sledeće činjenice:

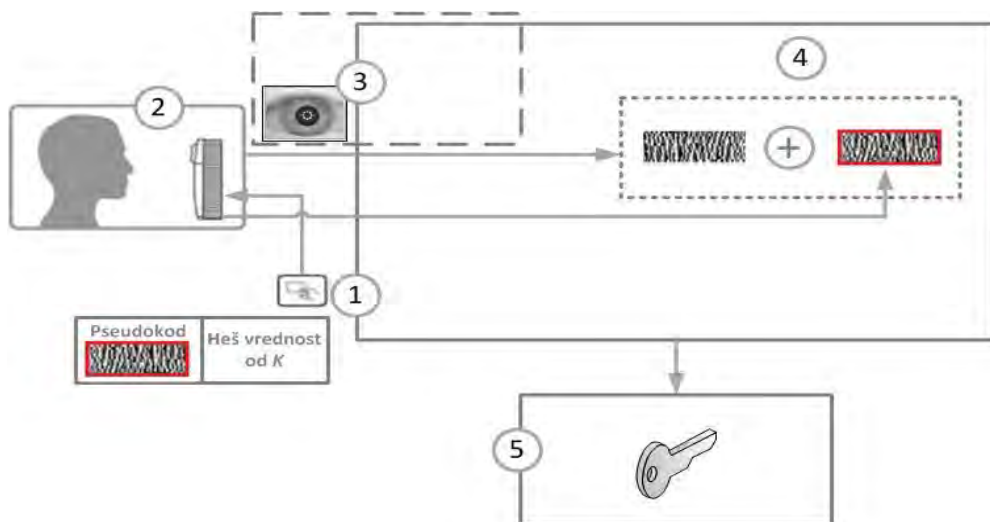
1. Osnovni problem kod biometrijskih podataka je varijabilnost koja je prisutna svaki put u podacima nakon akvizicije biometrijskih podataka. Drugim rečima, svaki novi biometrijski podatak generisan na istom biometrijskom izvoru se uvek razlikuje 10% - 20% od svih prethodnih, dok se biometrijski podaci generisani na različitim biometrijskim izvorima razlikuju od 40% do 60%.
2. Kao odgovor na pomenuti problem varijabilnosti u biometriji irisa, nastala je ideja o ekvivalenciji sa drugim komunikacionim kanalima. Ova ideja je uvela primenu zaštitnih kodova za ispravljanje grešaka (engl. *error correcting code*), a tehnika je preuzeta iz oblasti komunikacija.
3. Kapacitet koda za ispravljanje grešaka u ovom slučaju performanse dekodera, moraju biti takve da odvajaju originalnog korisnika od lažnog. Na primer, biometrijski kanal indukovan sa dva iris koda sa istog biometrijskog izvora, mogu biti u stanju da prenesu poruku bez grešaka u našem slučaju ključ K , dok kanal indukovan sa dva iris kod sa različitih biometrijskih izvora, ne sme da prenese ključ K , čak šta više poželjno je da ključ K bude uništen, tako da je uzajamna informacija $(K; K') = 0$.
4. Postizanjem pomenutih performansi, uspeh bi predstavili sa rezultatom $K == K'$, dok se K' koristi kao kriptološki ključ.
5. Pravljenjem kompromisa između ukupne količine informacije H iris koda i njihove uzajamne informacije I između istih i različitih kodova irisa, dobijamo okvire za maksimalnu veličinu ključa K .
6. Interliver je tehnika koja se koristi za raspršivanje paketskih grešaka. Analizom je utvrđeno da iris kod sadrži paketske greške. Ova tehnika se kod klasičnih komunikacionih kanala koristi za podizanje performansi zaštitnih kodova ili kodova za ispravljanje grešaka.

Sada možemo da zaključimo da sve ove činjenice nezaustavno utiču na stvaranje jedne nove oblasti, koja opravdano nosi ime biometrijska kriptografija.

5.4.7. OBLAST PRIMENE I BUDUĆI RAZVOJ OBLASTI

Osnovna primena predloženog i razvijenog rešenja je u domenu kriptografskih potreba. Dobijeni ključevi mogu biti korišćeni u kriptografske svrhe, kao i kod sistema za bezbednu autentifikaciju korisnika na bazi heš vrednosti ključa K . Arhitektura predloženog sistema zasniva se na tri bezbednosna faktora, a to su,

korisnička lozinka (PIN), biometrijski uzorak i *token* (*smart* kartica, *USB*,...). Arhitektura predloženog biometrijskog sistema omogućava proveru identiteta i generisanje ključeva u „*off-line*“ režimu rada. Na ovaj način se izbegava centralizovana baza podataka, što doprinosi stvaranju pozitivnih utisaka za socijalno prihvatanje sistema. Na sledećoj slici (Slika 5.18), prikazana je jedna univerzalna šema za implementaciju predloženog rešenja u „*off-line*“ režimu rada.



Slika 5.18 Jedna šema primene sistema

Na slici su označene faze u sistemu sa brojevima od 1 do 5. U prvoj (1) fazi korisnik sistema prilaže *smart* karticu koja na sebi sadrži pseudokod i heš vrednost od zaključanog ključa u pseudokodu. Nakon unosa ispravne korisničke lozinke, podaci sa smart kartice se prosleđuju sistemu za regenerisanje ključa (4). U drugoj (2) fazi, očitava se i prosleđuje korisnikova originalna biometrija irisa preko biometrijskih skenera. U trećoj (3) fazi primenjuje se sistem za generisanje iris koda (biometrijskog obrasca). Zatim, generisani iris kod se prosleđuje sistemu za regenerisanje ključa. U četvrtoj (4) fazi, prelazi se u fazu regenerisanja ključa sa našim novopredloženim rešenjem u disertaciji. Uspešnost ove faze potvrđuje se sa identičnom heš vrednosti koja je dobijena sa smart kartice, a rezultat ove faze je biometrijski ključ koji se može koristiti u razne kriptografske svrhe.

Tabela 5.1 Poređenje sa postojećim rezultatima u ovoj oblasti

Biometrija	Dužina ključa (bit)	Stopa lažnog odbacivanja (FRR)	Stopa lažnog prihvatanja (FAR)
Glas	46	20%	-
Svojeručni potpis	40	28%	1,2%
Otisak prsta	-	-	-
	69	30%	-
	49 i 85	5,4% - 9,9%	3,2% - 2,5%
Lice	-	0,93%	
	58	3,5%	0%
Iris	140	0,47%	0%
	186	0,76%	0,096%
	400	4,75%	0%
EKG i Glas	240	1.27%	10.62%

U toku rada su uočene sledeće mogućnosti i pravci daljeg razvoja:

1. prototip za predloženo rešenje;
2. bimodalni biometrijski sistema;
3. biometrijske PKI infrastrukture.

Kada je zahtevano više faktora u autentifikaciji. Iris *LG 4000* je izuzetno fleksibilan sa ugrađenim čitačem *smart* kartica vodećih svetskih proizvođača. Više faktorska autentifikacija je podržana preko numeričke tastature za unos lozinke ili *PIN* koda u zavisnosti od modela uređaja.



Slika 5.19 LG Iris 4000 skener irisa

Kao mogućnost za dalji rad je razvoj bimodalnih biometrijskih sistema. Bimodalni sistemi kombinuju dva biometrijska signala. Ovo podrazumeva kombinovanje različitih biometrija. Na primer, kombinovanje EKG signala i govora, irisa i govora ili EKG signala i irisa.



Slika 5.20 Bimodalni biometrijski sistem

Takođe, i u ovom slučaju se koriste transformacione funkcije za ekstrakciju čiste informacije iz navedenih biometrija. Rešavanjem apstraktnih pojmova u domenu biometrijskih podataka, kao što je uzajamna informacija iz oblasti teorijsko-informacione analize, bićemo u mogućnosti da razvijemo algoritme za estimaciju

uzajamnih informacija između dve ili više biometrija. Ekstraktovana informacija koristiće se kao osnova za sintezu sistema za generisanje još kvalitetnijih kriptoloških ključeva većih dužina u odnosu na teorijski postavljene okvire.

Pod razvojem biometrijske *PKI* infrastrukture, podrazumevamo razvoj novog sistema sa javnim ključevima koji će biti ekvivalentan postojećoj *PKI* infrastrukturi. Ovaj sistem je direktno zasnovan na biometrijskim podacima. Zbog zahtevanih većih dužina ključeva, razvoj ovog rešenja zavisice od uspeha razvoja bimodalnih sistema. Ova ideja trenutno postoji samo na apstraktnom nivou. Prvi zadatak je pronalazak ekvivalentne šeme sa svim funkcionalnim komponentama koje postoje u tradicionalnoj šemi *PKI* infrastrukture.

Ideja o biometrijskoj *PKI* infrastrukturi ima veliki potencijal u današnjem informacionom društvu. Postoji više problema sa tradicionalnom *PKI* infrastrukturom u elektronskim servisima koji obezbeđuju tajnost, integritet i neporecivost. Glavni nedostatak je zahtev u poverenje u treću stranu od poverenja, koja je zadužena za izdavanje i potpisivanje privatnih ključeva. Postavlja se onda pitanje koliko možemo da verujemo jednom ovakvom sistemu, ukoliko se radi o primeni u institucijama od velikog značaja (vojska, diplomatija, policija)? Drugi problem je robusna infrastruktura koja onemogućava uzajamnu autentifikaciju u elektronskim servisima. Na primer, najveći prodavac knjiga u svetu je Amazon. Elektronski servis za plaćanje kod Amazona podržava samo jednosmernu autentifikaciju u smeru Amazon korisnik. Na ovaj način, korisnik može da se uveri u legitimitet Amazon elektronskog servisa, ali Amazon ne vrši proveru da li se radi o legitimnom vlasniku kreditne kartice. Možemo da zaključimo da je, uglavnom, krajnji korisnik nezaštićen. Ovakvih slučajeva ima mnoštvo i u bankarskim elektronskim servisima za Internet plaćanja.

Razvoj ovog sistema omogućava jednostavnije generisanje i distribuciju kriptoloških ključeva, s druge strane, bilo bi omogućeno da svaki korisnik ili učesnik neke *online* transakcije bude maksimalno bezbedan, tako što svako za sebe u komunikaciji predstavlja sopstveno sertifikaciono telo koje ima mogućnost da generiše i verifikuje sopstveni sertifikat, kao i da opozove sertifikat u slučaju da je bezbednost narušena.

6. TAJNA RAZMENA KRIPTOLOŠKOG KLJUČA JAVNIM KANALOM – BEZBEDNOST NA FIZIČKOM SLOJU

U savremenim informacionim sistemima, zaštita podataka predstavlja nezaobilazan proces. Bilo da se radi o zaštiti podataka u bazama podataka ili u komunikacionim kanalima pri prenosu podataka, kriptologija kao nauka obezbeđuje mnogobrojna kriptografska rešenja. Rešenja koja proizilaze korišćenjem kriptologije mogu se svrstati u dve grupe – rešenja koja pružaju teorijski dokazivu bezbednost i rešenja koja se zasnivaju na teško rešivim matematičkim problemima – praktična bezbednost.

Postoje mnoge fundamentalne razlike između klasične kriptografije korišćene na visokim slojevima protokola i bezbednosti na fizičkom sloju koja je zasnovana na teorijsko informacionoj analizi. Zbog toga je važno razumeti šta su te razlike i kako one utiču na izbor tehnologije u praktičnom scenariju. U ovom odeljku kada kažemo klasična kriptografija, ne mislimo na klasičnu istorijsku kriptografiju (klasične istorijske šifre), već na kriptografske mehanizme koji su danas dostupni u praktičnoj bezbednosti.

Klasična računarska bezbednost se zasniva na javnim ključevima za autentifikaciju i distribuciju ključeva za zaštitu podataka u prenosu sa simetričnim kriptomehanizmima. Najčešća kombinacija algoritama koja se primenjuje u današnjoj praksi je kombinacija RSA i AES, koja se smatra bezbednom za veliki broj aplikacija, jer do sada nema poznatih efikasnih napada na sisteme sa javnim ključevima. Mnoge simetrične šifre su razbijene u prošlosti, ali one koje su bile razbijene su dosledno zamenjene novim algoritmima, čija je kriptoeanaliza zahtevnija i zahteva velika računarska izračunavanja. Pod pretpostavkom da napadač ne može da razbije jake klasične kriptografske mehanizme, moguće je dizajnirati sistem koji je bezbedan sa verovatnoćom 1. Tehnologija je lako dostupna i jeftina.

Rešenja iz praktične bezbednosti su uglavnom zastupljena i koriste algoritme za šifrovanje podataka poput *AES*, *DES* ili algoritama kao što su *RSA* i *DSA*. Algoritmi *AES* i *DES* nemaju dokazanih propusta koji bi omogućili pronalaženje otvorenog teksta na osnovu šifrata za relativno kratko vreme od vremena potrebnog za potpunu pretragu ključeva. Sa druge strane *RSA* i *DSA* algoritmi zavise od težine rešavanja matematičkog problema – faktORIZACIJA velikih brojeva. Algoritmi za faktORIZACIJU napreduju iz dana u dan, iz tog razloga je kraće vreme potrebno za fak-

torizaciju, odnosno pronalazak privatnog ključa nekog od ova dva algoritma na osnovu poznavanja javnog ključa.

Danas procesorske snage računara rastu neverovatnom brzinom, i postoji veoma veliki broj moćnih komercijalnih proizvoda, tako da bezbednost algoritama sa dužinama ključa do 64 bita zavisi isključivo od protivnikove rešenosti da dođe do otvorenog teksta, odnosno od njegovih finansijskih mogućnosti koje bi upotrebio za razbijanje nekog kriptosistema. Na osnovu ovih činjenica dolazi se do zaključka da je potrebno preći na algoritme koji koriste duže ključeve ili na kriptografska rešenja iz perfektne bezbednosti.

Međutim postoje i mane u računarskom modelu. Bezbednost kriptografije sa javnim ključevima zasniva se na pretpostavci da za određene jednosmerne funkcije ne postoji drugi smer, opet nedokazano sa matematičke tačke gledišta. Računarske snage nastavljaju da narastaju brzim tempom, tako da napad sa potpunom pretragom koji se nekada smatrao neizvodljivim, danas je na dohvat ruke. Šta više, ne postoji precizna metrika za upoređivanje prednosti različitih šifara na rigorozan način. U principu, bezbednost kriptografskih protokola se meri preživljavanjem niza napada ili ne. Iz dela Šenona (*Shannon*) i Vinera (*Wyner*), jedan zaključuje da vladajuća kriptografska paradigma nikada ne može pružiti teorijsko informacionu bezbednost, zato što je komunikacioni kanal između dve prijateljske strane i napadača bešuman, kao i kapacitet bezbednosti jednak nuli. Šta više, postojeći sistemi za distribuciju ključeva su zasnovani na računarskom modelu i zahtevaju treću stranu od poverenja, kao i složene protokole i systemske arhitekture. Ako je potrebno generisati više ključeva, nekad je to bolje uraditi samo na osnovu jedne deljenje tajne i po cenu smanjenja nivo zaštite podataka.

Glavne prednosti bezbednosti na fizičkom sloju pod teorijsko informacionim bezbednosnim modelom su činjenice da nema računarskih ograničenja i da precizno možemo govoriti o količini iscurile informacije do koje može da dođe napadač, a ujedno ta količina informacije predstavlja funkciju kvaliteta tog komunikacionog kanal. bezbednost na fizičkom sloju je već realizovana u praksi preko kvantnih protokola za distribuciju ključeva. U teoriji, na ovaj način je moguće doći eksponencijalno blizu sistema perfektne tajnosti. Systemska arhitektura bezbednosti u osnovi je ista kao i ona za komunikaciju. Umesto klasične distribucije ključeva, na fizičkom sloju je moguće generisati u sekundi potreban broj ključeva.

Međutim, mi moramo prihvatiti neke nedostatke. Prvo i najvažnije, teorijsko informaciona analiza ove vrste bezbednosti se oslanja na prosečnim informacionim merama. Sistem može biti podešen i dizajniran do određenog nivo bezbednosti, tvrdeći sa velikom verovatnoćom, da će sistem biti bezbedan. Takođe smo primorani na korišćenje pretpostavki o kanalima koje možda nisu tačne u praksi. U većini slučajeva, postoji i jedna vrlo konzervativna pretpostavka o kanalima, što je verovatno da će dovesti do niskog kapaciteta tajnost u ovom kontekstu ili na kraju generisati nekvalitetan ključ. Do danas, nekoliko sistema je već razvijeno, pre svega mislimo na optičku komunikaciju, ali tehnologija nije široko dostupna i dalje je cena dosta visoka.

Na osnovu navedenih poređenja, vrlo je verovatno da će fizički sloj bezbednosti postati deo rešenja bezbednosnog protokola sa slojevitim dizajnom, u kojem je obezbeđen servis poverljivosti i autentifikacije od strane drugih slojeva, a svaki sa svojom specifičnom ulogom. Ovaj modularni pristup je sličan dizajnu skoro svih praktičnih sistemima koji danas postoje, ali bitno je imati na umu da fizički sloj pruža dodatni sloj bezbednosti koji još uvek ne postoji u komunikacionim mrežama.

Glavni cilj ovog poglavlja je upoznavanje za teorijskim osnovama bezbednosti na fizičkom sloju i pružanju nekih osnovnih metoda koje će omogućiti razvoj aplikacija i alata za sprovođenje ove ideje u realne sisteme. Preko scenarija koje su predložili Maurer i Viner, upoznaćemo se sa suštinskim teorijama i matematičkim modelima za procenu bezbednosti fizičkog sloja i njegovu karakterizaciju osnovnih ograničenja, kodne šeme za podatke na fizičkom sloju i drugim sistemskim aspektima bezbednosti na fizičkom sloju.

6.1. RAZMENA KLJUČA 1: SATELITSKI SCENARIO

Protokoli koji se danas koriste za razmenu kriptoloških ključeva prepuštaju bezbednost ključeva rešavanju matematičkih problema - faktorizacija. Najčešće korišćeni metodi za distribuciju ključeva su *Diffie-Hellman* protokol i zaštita ključeva korišćenjem asimetričnih šifara – *RSA* ili *DSA*. Protokoli koji proizilaze iz kvantne kriptografije daju osnovu za dalji razvoj protokola u klasičnoj kriptografiji.

Ueli Maurer je uvideo mogućnosti drugog dela *BB84* protokola i teorijski prikazao novi protokol, poznat pod nazivom „Satelitski Scenario“. Prvi deo protokola *BB84* koji zahteva jednosmerni kvantni kanal „zamenio“ satelitom koji slabom snagom konstantno emituje slučajne signale. Emitovani signali predstavljaju lošu kopiju signala koji je na satelitu. Baš iz razloga što je signal slab, svaki učesnik u protokolu će dobiti korelisani niz u odnosu na drugog učesnika, ali sa greškama na različitim mestima – dakle isto što proizilazi iz prvog dela *BB84* protokola.

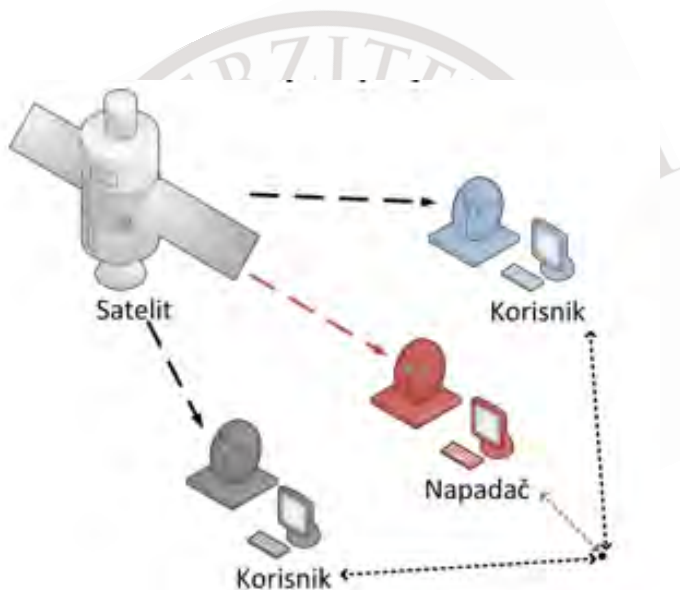
Jedan od najznačajnijih protokola iz protokola u kvantnoj kriptografiji je *BB84*. *BB84* zahteva dva komunikaciona kanala, jedan je jednosmerni kvantni kanal – optička veza između dva učesnika koja omogućava prenos svetlosti (fotona), dok je drugi dvosmerni javni kanal. Nakon prvog dela protokola u kome se koristi jednosmerni kvantni kanal, dva učesnika imaju korelisane (sadrže zajedničku informaciju) ali različite sekvence bitova koje je potrebno u drugom delu protokola ujednačiti kako bi dobijeni nizovi bili iskorišćeni kao materijal za ključ. Drugi deo *BB84* protokola, deo u kome se dva različita niza ujednačavaju, predstavlja takozvani kaskadni protokol ili mogućnost za polaznu tačku daljeg razvoja.

U narednim delovima rada biće prikazana detaljna analiza protokola za ispravljanje grešaka na korelisanim nizovima koje je delom razvio Ueli Maurer, a koje delom proizilaze iz kaskadnog protokola, kao i razvoj ovakvog protokola i jedne naše implementacija u savremenim računarskim mrežama.

Satelitski scenario je predstavljen tako da zahteva nekakav centralni izvor slučajno generisanih nizova (satelit) sa obaveznom uslovom da svaki učesnik, koji bi „slušao“ ono što satelit emituje, dobija signal sa greškama na različitim mestima u odnosu na originalni – emitovani signal. Možemo pretpostaviti da različiti faktori mogu da uzrokuju pojavu šuma u tom komunikacionom kanalu. Za ovakvu name-

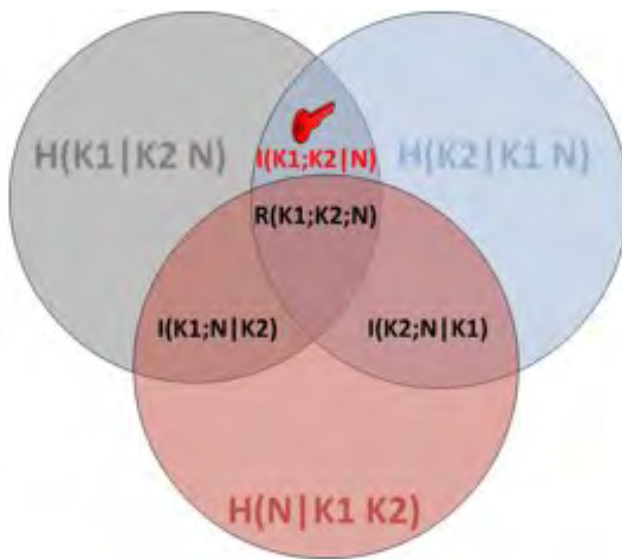
nu, pravi satelit bi bio idealno rešenje, ali ipak ne deluje moguće izvesti tako nešto. Potrebno je rešiti ovaj problem protokola kako bi protokol bio primenljiv u praktičnim mrežnim sistemima za komunikaciju. Na primer, bezbedna komunikacija između dva računara u istoj mreži.

Osim toga što ovaj protokol omogućava razmenu simetričnog ključa bez ikakvih unapred poznatih parametara, ovaj protokol takođe teorijski ne ograničava dužinu ključa koji će biti ustanovljen. Dakle, moguće je koristiti ovaj protokol za uspostavljanje ključeva većih dužina, što otvara mogućnosti za sintezu perfektne bezbednost. Implementacijom ovog protokola bi se rešio problem nedokazivo bezbednih šifara i uvelo korišćenje dokazivo bezbedne šifre – *OneTime pad*.



Slika 6.1 Apstraktna šema protokola „Satelitski scenario“

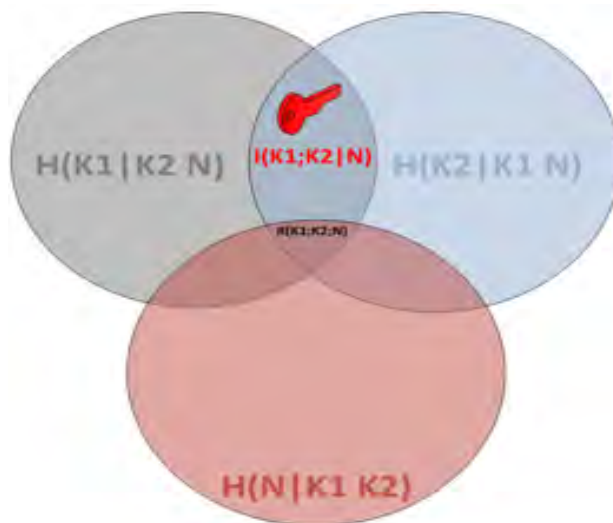
Deo protokola koji se bavi ispravljanjem grešaka u korelisanim nizovima tj. procesom usaglašavanja nizova, sastoji se od tri faze. Prva faza je destilacija prednosti (engl. *Advantage Distillation*), druga faza je usaglašavanje informacija (engl. *Information Reconciliation*) i treća faza je pojačavanje privatnosti (engl. *Privacy Amplification*). Detaljno će biti razmotrene i informaciono slikovito prikazane sve tri faze ovog protokola.



Slika 6.2 Dijagram početnih stanja, informaciona analiza

Nakon emitovanja slučajnih nizova, dijagram početnog stanja koji predstavlja informacione mere je prikazan na slici (Slika 6.2). Pretpostavka je da su sve tri strane dobile podjednako slične ili različite nizove sa zamišljenog satelita u ovom teorijskom scenariju. Vidimo sa slike prostor u kome se nalazi materijal koji će kasnije Alisa i Bob iskoristiti za generisanje zajedničkog ključa. Taj prostor je označen sa $I(K1;K2|N)$.

Sledeća faza je destilacija prednosti. Pretpostavlja se da emitovani signal satelita nikada ne slušaju samo legitimni korisnici protokola već i treća strana koja za nas predstavlja napadača. Destilacija prednosti se svodi na smanjivanje uzajamnih informacija između Alise i Boba, u ovom scenariju dve prijateljske strane koje žele da uspostave zajednički ključ, a sa druge strane ova faza protokola smanjuje uzajamnu informaciju između Alise i napadača i Boba i napadača (Trudi). Ova faza se direktno oslanja na model postavljen od strane teorijsko informacione analize. Dijagram novih stanja između Alise i Boba je predstavljen na slici (Slika 6.3). Vizuelno možemo da primetimo da je prostor materijala za budući kriptološki ključ značajno porastao, zapravo uzajamna informacija između Alise i Boba se povećala, dok je uzajamna informacija sa napadačem smanjena na minimalnu količinu informacija.

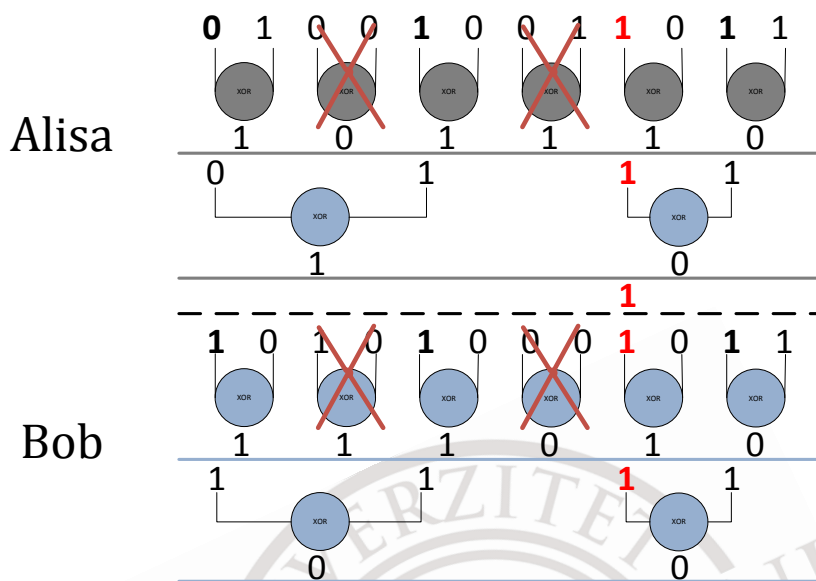


Slika 6.3 Stanja dijagrama posle destilacije prednosti

Destilacija prednosti ili invertovanje kanala počinje tako što legitimni korisnici (Alisa i Bob) u međusobnoj javnoj diskusiji „govore“ jedno drugome parne bitove računane za svaki par bitova iz originalnog niza. Dakle, originalni niz se deli na parove od po 2 bita, za svaki par se računa parnost, i ako su bitovi parnosti isti kod oba korisnika, korisnici zadržavaju prvi ili levi bit para. Ako se bitovi parnosti razlikuju, korisnici ne zadržavaju nijedan bit iz izdvojenog para i taj par se odbačuje iz protokola.

Ova faza protokola može sadržati nekoliko runde. Teorijski model koji je Maurer izneo, pretpostavlja tri runde ove faze protokola. Broj rundi može u praksi zavistiti od toga, kolika je pretpostavljena greška između legitimnih korisnika.

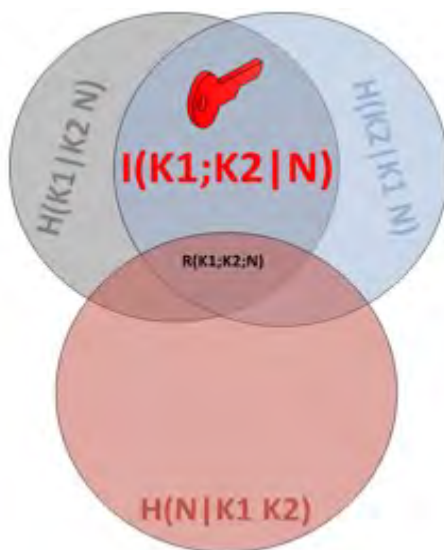
Na slici (Slika 6.4) prikazan je metod faze za destilaciju prednosti. U prvom redu, 12 bitova pripada Alisi, dok drugih 12 bitova u drugom redu pripada Bobu. Oni ih dele na parove i računaju njihovu parnost. Za prva dva bita kod Alise (0 i 1) parnost 1, a kod Boba (0 i 1) parnost je takođe 1. U tom slučaju Alisa zadržava 0, a Bob zadržava 1 i td. Parovi kod kojih je parnost različita su precrtani i odbačeni.



Slika 6.4 Proces destilacije prednosti

Sledeća faza je usaglašavanje informacija. Ova faza predstavlja proces u kome se dva niza u potpunosti izjednačavaju. Posmatra se niz jednog korisnika u odnosu na niz drugog, na način gde jedan niz predstavlja originalnu sekvencu, dok drugi niz kod drugog korisnika predstavlja isti taj niz ali sa greškama. Shodno tome, usaglašavanje informacija predstavlja proces ispravljanja grešaka u nizu kod jednog od korisnika. Ovaj proces je nalik na tehnike iz teorije o zaštitnom kodovanju u kanalima sa prisustvom šuma.

Proces usaglašavanja informacija počinje tako što se nizovi kod u ovom slučaju Alise i Boba, podele u blokove unapred određene dužine, zatim se za svaki blok računa bit parnosti. Ako se na bloku istog indeksa (npr. na drugom bloku u sekvenci i jednog i drugog korisnika) bit provere parnosti razlikuje, to znači da postoji razlika u tom bloku ili greška kod kod Boba, ukoliko posmatrao Alisin niz kao originalni u toj fazi protokola. Treba napomenuti da ovakva provera može da detektuje samo neparan broj grešaka u bloku – jer ako postoje dve greške u bloku, bit parnosti će biti „0“, a to će kod ove tehnike značiti da ne postoje greške. Iz tog razloga bitno je u zavisnosti od mesta primene proceniti optimalan broj rundi u fazi koju Maurer naziva destilacija prednosti.

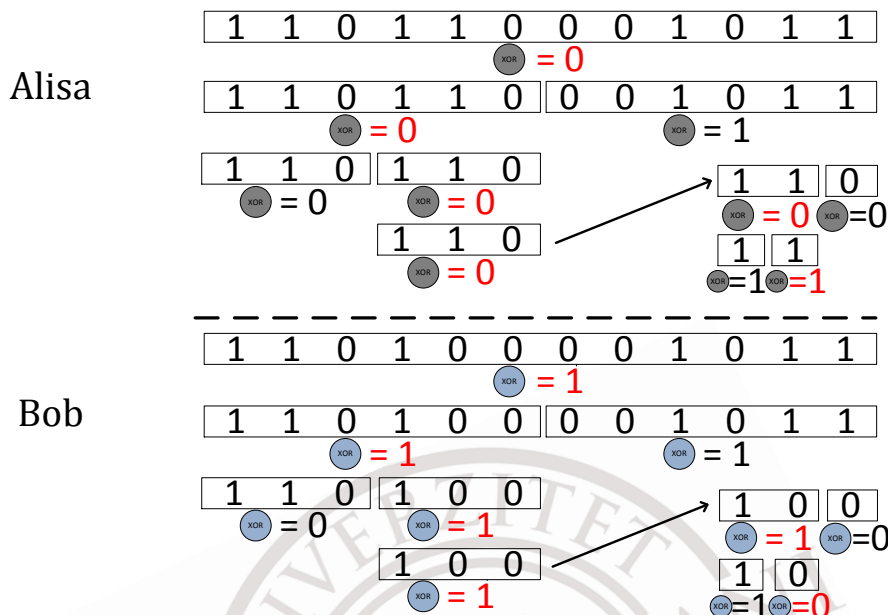


Slika 6.5 Stanja dijagrama nakon usaglašavanja informacija

Takođe, faza usaglašavanja se obavlja iz više rundi, pa sve dok se ne isprave sve greške. Broj rundi će zavisi od optimalne veličine blokova, dok će veličina blokova po rundama zavisi od osobine šuma koji je bio prisutan u kanalu na početku ovog protokola ili u momentu kada su signali emitovani sa satelita na zemlju.

Veličina blokova je takođe promenljiva zbog postojanja rafalnih grešaka „engl. *burst-error*“ koje se mogu javiti u nizu koji se ispravlja. Menjanjem veličine blokova se dobija sličan efekat kao kada se primeni interliver nad nizovima.

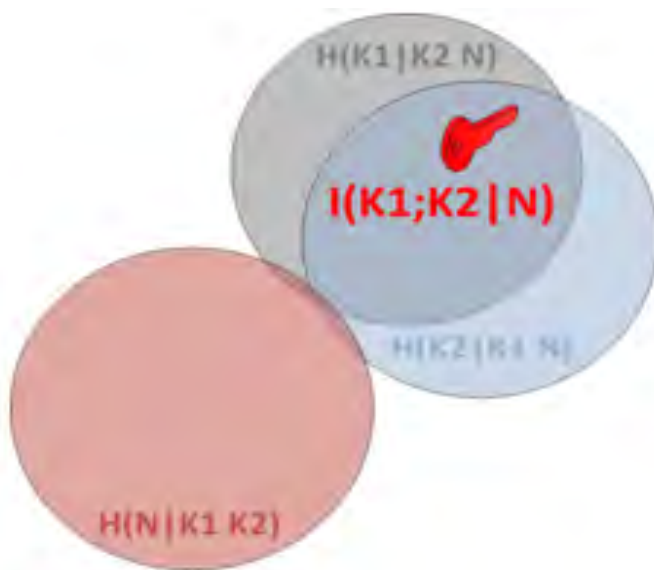
Na slici (Slika 6.6) prikazan je proces usaglašavanja informacija, nad nizovima koji su preostali nakon destilacije prednosti. Nizovi koji preostanu nakon faze usaglašavanja, predstavljaju materijal za ključ koji će Alisa i Bob iskoristiti za generisanje zajedničkog simetričnog ključa.



Slika 6.6 Proces usaglašavanja informacija

Dolazimo do faze za pojačavanje privatnosti. Možemo da kažemo da je ova faza poslednja faza protokola. Ova faza predstavlja metod za potpuno izbacivanje napadačeve (Trudi) uzajamne informacije sa nizovima legitimnih strana (Alisa i Bob). Ovo je postignuto primenom slučajno izabrane funkcije nad oba niza legitimnih strana. Funkcije koje se primenjuju u ovoj fazi, pripadaju zatvorenom skupu univerzalnih heš funkcija, čiji rezultat predstavlja krajnji ključ koji će se koristiti u kriptografskim mehanizmima za šifrovanje.

Ukratko ćemo objasniti korake ove faze. Prvi korisnik bira funkciju koja će se primeniti na slučajan način. Nakon toga, prvi korisnik šalje opis funkcije drugom korisniku kako bi na strani drugog korisnika bila primenjena ista funkcija. Opis je unapred dogovoren, može predstavljati nekakav parametar ili broj koji određuje tačnu funkciju iz zatvorenog skupa funkcija.



Slika 6.7 Dijagram stanja posle pojačavanja privatnosti

Ovaj protokol je apstraktni i iz tog razloga je i teorijski protokol, koji je u svetu nauke poznat pod imenom „Satelitski scenario“. Autor ovog perfektnog protokola ili bezuslovno bezbednog protokola je naučnik Ueli Maurer, koji je protokol prikazao samo na teorijskim osnovama i projektovanim teorijskim ograničenjima koje zajedno čine glavne teorijske okvire ovog protokola. Na osnovu našeg iskustva u oblasti bezbednosti na fizičkom sloju, prikazaćemo u poslednjem odeljku ovog poglavlja jednu našu praktičnu implementaciju ovog protokola u lokalnoj računarskoj mreži. Na ovaj način smatramo da smo pronašli adekvatnu ekvivalentnu šemu protokola „Satelitski scenario“, na osnovu dobijenih rezultata i rigoroznih teorijsko informacionih analiza koje su bile neizostavne za taj rad.

6.2. RAZMENA KLJUČA 2: WAYNER WIRE-TAP KANAL

Da bismo rešili problem distribucije ključeva na bezbedan način kod *One-Time* pad, mogli bismo doći u iskušenju da generišemo duge pseudo slučajne nizove koristeći čisto slučajna inicijalna stanja čija je dužina u odnosu na proizvod generatora neuporedivo manja. Međutim, teorija informacija pokazuje da je neodređenost napadača (Trudi) određena sa brojem slučajnih bitova u ključu. Ukoliko je ključ manji (posmatrano u kontekstu informacionih bitova), veća je verovatnoća da će napadač uspeti da izdvoji neke informacije iz kodnih reči - šifrata. U tom slučaju, jedina prepreka sa kojom je napadač susretnut je računarska kompleksnost, koja vodi direktno do koncepta računarske bezbednosti. Dobro poznata pravila za bezbedan rad *One-Time* pad šifre su verovatno odgovorna za skepticizam kod kriptografskih praktičara, zbog čega odustaju od teorijsko informacione bezbednosti. Već sada se vidi na prvi pogled, da je model *One-Time* pad šifre podobno komunikaciono bezbednosno rešenje, moguće i za širu primenu. Za širu primenu ove perfektne šifre neophodno je razmotriti nove metode za teorijsko informacionu distribuciju ključeva na fizičkom sloju bezbednosti. Prelazimo na sledeći primer.

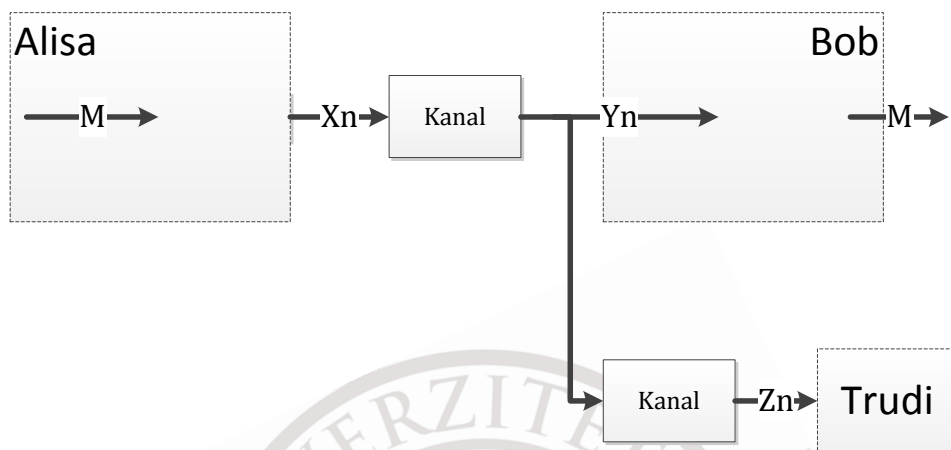
Kao što je pomenuto ranije, slučajni šum je sastavni element skoro svih komunikacionih kanala. U nastojanju da razume ulogu šuma u kontekstu bezbednih komunikacija, Viner (*Wayner*) je predstavio model kanala sa prisluškivanjem na slici (Slika 6.8). Osnovne razlike između ovog pristupa i Šenonovog originalnog perfektnog sistema su:

- legitimni predajnik koduje poruku M u kodne reči X^n koja se sastoji od n simbola, koji se šalju preko kanala sa čumom do legitimnog prijemnika.
- prisluškivač uzima poruku sa šumom, označenu sa Z^n , koja je jednaka sa signalom Y^n koja se dostupna na prijemniku.

Pored navedenih razlika, Viner je predložio novu definiciju tajnosti. Umesto ekvivokacije napadača, gde važi pretpostavka da neodređenost napadača treba da bude jednaka entropiji poruke, sada razmatramo o ekvivacionoj stopi:

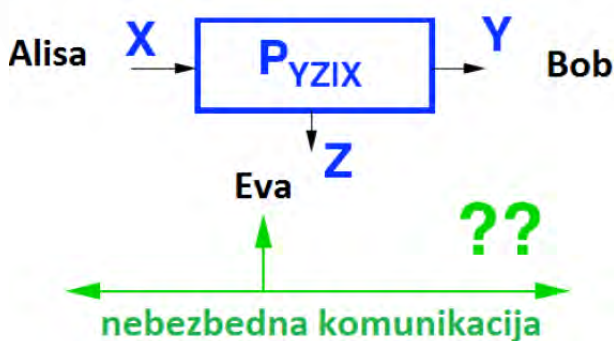
$$(1/n)H(M|Z^n),$$

koja može biti proizvoljno blizu stopi entropije poruke $(1/n)H(M)$ za dovoljno velike dužine šifrata n .



Slika 6.8 Vinerov model kanala

Sa ovim blažim bezbednosnim ograničenjem, tada može da se pokaže da postoje takvi kanalni kodovi koji garantuju asimptotski oboma proizvoljno malu verovatnoću greške na strani prijemnika i tajnosti. Takvi kodovi su kolokvijalno poznati kao kodovi prisluškivanja (engl. *Wiretap*). Maksimalna brzina prenosa koja se može postići pod ovom pretpostavkom zove se kapacitet tajnosti, a može da se pokaže da Z_n onoga ko prisluškuje, sadrži više grešaka od Y_n na prijemniku.



Slika 6.9 Kapacitet tajnosti

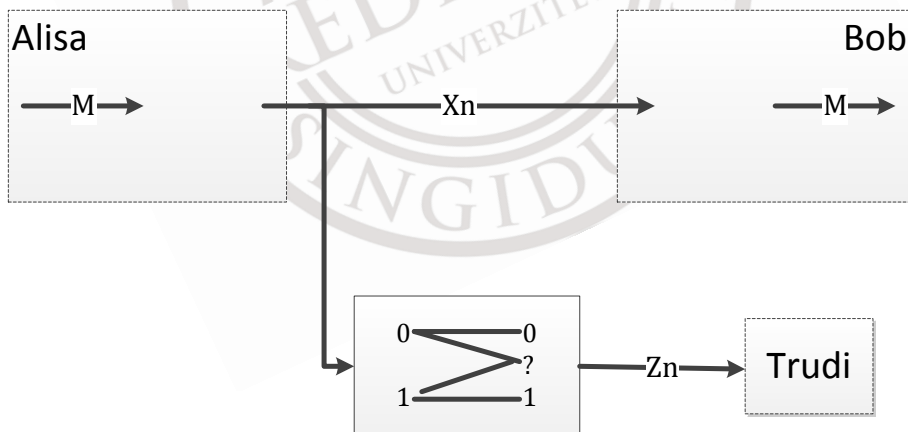
Kapacitet tajnosti kanala je definisan sledećim izrazom:

$$\text{kapacitet tajnosti} \geq I(X;Y) - I(X;Z),$$

a ako je kapacitet tajnosti jednak 0, tada je napadačev (Trudi) kanal bolji od kanala između legitimnih strana i tada je komunikacija nebezbedna.

U 70-im i 80-im godinama, uticaj Vinerovih rezultata bio je ograničen zbog nekoliko važnih prepreka. Prvo, praktični kodovi za realizaciju ovog kanala nisu bili dostupni. Drugo, model kanala sa prisluškivanjem podrazumeva da napadač prima zašumljene verzije signala legitimnog prijemnika je prilično nerealna. Pored toga, pre nego što se pojavio pojam „kapacitet tajnosti“, teorijsko informaciona bezbednost se našla u senci *Diffie-Hellman* protokola koji je razvijen na osnovama kriptografije sa javnim ključem, koja se oslanja na matematičke funkcije za koje se veruje da su teško izračunive i od tada dominira u oblasti bezbednosnih istraživanja.

Iako su dosadašnji rezultati zasnovani na kapacitetu tajnosti, dokazali postojanje sposobnih kodova koji garantuju pouzdanu komunikaciju pod uslovom da je zadovoljen uslov tajnosti, ali i dalje nije jasno kako mogu takvi kodovi da budu konstruisani praksi. U nastavku razmatraćemo konstrukciju kanalnog kodovanja za postizanje tajnosti.



Slika 6.10 Komunikacija preko binarnog kanala sa brisanjem

Razmislite o modelu prikazanom slici (Slika 6.10), u kom Alisa želi da pošalje jedan bit informacije Bobu preko kanala bez šuma, dok je kanal koji koristi Trudi binarni kanal sa brisanjem *BEC* (engl. *Binary erasure channel*), koji briše poneki

ulazni simbol sa nekom verovatnoćom e . BEC kanal je uobičajeni komunikacioni model kanala korišćen u teoriji kodovanja i teoriji informacija za različite analize. U ovom modelu, predajnik šalje bit (0 ili 1), a prijemnik prima bit ili dobija poruku da bit nije primljen ili "izbrisan".

Razmotrimo sada ovaj model kanala. Ako Alisa pošalje nekodovani bit poruke, tada je Trudi sposobna da primi isti sa verovatnoćom $1 - e$, što dovodi do ekvivokacije jednake sa e . Sledi da, ukoliko je $e = 1$, tada je Trudi u stanju da dobije netrivialnu količinu informacije.

Alternativno, Alisa može koristiti neki koder koji dodeljuje jednu ili više kodnih reči svakoj od dve moguće poruke, 0 ili 1. Pretpostavimo da ona uzima sve binarne sekvence dužine n i mapira ih na takav način da onima sa parnim paritetom odgovara $M = 0$, a onima sa neparnim paritetom odgovara $M = 1$. Ako Bob primi jednu od ovih kodnih reči preko kanala bez šuma, on može da dobije tačnu vrednost poruke određivanjem pariteta primljene kodne reči. Trudi, s druge strane, ostaje sa nekim prosekom od n brisanja. Čim se jedan ili više bitova brišu, Eva gubi svoju sposobnost da odredi paritet binarne sekvence u prenosu. Ovaj događaj se dešava sa verovatnoćom $1 - (1 - e)^n$ i to može da se pokaže kao:

$$H(M|Z^n) \geq 1 - (1 - e)^n,$$

gde n teži beskonačnosti. Drugim rečima, za dovoljno velike dužine kodnih reči, dobijamo ekvivokaciju koja je proizvoljno blizu entropije poruke. Nedostatak ove kodne šeme je brzina prenosa od $1/n$ koje teži nuli asimptotski sa n , što je dobro. Alisa i Bob mogu bezbedno da komuniciraju generisanjem više kodnih reči za istu poruku, ali tajnost koja je postignuta plaća cenu u brzini prenosa.

Intuicija koja je razvijena na javnom kanalu sa brisanjem, treba biti prenošena na više opštih kanala. Ako Bobov kanal indukuje manje grešaka od Trudi, Bob i dalje treba da bude u stanju da oporavi poruke koristeći kanalne kodove, nasuprot tome, Trudi treba da ostane sa više mogućih kodnih reči i poruka. Nažalost, do današnjeg dana, praktična konstrukcija javnog kanala je poznata samo za nekoliko specifičnih kanala.

Do sada smo pretpostavljali da je Trudi pasivan napadač, koji želi da izvuče što je više moguće informacija iz kanala. Međutim, pored pasivnog napada, Trudi ima širok spektar aktivnih napada na raspolaganju. Trudi može da imitira Alisu ili da

kod Boba izazove dodatnu konfuziju, tako što će presretnuti saobraćaj, izmeniti poruke koje su poslate preko kanala sa šumom ili samo jednostavno ometati Alisu i Boba u komunikaciji.

Autentifikacija pošiljaoca je prećutna pretpostavka u većini doprinosa teorijsko informacione bezbednosti. Osim u posebnim i retkim slučajevima, uspostavljeni ključ između Alise i Boba zahteva potvrdu autentičnosti sa obe strane. Potrebno je obezbediti autentifikaciju. Na primer, ako Alisa i Bob koriste bežične mreže, prijemnik može da poveže određeni kanal sa impulsnim odzivom sa određenim predajnikom i da je praktično nemoguće da se protivnik nalazi na drugoj poziciji da bi mogao da generiše slične impulsne odzive na prijemniku. Sa autentifikacijom na ovaj način napadač ne može da imitira legitimne strane komunikacije i da falsifikuje poruke.

Međutim, napadač može da odluči da ometa komunikaciju nekim metodama za ometanje signala. Treba istaći da ometanje signala nije ograničeno samo na aktivnog napadača. Združeno ometanje, kod koga jedan ili više legitimnih korisnika šalje kodovane poruke, povećava konfuziju kod napadača, što efikasno utiče na povećanje kapaciteta tajnosti. Sofisticirana obrada signala, pre svega kroz upotrebu višestrukih antena, takođe može dodatno poboljšati bezbednosne prednosti.

6.3. RAZMENA KLJUČA 3: KARTE

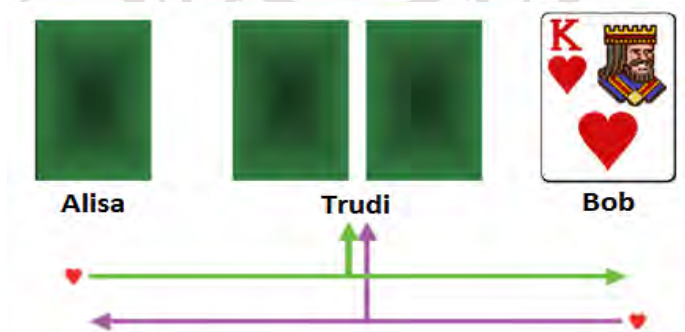
U ovom jednostavnom protokolu za uspostavljanje tajnog ključa pretpostavimo da postoje samo četiri karte.



Slika 6.11 Četiri karte koje se koriste za ovaj jednostavni protokol

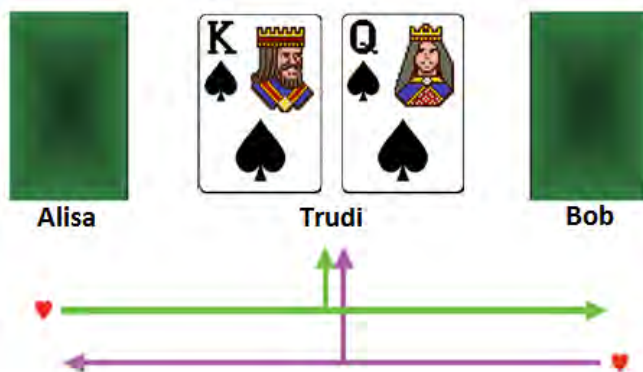
Osoba od poverenja meša karte i deli redom Alisi, Bobu i Trudi. Alisa i Bob sprovode jednu od sledećih slučajeva, koji zavise od podeljenih karata:

- A. Alisa i Bob javnim kanalom otkrivaju boje svojih karata;
- B. Ako je boja identična i kod Boba i kod Alise, tada se slažu oko bita tajnog ključa „0”, ako Alisa ima kralja (što implicira da Bob ima kraljicu), odnosno oko bita tajnog ključa „1”, ukoliko Alisa ima kraljicu (što implicira da Bob ima kralja);
- C. Ako su boje karata Alise i Boba u tekućoj podeli različite, odustaju od uspostavljanja zajedničkog bita tajnog ključa u ovoj rundi;



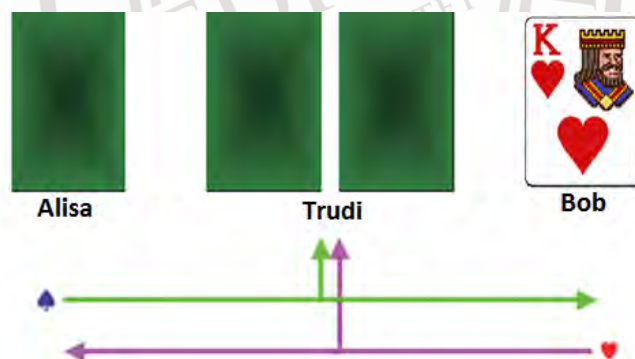
Slika 6.12 Karte - slučaj A.

U slučaju B. sa slike (Slika 6.12), pošto se boje slažu i Bob ima kralja, Alisa u tom slučaju mora da ima kraljicu. Prema pravilima protokola, Alisa i Bob se slažu oko bita tajnog ključa „1”.



Slika 6.13 Karte - slučaj B.

U slučaju B. sa slike (Slika 6.13), Trudi zna da Alisa i Bob imaju istu boju, ali ne zna ko ima kralja a ko kraljicu, pa stoga da li je bit tajnog ključa oko koga su se složili „0” ili „1”.



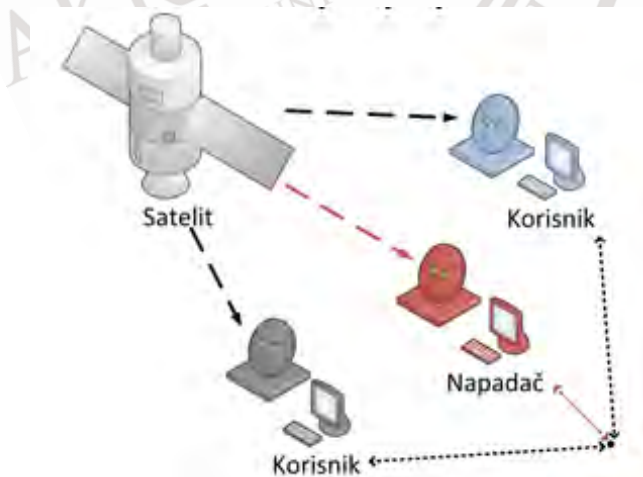
Slika 6.14 Karte - slučaj C.

U slučaju C. sa slike (Slika 6.14), Bob ima kralja srce i zna da Alisa ima pik, ali ne zna da li je to kralj pik ili dama pik. U ovom slučaju Alisa i Bob odustaju od uspostavljanja zajedničkog tajnog ključa i prelaze na novu rundu deljenja. Broj rundi zavisice od željene dužine tajnog ključa između Alise i Boba.

6.4. JEDAN ALGORITAM ZA RAZMENU KLJUČEVA U LOKALNOJ RAČUNARSKOJ MREŽI

U ovom odeljku bavimo se implementacijom teorijskog protokola za distribuciju kriptoloških ključeva preko javnog komunikacionog kanala. Polazeći od teorijskih osnova i pregleda aktuelnog stanja u oblasti istraživanja, predložićemo jednu realnu implementaciju protokola pod nazivom „Satelitski scenario“. Realizacija protokola trenutno postoji samo na teorijskoj osnovi. Protokol o kome je reč podrazumeva razmenu kriptološkog ključa između bilo koja dva korisnika bez poznavanja početnih parametara. Ovo je jedan realan praktični primer vezan za bezbednost na fizičkom sloju.

Osnovni ideja je generisanje i distribucija kriptoloških ključeva preko javnih komunikacionih kanala u savremenim računarskim mrežama, kao i razvoj sopstvenog rešenja na osnovu jasno definisanih teorijskih osnova. Iz navedenog zaključujemo da je jedini dobar bezbedan način, upotreba ključeva većih dužina u algoritmima perfektnih kripto sistema ili u algoritmima koji nude praktičnu bezbednost, za koje je potrebno generisati i distribuirati ključeve 128 ili 256 bitova. Iz tog razloga potrebno je razvijati protokole koji obezbeđuju distribuciju takvih ključeva.



Slika 6.15 Apstraktna šema protokola

Sve faze protokola se odvijaju kroz javnu diskusiju. U inicijalnoj fazi protokola svi korisnici dobijaju binarne nizove koji su međusobno korelisani. Ovi nizovi su emitovani iz informacionog izvora koji je zajednički za sve učesnike i predstavlja-ju lošu kopiju originalnog niza na izvoru koji nikome od učesnika nije poznat.

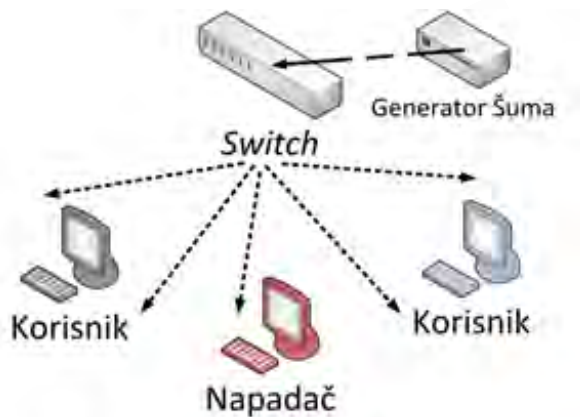
Ovaj protokol je zasnovan na zajedničkoj informaciji između bilo koja dva učesnika, preko koje se kroz naredne faze protokola vrši estimacija simetričnog kriptološkog ključa. Pored navedenih mogućnosti protokola, jedino ograničenje je nemogućnost realizacije protokola u komunikacionom kanalu bez šuma. Za potrebe rada će biti programski razvijene sve faze protokola i definisana implementacija jedne ekvivalentne šeme koja po svojim karakteristikama odgovara Mauerovom „Satelitskom scenariju“.

Protokol o kome diskutujemo predstavlja jedan pokušaj implementacije Mauero-vog protokola „Satelitski scenario“. Predstavljeno je rešenje u kome je satelit zamenjen jednim generatorom slučajnih brojeva i na taj način je protokol implementiran u savremenu računarsku mrežu. Potrebno je uvesti generator (generator će imati ulogu satelita) u računarsku mrežu, takav da minimalno remeti već postojeću infrastrukturu mreže i koristi već postavljene provodnike. Satelit je hardverski generator šuma, zasnovan na termičkom šumu diode. Generator proizvodi šum u frekventnom opsegu koji se može čuti i moguće je korišćenjem zvučne kartice snimiti šum i daljim procesiranjem ga konvertovati u nizove bitova. Količina bitova koja se može dobiti iz jedne sekunde snimljenog materijala zavisi od brzine smplovanja signala i preciznosti smplovanja. Ako se šum smp- ljuje brzinom od 8000 smplova u sekundi (8000 Hz) i preciznošću od 16 bita, za jednu sekundu se dobija: $8000 \cdot 16 = 128000$ bitova.

Generisan šum se može prenositi do svakog računara u mreži preko neiskorišće- nih provodnika u kابلu korišćenim za umrežavanje. U ovom slučaju potrebno je modifikovati konektor *UTP* kabla tako da je moguće bez oštećenja provodnika preuzeti audio signal i usmeriti ga u ulaz zvučne kartice računara. Drugi način za prenos šuma do računara je postavljanje dodatnih kablova koji bi služili samo u te svrhe. Dovođenjem signala do svakog računara napravljena je situacija koja se može poistovetiti sa situacijom u teorijskim radovima Ueli Maurera, gde je u o- vom slučaju generator šuma satelit (Slika 6.16). U narednim koracima potrebno je da korisnici koji žele da razmene zajednički ključ, snime signale, zatim predsta-

ve snimljeni signal u obliku niza bitova kako bi bilo moguće ostvariti korake objašnjene u nastavku ovog odeljka.

Eksperimentalni rad obavljen je unutar elektronske učionice gde je na raspolaganju bilo preko 100 umreženih računara. Distribucija zvučnog signala šuma obavljena je korišćenjem posebnih kablova koji direktno spajaju generator i ulaze zvučnih kartica računara. Karakteristike računara, mrežne opreme i zvučnih kartica koje poseduju su predstavljene u tabeli (Tabela 6.1).



Slika 6.16 Predložena šema protokola

Tabela 6.1 Eksperimentalni računarski sklop

Računar 1:	HP Pro, Intel i3-2120 @ 3.30GHz, 4GB Ram
Računar 2:	Fujitsu Siemens ESPRIMO 5925 EPA
Zvučna kartica 1:	Realtek High Definition Audio
Zvučna kartica 2:	ALC262 /Realtek
Switch:	Cisco small bussiness SRW2052

Iz tabele se može zaključiti da su sve komponente kao i računari korišćeni u eksperimentalnom radu standardnih karakteristika i nisu potrebne dodatne izmene. Nakon povezivanja računara i generatora, potrebno je snimiti šumni signal. U svrhe eksperimentalnog rada, signal je sniman korišćenjem softvera za obradu zvuka pod nazivom (engl. *Sound Forge*).

Problem koji nastaje kod snimanja signala je sinhronizacija. Naime, potrebno je sinhronizovati početak snimanja na dva računara koja treba da razmene zajednički ključ. Kod snimanja bez vremenske sinhronizacije, gde korisnici „usmeno“ vrše sinhronizaciju, može doći do situacije u kojoj su dva snimljena niza različita do 50%. U takvim uslovima nije moguće uspešno realizovati protokol do kraja.

Problem sinhronizacije je rešen preko softvera koji je iskorišćen za snimanje emitovanog signala. Pre svega potrebno je sinhronizovati vreme na svim računarima koji učestvuju u protokolu – što je jednostavno rešivo na operativnim sistemima, sinhronizacijom vremena preko zajedničkog servera za vremensku sinhronizaciju. Ovakva sinhronizacija se oslanja na *NTP* (engl. *Network Time Protocol*) i omogućava preciznost sinhronizacije do hiljaditog dela sekunde. Nakon uspešne sinhronizacije za zadatu vremensku toleranciju, softver snima emitovani signal sa generatora, ali zbog uticaja više spoljnih faktora, nijedan računar u mreži ne dobija identične sekvence.

U teorijski prikazanom satelitskom scenariju, greške između sekvenci različitih korisnika moraju biti u opsegu od 0% do 50%, pri čemu je kod 0% nemoguće izdvojiti zajedničku informaciju između dva korisnika jer svi korisnici imaju identične sekvence, a kod 50% je nemoguće izdvojiti zajedničku informaciju jer su sve sekvence potpuno različite. Idealna greška, odnosno razlika između dve sekvence korisnika je od 20% do 30%.

Snimanja signala bez vremenske sinhronizacije računara, greške između sekvenci se približavaju 50%, a u tom slučaju nije moguće izvući bilo kakvu zajedničku informaciju. Kada se signal snima sinhronizovano sa softverom, greška između sekvenci je oko 35%. U narednoj tabeli biće prikazan broj emitovanih bitova i broj zajedničkih bitova na kraju protokola.

Tabela 6.2 Prikaz grešaka sa i bez sinhronizacije

	Bez Sinhronizacije	Sa Sinhronizacijom
Trajanje snimanja	3 sekunde.	3 sekunde.
Generisani bitovi	417.791 bitova.	407.999 bitova.
Broj različitih bitova.	214.540 bitova.	143.307 bitova.
Greška	51.3 %	35.1 %

U tabeli su prikazani eksperimentalni rezultati. Iz rezultata vidimo da su vrednosti šuma idealni kod sinhronizovanog snimanja signala, jer na taj način dobijamo idealne vrednosti koje su zahtevane u ovom protokolu. Posle snimanja signala, dva korisnika treba da započnu preostale faze protokola (destilacija prednosti i usaglašavanje informacija). U tabeli (Tabela 6.3) prikazani su rezultati implementiranog protokola. Primenom metoda za destilaciju prednosti i usaglašavanja informacija, moguće je ustanoviti ključ dužine do 1544 bita, samo na osnovu 3 sekunde snimljenog signala.

Brzina ključa kod prikazanog eksperimenta dostiže 1.544 bitova za vreme od 5 sekunde. Za potrebe eksperimenta snimanje je trajalo tačno 3 sekunde sa početnih 407.000 bitova, kako bi se nakon faze destilacije prednosti i usaglašavanja informacija, izvuklo 1.544 bita zajedničke informacije između dva korisnika u mreži. Prikazano je 6 koraka destilacije prednosti i 2 koraka usaglašavanja informacija za koje je potrebno ukupno 2 sekunde preko algoritma napisanog u Java programskom jeziku. Na kraju protokola potrebno je uraditi i poslednji korak, a to je pojačavanje privatnosti na način na koji je opisan u ovom poglavlju.

Rezultati ove implementacije jasno pokazuju da se radi o potpuno ekvivalentnom scenariju u odnosu na vrednosti šuma u emitovanom signalu i da teorijski okviri postavljeni od strane Maurera i dalje važe. Brzinu ključa koju smo postigli je 308

bitova/s. Sa ovom brzinom ključa obezbedili smo razmenu ključeva velikih dužina koji u potpunosti zadovoljavaju potrebe današnjih kriptografskih algoritama.

Tabela 6.3 Dobijeni rezultati na kraju protokola

	Ukupno bitova	Različitih bitova	Greška
Početno stanje	407.999	143.307	35.1%
Destilacija prednosti 1	137.545	41.233	29.9%
Destilacija prednosti 2	46.717	10.864	23.2%
Destilacija prednosti 3	16.232	2.001	12.3%
Destilacija prednosti 4	6.723	295	4.3%
Destilacija prednosti 5	3.136	39	1.2%
Destilacija prednosti 6	1.544	6	0.3%
Usaglašavanje Info. 1 Veličina bloka = 5	1.544	1	0.06%
Usaglašavanje Info. 2 Veličina bloka = 4	1.544	0	0%

Servis autentifikacije u ovoj realizaciji protokola nije dostupan. Kombinacijom servisa sa viših slojeva, moguće je razviti jedan dovoljno pouzdan i bezbedan protokol zasnovan na teorijsko informacionoj i praktičnoj bezbednosti.

LITERATURA

A. Burnett, F. Byrne, T. Dowling, and A. Duffy. A Biometric Identity Based Signature Scheme. [Radovi] // Applied Cryptography and Network Security Conference. - New York : [s.n.], 2005.

A. Goh, D.C. L. Ngo Computation of Cryptographic Keys from Face Biometrics [Radovi] // Proc. Int'l Federation for Information Processing 2003. - 2003. - str. 1-13.

A. J. Viterbi and J. K. Omura. Principles of Digital Communication and Coding. [Knjiga]. - New York : McGraw-Hill, 1979.

Agaian S.S. Hadamard Matrix and Their Applications [Radovi]. - [s.l.] : Springer Verlag, 1985.

Aiden A. Bruen, Mario A. Forcinito Cryptography, information theory, and error-correction [Knjiga]. - New Jersey : A John Wiley & Sons, 2005.

Ari Juels, Martin Wattenberg A fuzzy commitment scheme [Radovi] // CCS '99 Proceedings of the 6th ACM conference on Computer and communications security. - New York : ACM, 1999. - str. 28-36.

Bennet C. H., Bessette F. / Brassard G. Experimental Quantum Cryptography [Naučni radovi]. - [s.l.] : Journal of Cryptology Vol.5, 1992.

Blahut, Richard E. Theory and Practice of Error Control Codes [Knjiga]. - [s.l.] : Addison-Wesley, 1983.

Boneh Dan, Dunworth Christopher / Lipton Richard J. Breaking DES Using a Molecular Computer [Naučni radovi]. - Princeton : Princeton, NJ 08544.

C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B.V.K. Vijaya Kumar Biometric Encryption [Radovi] // ICSA Guide to Cryptography, McGraw-Hill. - 1999.

Daugman J. The Importance of Being Random: Statistical Principles of Iris Recognition [Časopis] // Pattern Recognition. - 2003. - str. 279-291.

Diffie Whitfield / Hellman Martin E. New Directions in Cryptography [Časopis] // IEEE Transactions on Information Theory. - 1976. - 6 : Tom. VOL. IT-22.

Dušan B. Drajić, Predrag N. Ivaniš Uvod u teoriju informacija i kodovanje [Knjiga]. - Beograd : Akademska misao Beograd, 2009.

F. Bavaud, J.-C. Chappelier, J. Kohlas An Introduction to Information Theory and Applications [Knjiga]. - 2005 : [s.n.].

F. Hao, C.W. Chan Private Key Generation from On-Line Handwritten Signatures [Časopis] // Information Management & Computer Security. - 2002. - str. 159-164.

F. Hernandez Alvarez, L. Hernandez Encinas, C. Sanchez Avila Biometric Fuzzy Extractor Scheme [Radovi] // The 2009 International Conference on Security and Management (SAM'09). - Las Vegas : WORLDCOMP'09, 2009. - str. 563-569.

F. Monrose, M.K. Reiter, Q. Li, S. Wetzel Cryptographic Key Generation from Voice [Radovi] // Proc. 2001 IEEE Symp. Security and Privacy, May 2001. - 2001.

F. Monrose, M.K. Reiter, R. Wetzel Password Hardening Based on Keystroke Dynamics [Radovi] // Proc. Sixth ACM Conf. Computer and Comm. Security (CCCS). - 1999.

Feng Hao, Ross Anderson, John Daugman Combining Crypto with Biometrics Effectively [Radovi] // IEEE TRANSACTIONS ON COMPUTERS. - [s.l.] : IEEE Computer Society, 2006. - str. 1081-1088.

FIPS DATA ENCRYPTION STANDARD (DES) [Naučni radovi]. - [s.l.] : Federal Information Processing Standards Publication 46-2, 1993.

FPIS ADVANCED ENCRYPTION STANDARD (AES) [Naučni radovi]. - [s.l.] : Federal Information Processing Standards Publication 197, 2001.

G.I. Davida, Y. Frankel, B.J. Matt, and R. Peralta On the Relation of Error Correction and Cryptography to an Off Line Biometrics Based Identification Scheme [Radovi] // Proc. Workshop Coding and Cryptography. - 1999.

H. A. Garcia-Baleon, V. Alarcon-Aquino, O. Starostenko, J. F. Ramirez-Cruz Bimodal Biometric System for Cryptographic Key Generation Using Wavelet [Radovi] // 2009 Mexican International Conference on Computer Science. - 2009. - str. 186-196.

<http://csis.org/> [Na mreži] // <http://csis.org/>. - CSIS Center for Strategic and International Studies, 2014.

Lang, Serge. Algebra [Knjiga]. - [s.l.] : Addison-Wesley, 1993. - T. Third Edition.

Lewis James Andrew [Na mreži]. - Center for Strategic and International Studies, 2014. - www.csis.org.

Lin, Shu and Daniel J. Costello, Jr. Error Control Coding: Fundamentals and Applications. Englewood Cliffs [Knjiga]. - [s.l.] : Prentice-Hall, 1983.

M. van der Veen, T. Kevenaar, G.-J. Schrijen, T. H. Akkermans, and Fei Zuo Face Biometrics with Renewable Templates [Radovi] // Proceedings of SPIE, Volume 6072: Security, Steganography, and Watermarking of Multimedia Contents VIII, Edward J. Delp III, Ping Wah Wong, Editors, 60720]. - San Jose : [s.n.], 2006.

Matthieu Bloch, Joao Barros Physical-Layer Security [Knjiga]. - Cambridge : United States of America by Cambridge University Press, New York, 2011. - T. 1.

Maurer Ueli M. Secret Key Agreement by Public Discussion [Naučni radovi]. - [s.l.] : IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 39, NO. 3, 1993.

Maurer Ueli M. Secret Key Agreement by Public Discussion [Časopis]. - [s.l.] : IEEE TRANSACTIONS ON INFORMATION THEORY, 1993. - 3 : T. 39.

Milan Milosavljević, Jovan Jovanović, Saša Adamović, Marko Šarac, Aleksandar Jevremović i Vladislav Mišković Protokol za generisanje i razmenu apsolutno tajnih kriptoloških ključeva putem javnih kanala u savremenim računarskim mrežama [Radovi] // 57 konferencija ETRAN 2013. - Zlatibor 03-07 : [s.n.], 2013.

Mladen Veinović, Saša Adamović Kriptologija 1 [Knjiga]. - Beograd : Univerzitet Singidunum, 2013. - T. 1.

N. M. Abramson. Information Theory and Coding. [Knjiga]. - New York : McGraw-Hill, 1963.

Nagarajan Rajagopal / Papanikolaou Nikolaos Classical Security Protocols for QKD Systems [Naučni radovi]. - [s.l.] : Department of Computer Science, The University of Warwick.

P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G.-J. Schrijen, A. M. Bazen, and R. N.J. Veldhuis. Practical Biometric Authentication with Template Protection [Radovi] // 5th International Conference, AVBPA. - Newyork : [s.n.], 2005. - str. 20-22.

R. Adler. Ergodic and mixing properties of infinite memory channels [Radovi]. - [s.l.] : Proc. Amer. Math. Soc, 1961. - 12:924-930.

R.L. Rivest A. Shamir, and L. Adleman* A Method for Obtaining Digital Signatures and Public-Key Cryptosystems [Naučni radovi]. - New York, NY : Communications of the ACM, 1978. - 10.1145/359340.359342.

Raymond W Yueng A new Outlook on Shannon Information Measures [Radovi] // IEEE Transactions on IT. - 1991. - T. 37.

Sanjay K, Danielle C, Emine K, Dijana P.D, and Bernadette D. Three Factor Scheme for Biometric-Based Cryptographic Key Regeneration Using Iris [Radovi]. - France : TELECOM & Management SudParisEvry, 2008.

SciEngines Break DES in less than a single day [Na mreži]. - SciEngines, 2009. - 23 April 2013. - <http://www.sciengines.com/company/news-a-events/74-des-in-1-day.html>.

Shannon C. E. A mathematical theory of communication [Časopis] // Bell System Tehnical Journal. - 1948. - str. 379-423.

Shannon Claude Communication Theory of Secrecy Systems [Naučni radovi]. - [s.l.] : Bell System Technical Journal 28, 1949. - 656-715.

Simmons G. J. Authentication theory/coding theory, in Advances in Cryptology [Knjiga]. - [s.l.] : CRYPTO '84, 1985. - T. Lecture Notes in Computer Science 196 .

Stamp Mark Information security [Knjiga]. - [s.l.] : A John Wiley & Sons, INC., Publication, 2005. - T. Second Edition.

T.C. Clancy, N. Kiyavash, D.J. Lin Secure Smart Card-Based Fingerprint Authentication [Radovi] // Proc. 2003 ACM SIGMM Workshop Biometrics Methods and Application (WBMA). - 2003.

Timothy I. Calver Captain, USAF AN EMPIRICAL ANALYSIS OF THE CASCADE SECRET KEY RECONCILIATION PROTOCOL FOR QUANTUM KEY DISTRIBUTION [Naučni radovi]. - [s.l.] : AIR FORCE INSTITUTE OF TECHNOLOGY, 2011. - AFIT/GIR/ENV/11-S01.

U. Martini, S. Beinlich. Virtual PIN: Biometric Encryption Using Coding Theory. BIOSIG: Biometric and Electronic Signatures [Radovi] // the 1st Conference on Biometrics and Electronic Signatures of the GI Working Group BIOSIG. - Darmstadt : [s.n.], 2003. - str. 91–99.

Van Lint, J. H. Introduction to Coding Theory [Knjiga]. - [s.l.] : Springer-Verlag, 1982.

Xavier Boyen, Voltage Security, Palo Alto Reusable Cryptographic Fuzzy Extractors [Radovi] // In 11th ACM Conference on Computer and Communications Security (CCS 2004). - New York : ACM Press, 2004. - str. 82-91.

Y. Dodis, L. Reyzin, A. Smith Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data [Radovi] // Eurocrypt 2004. - [s.l.] : Eurocrypt 2004, 2008. - str. 523-540.

DODATAK – HRONOLOŠKI PREGLED OBJAVLJENIH INCIDENATA NA INTERNETU U PERIODU OD 2006. DO 2012. GODINE.

U ovom poglavlju prikazaćemo hronološki najveće i najuspešnije napade na vladine institucije i visoko tehnološke kompanije. Ove napade možemo okarakterisati kao visoko tehnološki kriminal koji dovodi do gubitka više stotina miliona dolara. Svakako, ovim izveštajem nisu obuhvaćeni svi incidenti, neki napadi ostaju tajna velikih kompanija, koje tako žele da zaštite svoj ugled na tržištu.

Maj 2006. Mreža državnog sektora je hakovana, reč je o nepoznatim stranim uljezima, koji su preuzeli terabajte podataka. Kineski ili ruski špijuni su fizički pristupili državnom sektoru, onesposobili čuvaru, pristupili kabinetima sa fajlovima. Ovakav akt ima sve čino ve rata. Ovaj događaj vezan je za *cyber* prostor i teško se može detektovati.

Av gust 2006. Viši službenik vazduhoplovstva javno je izjavio „Kina je preuzela 10 do 20 terabajta podataka iz *NIPRNet* (ne klasifikovana vojna mreža)“.

Novembar 2006. Haker pokušao da proдре u američku vojnu mrežu, što je dovelo do zatvaranja institucije na dve nedelje, a zaražene mašine su obnovljene.

Decembar 2006. NASA je bila primorana da blokira emajlove sa prilozi ma pre lansiranja svemirskog broda, zbog straha da će biti hakovan lansirni centar. Kasnije, mediji su objavili da su planovi o najnovijim američkim svemirskim letilicama bili dostupni nepoznatim stranim uljezima.

April 2007. Ministarstvo trgovine je moralo da angažuje biro za industrijsku bezbednost u *oflajn* mrežama na nekoliko meseci, jer je mreža hakovana os strane nepoznatih stranih uljeza. Biro za bezbednost je uradio reviziju poverljivih informacija i načina za raspolaganje sa njima.

Maj 2007. Univerzitet nacionalne odbrane je morao da obustavi rad sistema elektronske pošte, zbog hakerskog napada od strane nepoznatih hakera, koji su uspe li da postave špijunske softvere..

Maj 2007. Estonske vladine mreže su bile onemogućene u pružanju usluga od strane nepoznatih uljeza, najverovatnije po nalogu ruske vlade. Neki vladini Internet servisi su bili privremeno obustavljeni, kao i Internet bankarstvo. Ovaj

napad je okarakterisan kao visoko tehnološki napad, ne samo kao napad onesposobljavanja nekih servisa. Estonci su odgovorili veoma dobro. Međutim, stvorili su talas straha u *cyber* zavisnim zemljama poput *U.S.*

Jun 2007. Sekretar odbrane je preko naloga elektronske pošte bio žrtva hakerskog napada, nepoznatih napadača, kao i deo većeg niza napada za pristup i iskorišćenje ranjivosti mreže.

Avgust 2007. Britanska služba bezbednosti, Kancelarija francuskog predsednika i nemačke kancelarke Angele Merkel, bila je žrtva hakerskih napada, koji su prepoznati kao napadi iz Kine. Merkelova je čak uputila zvanično pitanje predsedniku Kine.

Septembar 2007. Izrael je prekinuo rad sirijske mreže za vazдушnu odbranu, navodno tokom bombardovanja sirijskog nuklearnog postrojenja.

Septembar 2007. Frensis Delon, generalni sekretar za narodnu odbranu u Francuskoj, izjavio je da su se u francuske informacione sisteme infiltrirale grupe iz Kine.

Septembar 2007. Britanske vlast saopštile su da su hakeri, za koje veruju da dolaze iz Kineske Narodnooslobodilačke armije, prodrle u mrežu spoljnih poslova i drugih ključnih odeljenja.

Oktobar 2007. Kinesko ministarstvo državne bezbednosti dalo je izjavu da su strani hakeri, 45% iz Tajvana i 25% iz *SAD*-a, pribavljali informacije iz kineskih ključnih oblasti. U 2006, Kina je saopštila da su u mrežama *CASIC*-a (engl. *China Aerospace Science & Industry Corporation*) pronađeni špijunski softveri tajnih službi i korporativnih lidera.

Oktobar 2007. Više od hiljadu zaposlenih u *ORNL*-u (engl. *Oak Ridge National Labs*) dobilo je elektronsku poštu sa prilogom koji kada se otvori, pruža mogućnost nepoznatom napadaču da pristupi njihovim bazama podataka.

Novembar 2007. Džonatan Evans, šef britanske službe bezbednosti (*MI5*), upozorio je 300 poslovnih firmi o povećanju Internet pretnji iz ruskih i kineskih državnih organizacija, govoreći, „veliki broj zemalja izvaja dosta vremena i energije da pribavi naše važne informacije o civilnim i vojnim projektima, na ovaj na-

čin dolaze do političke i vojne inteligencije na naš račun. Oni će u budućnosti razvijati sve više sofisticiranih visoko tehnoloških napada, koristeći Internet za upad u mreže".

Januar 2008. Zvaničnik *CIA* je izjavio, da agencija pouzdano zna za četiri incidenta u inostranstvu, gde su hakeri izazvali ili mogli da ometaju elektro napajanje za četiri grada.

Mart 2008. Južnokorejski zvaničnici tvrde da je Kina pokušala da upadne u korejske ambasade i vojne mreže.

Mart 2008. Američki zvaničnici izjavili da su američke, evropske i japanske kompanije doživele značajne gubitke intelektualne svojine i poslovnih informacija preko napada u vidu industrijske špijunaže u *cyber* prostoru.

April – Oktobar 2008. *WikiLeaks* izvestio da su hakeri uspešno ukrali 50 megabajta elektronske pošte sa priloženom dokumentacijom, kao i kompletan spisak korisničkih imena i lozinki iz neutvrđene vladine organizacije. Pretpostavlja se da neki od napada potiče iz Šangaja, sedište hakerske grupe povezane sa *PLATD (People's Liberation Army's Third Department)*.

Maj 2008. Indijski vesnik izvestio da je indijski zvaničnik optužio Kinu za hakisanje vladinih računara. Zvaničnik je izjavio da je jezgro kineskih napada skeniranje i mapiranje službenih mreža Indije za pristup sadržaju kako bi se planirale mogućnosti za sprečavanje rada mreže tokom sukoba.

Jun 2008. Mreža nekoliko kongresnih kancelarija je hakovana od strane nepoznatih stranih uljeza. Neke infiltracije uključuju i kancelarije koje se bave interesima ljudskih prava na Tibetu.

Leto 2008. Baze podataka, Demokratske i Republikanske predsedničke kampanje su hakovane i preuzete od strane stranih nepoznatih uljeza.

Leto 2008. *Marathon Oil*, *ExxonMobil* i *ConocoPhillips* su hakovane. Kompanije su izgubile poslovne podatke o vrednosti i lokacijama naftnih polja širom sveta. Šteta je bila ogromna, procenjuje se na milione dolara.

Avgust 2008. Računarske mreže u Gruziji su hakovane od strane nepoznatih uljeza, najverovatnije po nalogu ruske vlade. Ispisani su brojni grafiti po gruzij-

skim sajtovima. Došlo je do prekida usluga kod različitih servisa, ovo je bio pritisak na gruzijsku vladu, koordinisan sa ruskim vojnim akcijama.

Oktobar 2008. Policija otkrila visoko sofisticirani napad na lanac snabdevanja sa čitačima kreditnih kartica napravljenim u Kini, koji su korišćeni u Velikoj Britaniji u supermarketima, a u sebi su imali bežične uređaje. Uređaj pravi kopije kreditnih kartica, skladište podatke i prenosi podatke jednom dnevno preko bežične mreže do Lahorea u Pakistanu. Gubitak je bio 50 miliona dolara, a možda i više. Uređaj je mogao biti podešen da prikuplja podatke samo sa određene vrste kartica, kao što su zlatne kartice.

Novembar 2008. Hakeru upali u mreže Kraljevske banke u Škotskoj. Uspeli su da kloniraju 100 kartica za bankomate i tako povuku sa računa u banci preko 9 miliona dolara, iz 49 gradova širom sveta.

Novembar 2008. Klasifikovane mreže *DOD* i *CENTCOM* bile su hakovane od nepoznatih stranih uljeza. Da bude još gore, bilo je potrebno nekoliko dana da izbací uljeza i ponovo obezbedi mreže.

Decembar 2008. Maloprodaja giganta *TJX* je hakovana. Jedan haker je uhvaćen i osuđen, kasnije je izjavio da su stekli 11 miliona dolara hakerskim radom.

Decembar 2008. Čak i mali *CSIS* (*CSIS.org*) je hakovan od strane nepoznatih uljeza. Želeli su da pristupe elektronskoj pošti zaposlenih i tako da čitaju vesti unapred.

2008. Britanski poslanici su upozoreni na elektronsku poštu koju dobijaju od Evropskog parlamenta, zbog strahovanja da bi mogli da se iskoriste od strane kineskih hakera, koji bi mogli da ugrade u poštu viruse.

Januar 2009. Hakeri napali Internet infrastrukturu u Izraelu tokom vojne ofanzive u pojasu Gaze u januaru 2009. Napad je fokusiran na vladine sajtove, sa najmanje 5.000.000 računara. Izraelski zvaničnici su verovali da je napad sprovedla kriminalna organizacija iz bivšeg Sovjetskog Saveza, a plaća Hamas ili Hezbolah.

Januar 2009. Indijski zvaničnici su upozorili da su pakistanski hakeri umetali malvere na popularnim sajtovima za preuzimanje muzike.

Februar 2009. *FAA (Federal Aviation Administration's)* računarski sistem je hakovan. Povećana upotreba FAA mreže, takođe povećava rizik od namernog prekidu komercijalnog vazdušnog napada..

Februar 2009. 600 računara u Ministarstvu spoljnih poslova Indije je hakovano.

Februar 2009. Francuski mornarica je otkrila da su baze podataka na nosačima aviona bile zaražene virusom „conficker“. Zvaničnici mornarice su otkrili da je neko koristio zaražen USB.

Mart 2009. Nemačka vlada je upozorila da su hakeri nude besplatnu verziju Mikrosoftovog operativnog sistema koji instalira trojance.

Mart 2009. Kanadski istraživači pronašli špijunski računarski sistem za koji oni veruju da Kina implementira na državnim mrežama u 103 zemlje sveta.

Mart 2009. Izveštaji u štampi objavili planove marinaca (*Marine Corp 1.*), novog predsedničkog helikoptera (američkog predsednika), na Iranskim mrežama za deljenje podataka.

April 2009. Vol Strit časopis je izložio sve veću ugroženost električne mreže u SAD, zbog visoko sofisticiranih napada. Takođe, je obelodanio upade u F-35 baze podataka od strane nepoznatih napadača.

April 2009. Premijer Ben Ćiabao je izjavio da je haker iz Tajvana pristupio računarima kineskog Nacionalnog saveta, koji poseduje nacрте njegovog izveštaja o ljudima Nacionalnog Kongresa.

April 2009. Kineski hakeri navodno se infiltrirali u Ministarstvo finansija Južne Koreje, preko virusa u elektronskoj pošti koji su došli od osoba od poverenja.

Maj 2009. U maju 2009., Merik banka (*Merrick Bank*), vodeći izdavač kreditnih kartica, tvrdi da je ona izgubila 16 miliona dolara, nakon kompromitovanja čak 40 miliona kreditnih kartica i računa.

Maj 2009. *HSIN (Homeland Security Information Network)* je hakovana od strane nepoznatih uljeza. Hakeri su dobili pristup podacima i većina podataka je preuzeta.

Jun 2009. Džon Hopkins Univerzitet za primenjenu fiziku, na kome se vode istraživanja za Ministarstvo odbrane i NASA, bilo je primorano na nekoliko svojih mreža privremeno ugasi.

Jun 2009. Nemački ministar unutrašnjih poslova Wolfgang Šojble istakao, prilikom predstavljanja bezbednosnog izveštaja 2008, Kina i Rusija su povećale špijunske napore i Internet napade nad nemačkim kompanijama.

Jul 2009. Ponovo visoko sofisticirani napadi na sajtove SAD i južne Koreje, uključujući i jedan broj vladinih sajtova, pokrenuti od strane nepoznatih hakera. Južna Koreja optužila Severnu Koreju da stoji iza DoS napada. DoS napadi ne remete ozbiljno službu, već traju nekoliko dana i privlače veliku medijsku pažnju.

Avgust 2009. Albert Gonzales je optužen da je između 2006 i 2008, on i neidentifikovani ruski ili ukrajinski kolega, ukrali više od 130 miliona kreditnih i debitnih kartica, hakovanjem 5 sistema velikih kompanija. To je bio najveći hakerski napad u istoriji krađe identiteta u SAD.

Avgust 2009. Ehud Tenenbaum je osuđen za krađu 10 miliona dolara iz američkih banaka. Tenengaum je poznat po hakovanju DOD-ovih računara u 1998, što je rezultiralo osudom izrečenom u jednoj rečenici od šest meseci društveno korisnog rada iz izraelskog suda.

Novembar 2009. Jean-Pascal Impersele, potpredsednik Međuvladinog panela Ujedinjenih nacija o klimatskim promenama, pripisuje hakerisanje i oslobađanje hiljade mejlova sa Univerziteta za klimatska istraživanja Rusiji kao deo zavere da se podriju razgovori u Kopenhagenu o klimatskim promenama.

Decembar 2009. Vol Strit časopis objavio da je veliki broj američkih banaka hakovan, i da se tako gube desetine miliona dolara.

Decembar 2009. Američke bespilotne letilice hakovane od strane iračkih pobunjenika, ostvarili upad u prikupljene materijale nakon misije.

Januar 2010. U Velikoj Britaniji MI5 služba bezbednosti je upozorila tajne obaveštajne oficire iz Narodnooslobodilačke vojske i Ministarstva javne bezbednosti da ne uzimaju sa privredničkih sajmova poklone u vidu kamera i memorijskih

medija, koji sadrže malver koji pruža kinezima udaljeni pristup računarima korisnika.

Januar 2010. Upad u *google* mrežu, kao i u 30 drugih američkih kompanija. Cilj prodora, koji se pripisuje Kini, bio je prikupljanje informacija o tehnologiji, pristup elektronskoj pošti *GMAIL* i sistemima za upravljanje lozinkama.

Januar 2010. Morgan Stanley globalna firma za pružanje finansijskih usluga, doživela je vrlo osetljiv upad u svoje mreže od strane istih kineskih hakera koji su napali *google* računare u decembru 2009, na osnovu procurele elektronske pošte bezbednosnih kompanija koje rade za banku.

Januar 2010. Naraianan (*M. K. Narayanan*), savetnik za nacionalnu bezbednost Indije, rekao je da njegova kancelarija i drugih vladinih odeljenja napadnuta od strane kineza 15. decembra. Naraianan je rekao da to nije prvi pokušaj da se prodre u računare Indijske vlade.

Januar 2010. Grupa pod nazivom "*Iranian Cyber Army*" onesposobila popularni kineski pretraživač *Baidu*. Korisnici su preusmereni na stranicu koja prikazuje iransku političku poruku. Ranije, iste napadači su upali u *Twitter* u decembru i sa sličnom porukom.

Januar 2010. *Intel* objavio da je pretrpeo napad, otprilike u isto vreme kad i *Google*, *Adobe* i drugi. Hakeri su iskoristili ranjivost u softveru *Internet Explorer*. *Intel* je objavio da nije imao gubitke u vidu intelektualne svojine ili novca.

Mart 2010. *NATO* i EU upozorila da se broj napada protiv njihovih mreža značajno povećao u proteklih 12 meseci. Proglasili su Kinu i Rusiju za najveće protivnike.

Mart 2010. *Google* je objavio da je pronašao malver usmeren na vijetnamske korisnike računara. *Google* navodi da nije bio zlonameran, već korišćen za špijunažu. Malver je ugrađen u dodatak operativnog sistema za Vijetnamski jezik.

Mart 2010. Australijske vlasti objavile da je bilo više od 200 pokušaja za upad u mrežu pravnog tima za Rio Tinto. Cilj je bio pribavljanje dokumentacije o strategiji odbrane na suđenju.

April 2010. Kineski hakeri provalili u navodno tajni dosije Indijskog Ministarstva odbrane i indijske ambasade širom sveta, a u cilju pristupa indijskim raketama i oružanim sistemima.

Mart 2010. Nepoznati hakeri objavili stvarne prihode Litvanskih vladinih zvaničnika, preko pristupa sistemu poreske evidencije.

April 2010. Kineska telekomunikaciona kompanija slučajno emituje pogrešne informacije za oko 37,000 mreža, uzrokujući Internet saobraćaj koji se pogrešno prosledio kroz Kinu. Incident je trajao 20 minuta, a saobraćaj je izložen na 8,000 američkih mreža, 8,500 kineskih mreža, 1,100 australijskih mreža i 230 francuskih mreža.

Maj 2010. Kanadska služba bezbednosti upozorila na moguću špijunažu na svim nivoima države (Vlada Kanade, kanadski univerziteti, privatne kompanije i individualne mreže klijenata).

Juli 2010. Ruski obaveštajni agent (Aleksej Karetnikov), uhapšen je i deportovan nakon devet meseci rada u Microsoft odeljenju za testiranje softvera.

Oktobar 2010. Otkriven paket zlonamernih programa (*Stuxnet*) u Iranu, Indoneziji i na drugim mestima, dizajniran da ometa simensovo industrijsko postrojenje. Sve je na kraju dovedeno u vezu sa kontrolom iranskog nuklearnog programa.

Oktobar 2010. Vol Strit u svom časopisu objavio da hakeri koriste *Zevs* malver, dostupan u visoko tehnološkim kriminalnim krugovima crnog tržišta za oko 1200 dolara. Sa tim programom bili su u stanju da ukradu više od 12 miliona dolara od pet banaka u SAD i UK. *Zevs* koristi hiper linkove iz elektronske pošte za krađu informacija o računu, a kasnije ih koristili za transfer novca na bankovne račune. Kasnije je uhapšena grupa kriminalaca koja je otvarala lažne račune u bankama preko kojih su krali novac.

Oktobar 2010. Ministarstvo Odbrane Australije prijavilo ogroman porast napada na vojsku. Australijski ministar odbrane, Džon Fokner otkriva da je bilo 2400 incidenata na mreži u 2009-toj i 5551 incident između januara i avgusta 2010.

Decembar 2010. Britanski ministar spoljnih poslova Vilijam Hejg prijavio napade strane sile na ministarstva spoljnih poslova, odbrane i drugih institucija od velikog značaja, kao i tešku odbranu zbog pretvaranja da dolaze iz Bele kuće.

Decembar 2010. Indijski Centralni istražni biro (*CBI*) sajt (*cbi.nic.in*), hakovan je tako što su podaci izbrisani. Indija optužuje pakistanske hakere. Međutim važni podaci *CBI*-a bili su uskladišteni na računarima bez Internet pristupa.

Januar 2011. Hakeri upali berzu Evropske unije, omogućili kupovinu i prodaju akcija i tako uspjeli da ukradu više od 7 miliona dolara. Tržište je bilo primorano na privremeno zatvaranje.

Januar 2011. Hakeri izvukli 6,7 miliona dolara iz Južne Afrike banke preko novogodišnjih praznika.

Januar 2011. Kanadska vlada prijavila veliki napad na svoje organe. Napad fokusiran na Ministarstvo finansija i trezor. Privremeno su prekinute veze sa Internetom u cilju sprečavanja štete prouzrokovane napadom. Kanadski izvori pripisuju napad na Kinu.

Mart 2011. Hakeri upali u Francusku računarsku mrežu vlade, u potrazi za poverljivim informacijama o predstojećim sastancima grupe G-20.

Mart-April 2011. Između marta 2010 i aprila 2011, FBI je identifikovao 20 incidenata u kojima su *onlajn* bankarski akreditivi malih i srednjih preduzeća u U.S. kompromitovani i korišćeni za inicijalni transfer u kinesku ekonomiju preko trgovačkih kompanija. Od aprila 2011 ukupan pokušaj prevare iznosi oko 20 miliona dolara, stvarni gubici su 11 miliona dolara.

Mart-April 2011. Hakeri koriste tehnike pecanja u pokušaju da dobiju podatke ako bi kompromitovali *RSA "Secure ID"*, tehnologiju za autentifikaciju. Zabeleženi slučajevi prodora u kompanijske mreže na osnovu prethodno pribavljenih podataka.

April 2011. Google prijavio napad tehnikom pecanja, koji je doveo do kompromitovanja stotine *gmail* lozinki istaknutih ljudi, uključujući i visoke američke zvaničnike. Google pripisuje napad Kini.

April 2011. Zaposleni u nacionalnoj laboratoriji (*Oak ridge National Laboratory*) primili su lažnu elektronsku poštu sa zlonamernim priložima. Dve mašine su inficirane i nekoliko megabajta podataka je preuzeto pre nego što su računari laboratorije isključeni sa mreže.

Maj 2011. Hakeri maskirani kao članovi grupe *anonymus* prodrli u mrežu *PlayStation*. Soni je izjavio da je kompromitovano podataka za više od 80 miliona korisnika ili iskazano u novcu 170 miliona dolara.

Juni 2011. Mreže IMF-a su bile ugrožene od stranih vlada. Napadači su koristili lažnu elektronsku poštu sa zlonamernim priložima i tako dobavili ogromnu količinu podataka.

Juni 2011. *Citibank* izvestila da su podaci kreditnih kartica od svojih 360000 klijenata preuzeti koristeći relativno jednostavnu manipulaciju sa *URL*-ovima.

Juli 2011. Zamenik sekretara Ministarstva odbrane za strategiju protiv visoko tehnološkog kriminala, saopštio je da je ministarstvo hakovano i da je preuzeto 28000 fajlova.

Juli 2011. Nemačka Federalna policija zajedno sa Saveznom carinskom službom je otkrilo da su hakeri upali na servere *GPS* sistema koji se koriste za lociranje ozbiljnih kriminalaca i osumnjičenih za terorizam. Serveri su morali da se privremeno ugase kako bi se sprečilo dalje gubljenje podataka.

Juli 2011. Južna Koreja objavila da su hakeri iz Kine prodrli preko Internet portala i ostvarili pristup telefonskim brojevima, adresama elektronske pošte i drugim podacima za 35 miliona Korejaca.

Avgust 2011. Prema izvorima japanske vlade, na udaru su se našle velike visoko tehnološke kompanije. Cilj je bio izvlačenje poverljivih informacija. Upad je ostvaren preko zlonamernih priloga elektronske pošte.

Avgust 2011. Kineski hakeri su preko trojanaca hakovali 480 članova japanskog zakonodavnog tela.

Septembar 2011. Nepoznati napadači hakovali holandsko *CA* (engl. *Certificate Authority*), što im je omogućilo da izdaju više od 500 lažnih sertifikata velikih kompanija i vladinih agencija. Sertifikati se koriste za proveru originalnosti sajta.

Izdavanjem lažnog sertifikata, napadač može da pretenduje da bude bezbedan njegov sajt, preko koga može da preuzme elektronsku poštu ili instalira zlonamerni program. Ovo je drugi pokušaj u 2011 godini da je hakovan CA.

Septembar 2011. Australijska uprava za odbranu izjavila je da su mreže odbrane napadnute više od 30 puta dnevno, uz povećanje napada za više od 350% do 2009. godine.

Septembar 2011. Računarski virus iz nepoznatog izvora uveden na teren kontrolnih stanica U.S. vazdušnih snaga. Prema izveštajima zaražena je mreža vazduhoplovne baze u Nevadi. SAD nije izgubio kontrolu nad letelicama, niti je nestao neki podataka, ali je bilo više zlonamernih pokušaja.

Oktobar 2011. Mreže od 48 kompanija iz hemijske industrije su hakovane sa ciljem pribavljanja intelektualne svojine. Proizvođači antivirusa (*Symantec*) su napade vezali za Kinu.

2011. Norveška agencija za nacionalnu bezbednost (*NSM*), izveštava da je hakovano najmanje 10 energetskih kompanija. Napadi su posebno skrojeni za svaku kompaniju, koristeći tehnike pecanja preko elektronske pošte. *NSM* je rekao da su napadi došli u vreme kada su se vodili pregovori oko velikih ugovora. Hakeri su pristupili poverljivim dokumentima, industrijskim podacima, korisničkim imenima i lozinkama.

Decembar 2011. Hakeri su potpuno prodrli više od godinu dana u mrežu Američke privrednu komoru. Hakeri su imali pristup svemu u Privrednoj komori, računarima i informacijama o industrijskoj poziciji U.S.

Mart 2012. Generalni inspektor NASE izvestio da je napad *APT (Advanced persistent threat)* uspešno kompromitovao NASA računare u 2011. u jednom napadu uljezi su akreditive od 150 korisnika, koje su mogli da koriste za neovlašćen pristup sistemima NASA.

Mart 2012. BBC izvestio o visoko tehnološkom napadu koji je imao cilj da onespособi BBC. Generalni direktor BBC okrivio je Iran za incident.

Mart 2012. Indijski ministar za komunikacije i informacione tehnologije otkrio u pisanom odgovoru na poslaničko pitanje, kojih je 112 vladinih sajtova bilo ugroženo od decembra 2011 do februara 2012. Većina incidenata potiče iz Pakistana.

Mart 2012. U.S. Ministarstvo za nacionalnu bezbednost izdalo je upozorenje o napadima na američke gasovode.

April 2012. Iran bio primoran da isključi ključna naftna postrojenja nakon hakerskog napada na interne kompjuterske sisteme. Malver je pronađen unutar kontrolnih sistema Kharg Island - Glavni iranski terminal za izvoz nafte. Svi računarski sistemi su bili isključeni zbog napada, kao mera predostrožnosti Iran je izvestio da napad nije uticao na proizvodnju nafte.

Maj 2012. Zvaničnici UK rekli za novine da je bilo nekoliko manjih upada u njihove službene mreže.

Maj 2012. Špijunski program pod nazivom "plamen", otkriven je na računarima iranskog Ministarstva za energetiku, kao i u drugim zemljama bliskog istoka, uključujući Izrael, Siriju, Sudan i druge zemlje širom sveta.

Maj 2012. Istraživači na Univerzitetu u Torontu izvestili o verziji softvera Simurgh, koga anonimne mreže koriste, a popularan je u zemljama kao što su Iran i Sirija u cilju izbegavanja vladine kontrole Interneta. Takođe, instalira program za špijunažu koji pribavlja korisnička imena i lozinke.

Juni 2012. Akcija pecanja na Internetu usmerena na U.S. stručnjake avio industrije koji su prisustvovali 2013. na IEEE konferenciji za vazduhoplovstvo.

Juni 2012. Organizovana prevara na svetskom nivou upotrebom verzija programa *SpyEye* i *Zeus Trojans*. Na udaru su bili lični podaci, korporativni nalozi za pristup sistemima i zaobilaženje dvo-faktorske autentifikacije..

Juni 2012. Šef britanske službe bezbednosti izjavio da je jedna londonska kompanija izgubila na proceni 1,2 milijarde dolara, kao rezultat Internet napada.

Juli 2012. Grupa iz Šangaja povezana sa narodno oslobodilačkom vojskom (*PLA*) uspešla je da pribavi podatke od predsednika Evropskog saveta, UK firme za odbrambena istraživanja (*Qinetiq*) i drugih komercijalnih entiteta u USA, Evropi i Indiji.

Juli 2012. Trojanac zvani „*Mahdi*“ otkriven u više od 800 inženjerskih firmi, vladinih agencija, finansijskih kuća i akademija širom Bliskog istoka i šire, uglavnom u Izraelu i Iranu. Virus je sadržao sekvence na persijskom jeziku.

Juli 2012. Indijski zvaničnici su potvrdili postojanje virusa koji prikuplja podatke iz važnih računarskih sistema u štabu Istočne pomorske komande. Podaci su prosleđeni na kineske IP adrese. Virus je kako se navodi dospao preko zaraženih USB memorija, koji su korišćeni za prenos podataka sa računara na kojima su se nalazili važni podaci.

Juli 2012. Direktor NSA, izjavio je da je došlo do povećanja za više od 17 puta, broja napada na američkim infrastrukturnim preduzećima između 2009 i 2011.

Juli 2012., Preko 10,000 adresa elektronske pošte indijskih zvaničnika sa vrha vlasti je bilo ugroženo, uključujući i zvaničnike u Kancelariji premijera, odbrane, spoljnih poslova i finansija, kao i obaveštajnih agencija.

Avgust 2012. Malver zvani „*Gauss*“ zarazio 2.500 sistema širom sveta. *Gauss* je imao za cilj da ugrozi libanske banke. Ovaj virus sadrži kod koji još nije poznat, jer šifra još nije razbijena (napadači nepoznati).

Avgust 2012. Grupa nazvana „*Cutting Sword of Justice*“ povezana sa Iranom koristi „*Shamoon*“ virus za napad na *Aramaco* (glavni snabdevač saudijske nafte), obrisani su podaci na preko 30,000 računara i zarazi kontrolne sisteme (bez izazivanja štete). Napad je takođe uticao i na katarske kompanije *RasGas*. Verovatno su zaražene i druge naftne kompanije.

Septembar 2012. Izz ad-Din al-Qassam, hakerska grupa povezana sa Iranom, pokrenula operaciju „*Ababil*“ ciljajući na bakarske sajtove i druge U.S. finansijske institucije.

Oktobar 2012. Upotrebom malvera od 2007 hakeri prikupljaju informacije o ciljevima u Istočnoj Evropi, bivšem SSSR-u i Centralnoj Aziji, zajedno sa ciljevima u Zapadnoj Evropi i Severnoj Americi. Informacije se prikupljaju najviše iz ambasada, istraživačkih firmi, vojnih infrastruktura, energetskih, nuklearnih i dugih kritičnih infrastruktura.



AES - Advanced Encryption Standard. Blokovska šifra sa simetričnim ključem, standardizovana od strane NIST-a. Pripada grupi modernih šifara. Dužina ključa je 128, 192, i 256 bitova.

ASCII - američki kodni standard za razmenu informacija. Ove kodove koristi veliki broj računarskih sistema za prevođenje karaktera u binarne brojeve.

Algoritam - opis za rešavanje nekog problema.

Asimetrični šifarski sistemi – sistemi sa javnim i privanim ključem. Primer ovog tipa algoritama je RSA koji se koristi za šifrovanje i digitalno potpisivanje.



Biometrija - tehnika za autentifikaciju koja koristi jedinstvene fizičke karakteristike nekog pojedinca. Postoje različiti tipovi biometrije.

Biometrijski templejt - digitalizovana fizička karakteristika nekog pojedinca za određeni biometrijski izvor koji se koristi za autentifikaciju date osobe.

Binarna sekvenca - niz karaktera (jedinica i nula) ili binarni niz.

Blok kod – neprazan skup reči koje su iste dužine, predstavlja strukturu red.

V

VOIP - protokol koji se koristi za digitalizaciju govora, pakovanje i slanje preko TCP/IP veze.

Vizuelna kriptografija - specijalna tehnika šifrovanja koja omogućava skrivanje informacija na slici, na takav način da se može dešifrovati ljudskim okom bez upotrebe računara.

Venona - predstavlja One-time pad u realnosti. Koristila ga je sovjetska špijunska mreža koja je formirana na teritoriji SAD 1940-tih.

G

GSM - globalni sistem za telekomunikacije. Internacionalni standard za satelitske telefone.

D

DES - Data Encryption Standard. Blokovska šifra sa simetričnim ključem usvojena od strane NIST-a. Pripada grupi modernih šifara. Dužina ključa je 56 bitova, prevaziđen je od strane AES-a.

Digitalni potpis - protokol koji koristi primalac poruke da bi verifikovao pošiljaoca poruke. Za verifikaciju se koristi javni ključ pošiljaoca. Obezbeđuje servis neporecivosti.

Dešifrovanje - proces transformacije šifrata u otvoreni tekst.

Digitalni vodeni pečat - tehnika za zaštitu autorskih prava digitalnih sadržaja.

Difi-Helman - protokol namenjen za razmenu simetričnih ključeva preko javnih komunikacionih kanala.

E

Enigma - mašina za šifrovanje iz familije mehaničkih rotor mašina. Koristile je nemačke snage za vreme Drugog svetskog rata.

Entropija - mera za količinu neodređenosti ili prosečna količina informacije koju sadrže generisane poruke nekog informacionog izvora.

ECB - režim za šifrovanje kod blokovskih šifara u kom je svaki blok šifrata potpuno nezavisan. Ovaj režim može da bude nebezbedan.

I

Iris - šara irisa ili obojeni deo oka koji je prilično haotičan (neodređen) ili slučajan. Predstavlja biometrijski izvor sa visokim performansama.

Integritet - prevencija od neautorizovane izmene sadržaja (poruke).

Informacioni izvor – generator sekvence simbola koji predstavljaju poruke.

J

Javni ključ - element sistema sa javnim ključem ili javni ključ nekog korisnika koji je dostupan svim korisnicima u mreži. Koristi se u fazi šifrovanja.

Jednosmerna funkcija - sam naziv kaže da je funkcija neinvertibilna, ako je $y = f(x)$, tada je $x \neq f(y)$. Heš funkcije su vrsta jednosmernih funkcija.

K

Kapacitet kanala - maksimalna prosečna količina informacija na izlazu kanala koja je jednaka količini informacije na ulazu.

Kodna reč - binarna sekvenca kojom je predstavljen simbol izvorne poruke.

Kriptoanaliza - umetnost i nauka o razbijanju šifrovanih poruka.

Komunikacioni kanal - formalizacija šta se dešava u prenetoj poruci između predajne i prijemne strane.

Kompletan kod - prefiksni kod čije kodno stablo ne sadrži nekorišćene listove.

Kodovanje - transformacija simbola poruke u kodne reči.

Kriptološki ključ - binarna sekvenca veće dužine, poseduje osobine slučajnih nizova. Koristi se kao početno stanje algoritma u fazi šifrovanja i dešifrovanja.

Kriptograf - lice koje dizajnira šifre.

Kriptoanalitičar - lice koje dizajnira metode za razbijanje šifara.

Kriptografija - nauka o pravljenju algoritama za šifrovanje.

Kriptoanaliza - nauka o razbijanju algoritama za šifrovanje.

L

LAN - lokalna mreža.

LFSR - linearni pomerački registar sa povratnom spregom. Njegova uloga se sastoji u generisanju pseudoslučajnih sekvenci. Ima periodu (ponavlja se nakon izvesnog vremena).

LSB - steganografska tehnika za ugrađivanje tajnih poruka u podatak nosilac po principu zamene bitova sa najmanjim značajem.

Lozinka - tajni akreditiv (string od prosečno 8 karaktera) koji se koristi za autentifikaciju kod tradicionalnih sistema za autentifikaciju. Korisnik je u

stanju da zapamti više lozinki, dok kriptološke ključeve nije moguće zapamtiti.

M

MAC - kod za proveru autentičnosti poruke.

N

NIST - američka federalna agencija za standarde i tehnologiju.

NSA - nacionalna agencija za bezbednost. Američka agencija koja je odgovorna za bezbednost i kriptanalizu elektronskih komunikacija.

O

One-time pad - perfektna šifra koja pripada grupi šifara sa simetričnim ključem. Ključ je generisan na slučajan način i ima jednaku dužinu kao i poruka. Ključ ne sme nikad da se ponavlja.

Otvoreni tekst - poruka u fazi šifrovanja ili rezultat funkcije za dešifrovanje.

P

PGP - program za bezbednu elektronsku poštu koji objedinjuje servise za kriptografsku zaštitu podataka i digitalno potpisivanje. Razvijen od strane Fila Cimermana.

PKI - infrastruktura sa javnim ključevima. Sadrži bazu javnih ključeva preko kojih obezbeđuje autentifikaciju u srednjim i velikim mrežama.

Privatni ključ - element sistema sa javnim ključem ili tajna koju čuva svaki korisnik. Koristi se u fazi dešifrovanja.

Protokol - protokol je skup pravila koje razumeju i poštuju strane u komunikaciji.

Poruka - podatak koji se razmenjuje preko komunikacionog kanala između predajne i prijemne strane. Može da bude kodovana i u šifrovanoj formi.

Perfektna tajnost – teorijski dokazan kriptografski mehanizam koji ne zavisi od računarske snage.

PRNG - generator za generisanje pseudoslučajnih brojeva na osnovu inicijalnog stanja koje je određeno na slučajan način.

R

RSA - kriptografski sistem sa javnim ključem, patentiran od strane Rivesta, Šamira i Adlemana 1976. Sigurnost RSA zasniva se na složenosti faktORIZACIJE velikih brojeva. Ima široku primenu, implementiran je u PGP i SSL-u.

RC4 - sekvencijalna šifra sa simetričnim ključem. Pripada grupi modernih šifara. Dužina ključa jednaka je poruci. Neki je nazivaju pseudoperfektna šifra. Za generisanje ključa koristi se generator za pseudoslučajne brojeve. Pravila implementacije su skoro ista kao i kod perfektnih šifara.

S

Sertifikat - elektronski fajl, obično sadrži javni ključ koji je digitalno potpisan od Sertifikacionog tela. Sertifikati se koriste za autentifikaciju na Internetu.

Sertifikaciono telo - treća strana od poverenja koja potpisuje i distribuira sertifikate.

SSL - široko primenjeni zaštitni protokol za autentifikaciju na Internetu (Internet transakcije)

Simetrični ključ - kriptološki ključ koji je identičan na predajnoj i prijemnoj strani.

Steganografija - nauka o skrivanju informacija u drugim bezazlenim podacima. Čest primer je skrivanje tekstualnog sadržaja u neku sliku.

Stacionarni izvor – informacioni izvor čija statistika ne zavisi od vremena.

Sesijski ključ – simetrični ključ za jednokratnu upotrebu.

T

TCP/IP - protokol koji se koristi za prenos informacija u računarskim mrežama. TCP/IP je postao standard za sve mreže povezane sa Internetom.

TDES - blokovska šifra sa simetričnim ključem, usvojena od strane NIST-a. Bazirana na sukcesivnoj aplikaciji tri DES algoritma sa različitim ključevima. Predstavlja ojačanje klasičnog DES-a.

TRNG - generator slučajnih brojeva; ovakve generatore je moguće konstruisati u prirodnim informacionim izvorima.

F

Faktorizacija - rastavljanje velikih prostih brojeva na činioce iz skupa prostih brojeva.

Fejstel šifra - nazvana po nemačkom kriptografu Horstu Fejstelu (Horst Feistel) koji je pionir u razvoju dizajna blokovskih šifara, radio je u IBM-u. Ovo su bila inicijalna istraživanja koja su kulminirala razvoju DES (Data Encryption Standard) algoritma 1970. godine. Fejstel šifra predstavlja dizajn blokovske šifre, a ne posebnu šifru.

H

Haker – originalno se termin koristi za kreativnog programera koji razvija programe za ilegalan pristup računarskim mrežama u cilju krađe ili uništenja informacija. Dobar haker treba da poseduje dobre kriptanalitičke veštine.

Hamingovo rastojanje - koristi se za određivanje razlike između dva niza jednake dužine.

Heš funkcije - funkcija koja generiše skraćenu verziju poruke. U kriptografskim aplikacijama heš funkcije moraju da budu jednosmerne sa malom verovatnoćom da dve različite poruke mogu da daju isti rezultat.



CRC - Cyclic Redudancy Check. Kod široke primene, koristi se za detektovanje grešaka. Obično pre dešifrovanja, CRC se proverava.

CBC - režim za šifrovanje kod blokovskih šifara. Radi na principu ulančavanja blokova šifrata.



Šifra - algoritam za šifrovanje. Mogu da postoje različiti tipovi šifara. Osnovne podele su na klasične i moderne, simetrične i asimetrične, apsolutno i praktično tajne.

Šifrat - rezultat funkcije za šifrovanje ili transformacija otvorene poruke koja je inverzna uz posedovanje pravog ključa.

Šifrovanje - proces transformacije otvorenog teksta u šifrat.

Na osnovu člana 23. stav 2. tačka 7. Zakona o porezu na dodatu vrednost („Službeni glasnik RS”, br. 84/2004, 86/2004 (ispr.), 61/2005, 61/2007 i 93/2012), Odlukom Senata Univerziteta Singidunum, Beograd, broj 260/07 od 8. juna 2007. godine, ova knjiga je odobrena kao osnovni udžbenik na Univerzitetu.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

003.26(075.8)
004.056.55(075.8)

МИЛОСАВЉЕВИЋ, Милан, 1952-
Kriptologija 2 / Milan Milosavljević,
Saša Adamović. - 1. izd. - Beograd :
Univerzitet Singidunum, 2014 (Loznica :
Mladost grup). - 239 str. : ilustr. ; 24 cm

Na vrhu nasl. str.: Fakultet za informatiku i
računarstvo. - Tiraž 300. - Rečnik pojmova:
str. 232-239. - Bibliografija: str. 214-218.

ISBN 978-86-7912-537-8
1. Адамовић, Саша, 1985- [аутор]
а) Криптологија б) Криптографија
COBISS.SR-ID 205455116

© 2014.

Sva prava zadržana. Nijedan deo ove publikacije ne može biti reprodukovan u bilo kom vidu i putem bilo kog medija, u delovima ili celini bez prethodne pismene saglasnosti izdavača.