

UNAPREĐENJE PROTOKOLA ZA RAZMENU KLJUČEVA NA BAZI LIČNIH IDENTIFIKACIONIH DOKUMENATA POŠILJAOCA I PRIMAOCA

By Aleksandar Mišković

UNIVERZITET SINGIDUNUM
BEOGRAD
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

UNAPREĐENJE PROTOKOLA ZA RAZMENU KLJUČEVA NA
BAZI LIČNIH IDENTIFIKACIONIH DOKUMENATA
POŠILJAOCA I PRIMAOCA

DOKTORSKA DISERTACIJA

mentor:
prof. dr. Mladen Veinović

student:
Aleksandar Mišković
broj indeksa: 2010460065

Beograd, 2019.

SINGIDUNUM UNIVERSITY
BELGRADE
DEPARTMENT FOR POSTGRADUATE STUDIES

IMPROVING KEY EXCHANGE PROTOCOLS BASED ON
SENDER AND RECEIVER ELECTRONIC IDENTIFICATION
DOCUMENTS

DOCTORAL DISSERTATION

Mentor:
Mladen Veinović

Student:
Aleksandar Mišković

Belgrade, 2019.

Strahinji

ZAHVALNICA

Ova doktorska disertacija je nastala kao rezultat dugogodišnjih istraživanja pod rukovodstvom prof. dr Mladena Veinovića.

Svako naučno istraživanje je i istraživanje sopstvenih granica i moći. Mentori su tu da bi nas svojim znanjem i iskustvom podstakli da pomeramo granice, a porodica i prijatelji da bi nam davali smisao, ljubav i snagu.

Hvala mom mentoru, prof. dr Mladenu Veinoviću, na nesebičnoj pomoći i podršci u svim fazama izrade ove disertacije, kao i na bezgraničnom poverenju, korisnim savetima, kako tokom izrade disertacije tako i tokom naše dugogodišnje saradnje.

Hvala mojoj najvećoj podršci i životnoj snazi supruzi Jasmini na bezgraničnom strpljenju, podršci i razumevanju tokom izrade doktorske disertacije.

Decembar 2019.

Beograd

Autor

Sažetak

Predmet rada doktorske disertacije je sagledavanje aktuelnih problema vezanih za pojmove razmena kriptografskih ključeva i autentifikacija korisnika sistema za tajnu komunikaciju. Rad se bavi analizom postojećih rešenja u oblasti istraživanja i razvijanjem sopstvenog sistema za tajnu komunikaciju.

Naučni cilj disertacije je unapređenje protokola za razmenu kriptografskih ključeva na bazi ličnih identifikacionih dokumenata. Izvršena je analiza postojećih pristupa u oblasti istraživanja s ciljem da se poboljša nivo zaštite prilikom tajne komunikacije i dobije osnova za razvoj sopstvenog sistema. Kombinovanjem kriptografskih metoda koje obezbeđuju poverljivost, autentičnost i integritet, uz primenu steganografskih metoda za razmenu informacija na skriven način, korisnicima predloženog sistema se pruža mogućnost da na efikasan i siguran način razmenjuju tajne poruke.

Analizom rezultata istraživanja zaključeno je da postoji opravdanost upotrebe ličnih identifikacionih dokumenata za razmenu kriptografskih ključeva koji se koriste u tajnoj komunikaciji.

Ključne reči: razmena kriptografskih ključeva, tajna komunikacija, lični identifikacioni dokument, steganografija

Abstract

The subject of the doctoral dissertation is looking at current issues related to the concepts of cryptographic key exchange and authentication of users of a secret communication system. The paper deals with the analysis of the existing solutions in the field of research and development of own secret communication system.

The scientific goal of the dissertation is to improve the protocol for exchanging cryptographic keys based on electronic identification (eID). Analysis of the existing approaches in the research was carried out in order to improve the level of protection during secret communication and to provide the basis for the development of own system. By combining cryptographic methods that ensure confidentiality, authenticity and integrity, along with the use of steganographic methods for information exchange in a secret way, users of the proposed system are given the opportunity to exchange secret messages in an efficient and secure manner.

By analysing the research findings, it has been concluded that it is justified to use electronic identification for exchanging cryptographic keys used in secret communication.

Keywords: cryptographic keys exchange, secret communication, electronic identification, steganography

Sadržaj

1.	Uvod	12
1.1.	Očekivani doprinosi	13
1.1.1.	Stručni doprinos	13
1.1.2.	Naučni doprinos	13
1.2.	Metode koje će se primenjivati u istraživanju	14
1.3.	Cilj istraživanja	15
1.4.	Naučne hipoteze	15
1.5.	Struktura doktorske disertacije	16
2.	Pregled u oblasti istraživanja	18
3.	Teorijske osnove istraživanja	24
3.1.	Kriptografija	25
3.1.1.	Osnovna pravila	25
3.1.2.	Simetrična kriptografija	28
3.1.2.1.	Sekvencijalni šifarski sistemi	29
3.1.2.2.	Blokovski šifarski sistemi	30
3.1.3.	Asimetrična kriptografija	33
3.1.3.1	<i>RSA</i> asimetrični algoritam	35
3.1.3.2	Sertifikaciona tela	36
3.1.3.3.	Princip rada sertifikacionog tela	39
3.1.3.4.	Digitalni sertifikat	40
3.1.3.5.	Struktura digitalnog sertifikata	42
3.1.3.6.	Izdavanje digitalnog sertifikata	43
3.1.3.7.	Lista opozvanih sertifikata	44
3.2.	Steganografija	45
4.	Pregled postojećih rešenja	49
4.1.	Encryption Wizard	50

4.2.	SteganPEG.....	52
4.3.	StegApp tool.....	53
4.4.	OpenPuff.....	54
4.5.	Sertifikaciono telo MUP-a Republike Srbije.....	55
5.	Model predloženog rešenja	56
5.1.	Opis problema.....	56
5.2.	Predloženo rešenje i njegova primena.....	57
5.2.1.	Primena i implementacija steganografije.....	59
5.2.2.	Predloženo rešenje i njegova implementacija.....	62
5.2.2.1.	Implementacija predloženog rešenja	66
6.	Evaluacija predloženog rešenja	68
6.1.	Prikaz eksperimentalnih rezultata	69
6.1.1.	Simulacija sistema za sigurnu razmenu <i>email</i> poruka.....	69
6.1.2.	Kritički osvrt na funkcionalnost <i>PKI</i> sistema.....	72
6.2.	Anketa	82
6.3.	Poređenje s postojećim rešenjima i pravci daljih istraživanja	84
7.	Zaključak	86
Literatura	89	
Prilog		95

Spisak slika

Slika 3.1. Komunikacija između Alise i Boba uz prisustvo uljeza Trudi	25
Slika 3.2. Podela savremenih kriptografskih sistema.....	26
Slika 3.3. Algoritam za šifrovanje simetričnim ključem prikazan	28
Slika 3.4. Sekvencijalni šifarski sistem – početno stanje	30
Slika 3.5. <i>ECB</i> režima rada	32
Slika 3.6. <i>CBC</i> režima rada	32
Slika 3.7. <i>CTR</i> režima rada	33
Slika 3.8. Princip slanja šifrovane poruke u asimetričnoj kriptografiji.....	34
Slika 3.11. Šematski prikaz izdavanja digitalnog sertifikata	41
Slika 3.12. <i>X.509 ver3</i> standardni sertifikat.....	42
Slika 3.13. Lanac sertifikacije	43
Slika 3.14. Prikaz <i>CRL</i> liste.....	45
Slika 3.15. Model steganografskog sistema.....	46
Slika 3.16. Umetanje slova "A" u 8 bajtova stego nosača	47
Slika 3.17. <i>DCT</i> pomoću <i>JPEG</i> modela kompresije pomoću bloka veličine 8 x 8 piksela ..	47
Slika 4.1. Izgled <i>Encryption Wizard</i> aplikacije.....	50
Slika 4.2. Odabir dužine <i>AES</i> ključa u <i>Encryption Wizard</i> aplikaciji	51
Slika 4.3. Odabir parametara za formiranje digitalnog sertifikata	51
Slika 4.4. Verzija <i>Encryption Wizard</i> aplikacije.....	52
Slika 4.5. Izgled <i>SteganPEG</i> aplikacije nakon postavljenih ulaznih datoteka	52
Slika 4.6. Šematski prikaz tajne komunikacije pomoću <i>StegApp</i> aplikacije	53
Slika 4.7. Korišćenje steganografije u <i>OpenPuff</i> aplikaciji.....	54
Slika 5.1. Očitavanje kvalifikovanih digitalnih sertifikata koji se nalaze na ličnom identifikacionom dokumentu.....	58
Slika 5.2. Aproksimacija <i>JPEG</i> slike nad kojom je vršena analiza kapaciteta za skrivanje podataka.....	60

Slika 5.3. Dijagram zavisnosti kapaciteta za skrivanje tajnih podataka i veličine <i>JPEG</i> slike u <i>KB</i>	60
Slika 5.4. Statistički prikaz poruka zapisanih u najmanjoj i najvećoj slici	61
Slika 5.5. <i>AES</i> ključ u šifrovanom obliku.....	61
Slika 5.6. Grafički prikaz kvaliteta <i>JPEG</i> slike putem opcije <i>Curves</i> u programu <i>Photoshop</i> 62	
Slika 5.7. Grafički prikaz kvaliteta <i>JPEG</i> slike putem opcije <i>Levels</i> u programu <i>Photoshop</i> 62	
Slika 5.8. Koraci koje preduzima Alisa u predloženom rešenju	64
Slika 5.9. Koraci koje preduzima Bob u predloženom rešenju	65
Slika 5.10. Pseudo kod predloženog rešenja	67
Slika 6.1. Dijagram kontrole toka odlučivanja u simulacionom modelu	68
Slika 6.2. Simulacioni model za razmenu tajnih poruka.....	69
Slika 6.3. Prosečna vrednost odlaznog saobraćaja na mreži	70
Slika 6.4. Prosečna vrednost dolaznog saobraćaja na mreži	70
Slika 6.5. Prosečno vreme odgovora servera na zahtev klijenata za slanje <i>email</i> poruke predstavljen funkcijom <i>time_average</i>	71
Slika 6.6. Prosečno vreme odgovora servera na zahtev klijenata za preuzimanje <i>email</i> poruke predstavljen funkcijom <i>time_average</i>	71
Slika 6.7. Simulacioni modela interneta sa pod mrežama u kojima se koristi <i>PKI</i> sistem	72
Slika 6.8. Imena i modeli objekata korišćeni u simulacionom modelu	73
Slika 6.9. Simulacioni model pod mreže <i>BG</i> (Beograd).....	74
Slika 6.10. Simulacioni model pod mreže <i>KG</i> (Kragujevac)	75
Slika 6.11. Imena i modeli objekata korišćeni u pod mrežama simulacionog modela.....	75
Slika 6.12. Konfigurisanje simulacionog objekta "Aplikacije"	76
Slika 6.13. Parametri aplikacionih modela.....	76
Slika 6.14. Konfigurisanje simulacionog objekta "Profili"	77
Slika 6.15. Nazivi atributa i opis njihovih aktivnosti.....	77
Slika 6.16. Rekonfigurisani simulacioni model pod mreže <i>KG</i> (Kragujevac)	78
Slika 6.17. Broj aktivnih sesija na serveru u pod mreži <i>BG</i> (Beograd).....	79

Slika 6.18. Vreme koje je potrebno da server obradi zahtev klijenta u podmreži BG (Beograd)	80
Slika 6.19. Prosečna stopa dolaznog saobraćaja u podmreži BG (Beograd)	80
Slika 6.20. Prosečna stopa odlaznog saobraćaja u podmreži BG (Beograd)	81
Slika 6.21. Da li posedujete biometrijsku ličnu kartu (sa čipom)?	82
Slika 6.22. Da li ste upoznati sa činjenicom da biometrijska lična karta (sa čipom) može da sadrži kvalifikovani digitalni sertifikat?	83
Slika 6.23. Da li ste upoznati sa činjenicom da upotrebom kvalifikovanog digitalnog sertifikata možete da zaštitite svoju privatnost na internetu?	83
Slika 6.24. Da li bi ste koristili biometrijsku ličnu kartu (sa čipom) koja sadrži kvalifikovani digitalni sertifikat za zaštitu svoje privatnosti na internetu? ...	84

1. Uvod

Do danas je razvijen veliki broj kompletnih servisa kojima se štiti privatnost i koji garantuju visok stepen zaštite razmenjenih informacija. Neki od ovih servisa su besplatni i mogu se koristiti bez ikakvih ograničenja, dok se drugi mogu koristiti uz određenu novčanu nadoknadu. Međutim, u današnje vreme postoje razne metode za prisluškivanje komunikacionog kanala preko koga se vrši razmena informacija. Nakon otkrivanja šifrovane komunikacije i presretanja šifrovanih poruka, postoji verovatnoća da će neko pokušati da izvrši kriptanalizu istih. U svrhu smanjivanja verovatnoće otkrivanja šifrovane komunikacije najčešće se koristi neka od opšte poznatih steganografskih metoda. Upotrebom steganografije potencijalnim napadačima se znatno otežava proces razotkrivanja tajne komunikacije jer se od njih skriva informacija da je do komunikacije uopšte i došlo.

Ovo je poslužilo kao osnova za sagledavanje aktuelnih problema u ovoj oblasti, kao i za analizu postojećih rešenja za zaštitu. Na osnovu utvrđenih problema i nedostataka postojećih rešenja za zaštitu, predložen je sopstveni model zaštite koji se, kao takav, po prvi put koristi kao kompletan sistem za privatnu, tj. tajnu komunikaciju.

Kombinovanjem kriptografskih metoda koje obezbeđuju tajnost, autentičnost i integritet, uz primenu steganografskih metoda za razmenu informacija na skriven način, korisnici tajne komunikacije mogu na efikasan i siguran način da razmenjuju tajne poruke, uvereni da one nisu u međuvremenu promenjene od strane nekog trećeg lica i da su tajni ključevi kojima se obezbeđuje tajnost razmenjeni na siguran način.

Slanje tajnih ključeva javnim komunikacionim kanalom, kao što je to internet, se smatra nebezbednim. Shodno tome, predloženi model koristi lična identifikaciona dokumenata građana Republike Srbije, na kojima su upisana dva kvalifikovana digitalna sertifikata izdata od strane sertifikacionog tela MUP Republike Srbije (*MUPCA*). Uz pomoć programa razvijenog u Java programskom jeziku pristupa se kvalifikovanim digitalnim sertifikatima na kojima se nalaze dva para *RSA* ključeva. Ovi ključevi se mogu koristiti za digitalno potpisivanje i šifrovanje, respektivno, a u predloženom modelu oni se koriste za šifrovanje tajnih ključeva, kojima se obezbeđuje tajnost, i autentifikaciju korisnika tajne komunikacije. *RSA* algoritam koji se u ovom slučaju koristi smatra se pogodnim i praktičnim za digitalno potpisivanje i šifrovanje.

Razvoj programa koji za šifrovanje i dešifrovanje koristi *RSA* ključ, koji se nalaze na kvalifikovanom digitalnom sertifikatu ličnog identifikacionog dokumenata, treba da ukaže na jednostavnost upotrebe predloženog sistema za tajnu komunikaciju i širok spektar mogućnosti koje se nude krajnjim korisnicima. Takođe, važno je napomenuti da postoje programski alati koje nudi *MUPCA* u okviru svojih usluga, koji vrše digitalno potpisivanje i očitavanje ličnog identifikacionog dokumenta, međutim, ne postoji javno

dostupan programski alat kojim bi se izvršilo šifrovanje *RSA* ključem koji se nalazi na ličnom identifikacionom dokumentu građana Republike Srbije.

1.1. Očekivani doprinosi

1.1.1. Stručni doprinos

Osnovni doprinos ovog rada, na osnovu razmatranih iskustava iz teorije i prakse, ogleda se u razvoju i primeni jednog novog sveobuhvatnog sistema za tajnu komunikaciju koji unapređuje protokol za razmenu kriptografskih ključeva. Predloženi sistem za tajnu komunikaciju koristi kvalifikovane digitalne sertifikate sa ličnih identifikacionih dokumenata građana Republike Srbije za distribuciju tajnih ključeva, kojima se obezbeđuje tajnost, i autentifikaciju korisnika tajne komunikacije.

Upotrebom ličnih identifikacionih dokumenata građana Republike Srbije se obezbeđuje široka dostupnost predloženog sistema tajne komunikacije, a primenom programa razvijenog u Java programskom jeziku, koji će biti javno dostupan svim građanima Republike Srbije, se znatno olakšava upotreba ličnih identifikacionih dokumenata u tajnoj komunikaciji.

Poseban doprinos se ogleda u tome što je u ovom radu razvijen novi program u Java programskom jeziku, korišćenjem standardne metodologije i alata za softversko modelovanje, radi proširivanja funkcionalnosti postojećih aplikacija za digitalno potpisivanje i šifrovanje korišćenjem ličnih identifikacionih dokumenata građana Republike Srbije.

1.1.2. Naučni doprinos

Naučni doprinos ovog rada ogleda se u analizi postojećih rešenja, gde će se jasno ukazati na prednosti i nedostatke tih rešenja. Rezultati ove analize treba da omoguće jasno sagledavanje trenutnog stanja u oblasti istraživanja i da daju osnovu za predlaganje novog sistema tajne komunikacije koji unapređuje eventualne nedostatke postojećih rešenja.

U skladu sa do sada navedenim, očekivani doprinosi ovog rada su:

- Novi protokol za razmenu tajnih ključeva na bazi ličnih identifikacionih dokumenata pošiljaoca i primaoca.
- Ne postoji potreba da se smešta i čuva veliki broj tajnih ključeva koji se mogu kompromitovati.
- Za svaku novu komunikacijsku sesiju generiše se novi tajni ključ koji korisnici tajne komunikacije lako i sigurno razmenjuju.

- Ostvaruje se potpuna *end-to-end* zaštita za svaku komunikaciju i za svaki par učesnika u tajnoj komunikaciji.
- Novi protokol je otporan na veliki broj napada na mreži.

Rezultati rada na ovoj doktorskoj disertaciji biće objavljeni u više radova u časopisima međunarodnog značaja i saopšteni na više naučnih skupova u zemlji i inostranstvu. Pojedine ideje su već izložene na međunarodnim stručnim konferencijama i časopisima.

1.2. Metode koje će se primenjivati u istraživanju

Metodologija istraživanja u ovom radu obuhvataće složen i organizovan postupak polazeći od logičkih načela i principa po utvrđenim fazama.

U istraživanju i prikupljanju primarnih i sekundarnih podataka, biće korišćene metode iz grupe osnovnih, opšte naučnih, posebnih i iz grupe statističkih metoda za prikupljanje podataka.

Složenost predmeta istraživanja zahteva primenu:

- analitičkih osnovnih metoda: metod analize, metod apstrakcije, metod specijalizacije i metod dedukcije;
- sintetičkih osnovnih metoda: sintezu, konkretizaciju, generalizaciju i indukciju;
- opštih naučnih metoda: hipotetičko-deduktivnu, analitičko-deduktivnu, komparativnu, statističku i metodu modelovanja.

Ovaj izbor istraživačkih metoda je upotrebljen da se istraživanje i tok istraživačkog procesa u svim fazama, tj. identifikaciji i definisanju problema, planiranju dizajna istraživanja, sakupljanju, obradi i analizi podataka, kao i formulaciji zaključaka, preکتno sprovede u skladu sa osnovnim principima naučno istraživačkog rada. Primenom ovih metoda, kako pokazuju dosadašnji rezultati istraživanja, moguće je validno ostvarenje naučnog i društvenog cilja istraživanja. Pristup istraživanju je interdisciplinaran i sintetički u tom smislu što se ni jednom metodološkom postupku ne daje isključiva prednost.

U prikupljanju podataka primeniće se: istraživanje, anketa i metoda analize sadržaja dokumenata.

Analiza će biti ostvarena na dva nivoa :

- na nivou eksperimentalne analize realnih subjekata i
- na nivou sekundarne analize rezultata ranijih istraživanja i adekvatne literature.

1.3. Cilj istraživanja

14

Cilj pokazuje osnovnu svrhu istraživanja. On može imati neposredno praktični, društveni, teorijski i naučni značaj.

Što se tiče teorijskog i naučnog cilja istraživanja, u predloženoj doktorskoj disertaciji pored analize teorijskih modela i principa za tajnu razmenu informacija, biće izvršena detaljna analiza postojećih pristupa u ovoj oblasti. Rezultati analize treba da ukažu na prednosti i mane postojećih sistema, s ciljem da se poboljša nivo zaštite prilikom tajne razmene informacija i dobije osnova za razvoj sopstvenog modela koji bi efikasno odgovorio na eventualne nedostatke postojećih rešenja.

Praktični cilj ovog istraživanja ogleda se u razvoju i primeni jednog novog sveobuhvatnog modela za tajnu komunikaciju, koji se kao takav, po prvi put koristi za privatnu, tj. tajnu komunikaciju. Predloženi novi model za tajnu komunikaciju korisnicima pruža mogućnost korišćenja steganografskih metoda u kombinaciji sa ličnim identifikacionim dokumenatima.

Sprovedena anketa među studentima prve godine Visoke tehničke škole strukovnih studija u Kragujevcu, studijskog programa Informatike, odmah nakon upisa, ukazuje na to da razvoj novog modela za tajnu komunikaciju treba da doprinese većoj društvenoj prihvatljivosti, koja treba da podstiče korisnike da koriste sredstva za zaštitu privatnosti koja su im lako dostupna. S podizanjem opšte svesti o jednostavnosti upotrebe predloženog modela i ukazivanjem na širok spektar mogućnosti koji se nude krajnjim korisnicima društveni cilj ovog istraživanja bi bio u potpunosti zadovoljen.

2

1.4. Naučne hipoteze

Hipoteze koje čine osnovu ovog rada:

- Razvojem novog sveobuhvatnog modela za tajnu komunikaciju koji objedinjuje upotrebu ličnih identifikacionih dokumenata sa steganografskim metodama poboljšava se nivo zaštite prilikom tajne razmene informacija.
- Realizovani model treba da obezbedi jednostavnost upotrebe, koja treba da podstiče korisnike da koriste sredstva za zaštitu privatnosti koja su im lako dostupna i mora da predstavlja sistem sa jasnim parametrima za tajnu komunikaciju u koji se može imati poverenja.
- Primena ličnih identifikacionih dokumenata u kombinaciji sa nekom steganografskom metodom potencijalnom napadaču u velikoj meri otežava proces razotkrivanja tajne komunikacije, a samim tim umanjuje se i verovatnoća da će doći do kriptanalize šifrovanih informacija.

Posebne hipoteze:

- Korisnici koji žele da primenjuju predloženi model za tajnu komunikaciju moraju da koriste usluge "treće strane od poverenja", tj. sertifikacionog tela koje izdaje kvalifikovane digitalne sertifikate na ličnim identifikacionim dokumentima.
- RSA ključ od 2048 bita koji se koristi u ličnim identifikacionim dokumentima građana Republike Srbije se još uvek smatra bezbednim.

1.5. Struktura doktorske disertacije

Doktorska disertacija se sastoji iz 8 (osam) poglavlja: Uvod, Pregled u oblasti istraživanja, Teorijske osnove istraživanja, Pregled postojećih rešenja, Model predloženog rešenja, Evaluacija predloženog rešenja, Zaključak i Literatura.

U prvom poglavlju je opisan predmet istraživanja, naznačeni su motivi za izradu jednog novog rešenja za tajnu komunikaciju, navedeni su očekivani doprinosi, prikazana je metodologija istraživanja, date su naučne hipoteze i cilj istraživanja.

Drugo poglavlje predstavlja pregled u oblasti istraživanja. Metodološki su analizirani naučni radovi iz vrhunskih međunarodnih časopisa, naučni radovi sa relevantnih međunarodnih konferencija i skupova, objavljenih knjiga i standarda.

U trećem poglavlju su opisane teorijske osnove koje su relevantne za oblast istraživanja. Dat je kratak pregled savremene kriptografije, uz istorijski osvrt ka razvoju kriptografskih sistema, kao i teoretske osnove steganografije.

Četvrto poglavlje predstavlja pregled postojećih rešenja koja se već koriste i koja su relevantna za oblast istraživanja. Dat je prikaz softverskih rešenja i opisane su njihove prednosti i uočeni nedostaci. Broj postojećih rešenja je sveden na ona koja su se koristila za poređenje sa predloženim rešenjem za tajnu komunikaciju iz ove disertacije.

Peto poglavlje opisuje predloženo rešenje za tajnu komunikaciju i prikazuje metod njegove primene. Dat je opis problema koji je bio i motiv za rad na ovoj doktorskoj disertaciji.

Šestim poglavljem su prikazani rezultati simulacija modela koji su doveli do razvoja novog sistema za tajnu komunikaciju, prikazana su poređenja predloženog rešenja sa već postojećim rešenjima opisanim u poglavlju četiri. Prikazani rezultati sprovedene ankete sa izvedenim zaključcima koji su proistekli iz iste. Dat je kritički osvrt na delove sistema za tajnu komunikaciju koji mogu da utiču na bezbednu upotrebu istog i date smernice za unapređenje nedostataka.

Sedmo poglavlje je zaključak gde su jasno izdvojeni naučni i stručni doprinosi ove doktorske disertacije i predloženi su pravci daljih istraživanja

U osmom poglavlju je dat spisak literature koja je korišćena u ovaj doktorskoj disertaciji.

2. Pregled u oblasti istraživanja

Bezbedna razmena kriptografskih ključeva je tema o kojoj se u nauci i profesionalnoj upotrebi kriptografije stalno govori. Može se reći da je to jedna od najslabijih karika u izgradnji jednog sistema za tajnu komunikaciju. Poznato je da postoji veliki broj za sada dokazano bezbednih rešenja, koja su pri tom i efikasna u praksi. O razmeni kriptografskih ključeva napisan veliki broj naučnih radova. Mnoga od tih rešenja su predstavljena samo u teoriji, neka su nedostupna za široku javnu upotrebu, a postoje i ona rešenja koja su komercijalno dostupna. Pored bezbedne i efikasne razmene ključeva oblast istraživanja ove disertacije pokriva i oblast tajne komunikacije, steganografiju i elektronska identifikaciona dokumenta (engl. *Electronic identity – eID*).

Lični identifikacioni dokument sa čipom građana Republike Srbije (Biometrijska lična karta) je u posebnom fokusu ovog istraživanja jer spada u grupu *eID*. Proširena primena *eID*, pored očigledne i jednostavne identifikacije, je trenutno u trendu kako kod nas, tako i svuda u svetu. Portali elektronske uprave, na državnom i lokalnom nivou, koji se razvijaju kod nas u zemlji omogućavaju građanima da veliki deo administrativnih stvari završe preko interneta sa svojih kućnih računara. Međutim, lični identifikacioni dokument sa čipom možemo posmatrati kao pametnu karticu (engl. *smart card*) pošto u sebi ima integrisan elektronski čip sa kojim je moguće sprovesti i niz drugih netipičnih aktivnosti, što će biti i prikazano u ovom poglavlju i disertaciji uopšte.

Pregled u oblasti istraživanja ove doktorske disertacije može se svesti na sledeće kategorije, koje su u velikom broju naučnih radova na neki način međusobno povezane:

1. razmena ključeva,
2. tajna komunikacija,
3. steganografija i
4. elektronski identifikacioni dokument.

Jedan od najnovijih pristupa u oblasti razmene ključeva je protokol za distribuciju ključeva na siguran i efikasan način putem grupne komunikacije koja je zasnovana na Adi Šamirovoj¹ šemi deljenja tajne [1]. Analizom drugih protokola autori su došli do zaključka da je njihova šema otporna na pasivne napade koji podrazumevaju prisluškivanje i nadgledanje komunikacionog kanala, napad "ponovnog slanja" (engl. *replay attack*) gde napadač lažno ponavlja prenos podataka koji je već korišćen u komunikaciji, kao i napad lažnog predstavljanja u kojem napadač preuzima identitet jedne od legitimnih strana u komunikaciji.

¹ Adi Šamir, izraelski kriptograf, jedan je od pronalazača *RSA* algoritma.

Sveobuhvatan pregled radova iz oblasti istraživanja [2], čiji je fokus bio na naučnim radovima koji se bave upravljanjem i distribucijom ključeva u mobilnim i *Cloud* mrežama, se analizom: sadržaja, prikazanih rezultata, performansi, doprinosa u oblasti istraživanja, društvene korisnosti i drugim faktorima, izdvojilo više radova. Kao relevantni za oblast istraživanja ove doktorske disertacije izdvajaju se radovi koji se bave: sigurnom komunikacijom među korisnicima društvenih mreža, generisanjem i opozivom ključeva na *Cloud* prostorima za skladištenje podataka i rešavanjem problema "curenja" (engl. *leakage*) tajnog ključa uspostavljanjem efikasne provere identiteta [3, 4 i 5].

Postoje razne inicijative zemalja širom sveta za poboljšanje sistema koji bi mogli nazvati elektronski zdravstveni sistem (engl. *e-health*), među kojima se izdvajaju Australija, Velika Britanija, Kanada, SAD, Holandija i Singapur. Predloženi sistem eliminiše složenu proceduru upravljanja digitalnim sertifikatima na način koji ne ugrožava sigurnost jednog složenog sistema kao što je to infrastruktura javnih ključeva [6]. Sličan pristup i novu efikasnu implementaciju deljenja digitalnog sertifikata standardnog formata X.509 između uređaja kao što su to pametni telefoni i personalni računari prikazan je kao primer za poslovno okruženje [7].

Sigurnosni protokol zasnovan na infrastrukturi javnih ključeva predložen je za implementaciju sigurnosnih mehanizama u operacijama prenosa podataka između satelita. Protokol je eksperimentalno razvijen i implemetiran kako bi pokazao da se protokolom zasnovanom na infrastrukturi javnih ključeva rešava problem bezbednosnih zahteva i obezbeđuju servisi autentifikacije, integriteta i poverljivosti podataka [8]. Razmena ključeva u mobilnim *Ad hoc* mrežama (engl. *MANET*), gde svaki čvor u mreži generiše svoje parove javnih i privatnih ključeva oslanja se na principe asimetrične kriptografije. Prednost ovakvog načina razmene ključeva se ogleda, prema tvrdnjama autora, u tome što se kreira više nezavisnih sertifikata koje potpisuje više različitih čvorova u mreži [9]. Uprkos uspešnoj primeni infrastrukture javnih ključeva uočeni su i nedostaci koji se ogledaju u tome da postoji mogućnost falsifikovanja digitalnih sertifikata. Za rešavanje pomenutog nedostatka predloženo je nekoliko efikasnih rešenja. Grupa autora [10] je predložila efikasno rešenje koje omogućava *TLS* serveru (*Transport Layer Security – TLS*) da detektuje napad koji ima za cilj da prouzrokuje falsifikovanje digitalnog sertifikata, kao i da sazna odakle napad potiče. Analiza [11] i poređenje simetrične kriptografije sa asimetričnom kriptografijom, kao i osvrt na prednosti i nedostatke infrastrukture javnih ključeva, podstakla je autora da predloži rešenje koje zadovoljava bezbednosne standarde u *Cloud* tehnologijama.

Asimetrični algoritam koji se najviše koristi u kombinaciji sa infrastrukturom javnih ključeva je *RSA*. Rešenja i primeri koji streme ka poboljšanju implementacije i primene jednog ovako robusnog algoritma su brojni. Softversko rešenje primenom *C#* programskog jezika u kombinaciji sa *SQL Server 2008 R2* koje ima za cilj da ubrza algoritam tokom prenosa podataka između različitih komunikacionih mreža, prikazano je kroz nov metod za razmenu ključeva između dva mrežna uređaja [12]. Diffie-Hellman

protokol za razmenu ključeva je poslužio kao osnova mnogim autorima da razviju svoje metode za razmenu ključeva u asimetričnoj kriptografiji. Skraćeno se često u literaturi on naziva i *DHKE* (*Diffie-Hellman Key Exchange*). *DHKE* je bio osnova za razvoj novog protokol, jasnog koncepta i praktične primene na mreži, koji pruža zaštitu privatnosti i predstavlja nove pravce primene u *IKE* (*Internet Key Exchange*) standardu [13].

Identifikacija i autentifikacija korisnika su važni servisi koji se primenjuju u nacionalnim službama elektronske uprave. Ove službe su u nekim zemljama dostigle visok stepen razvoja u kojima bitnu ulogu imaju elektronska identifikaciona dokumenta (engl. *electronic identification* – *eID*). U okviru strategije za razvoj, implementaciju servisa e-uprave i prihvatanja *eID* od strane pružaoca usluga, nacionalna služba za e-upravu Austrije je razvila nov modul pod nazivom *MOA-ID*. Grupa autora je iskoristila *MOA-ID* kako bi predstavila tri različita pristupa o tome kako se primena austrijske *eID* može sigurno premestiti u *Cloud* bez kršenja bilo kakvih aspekata privatnosti ili zaštite podataka. Na osnovu evaluacije predloženih pristupa predložen je model koji se oslanja na različite kriptografske metode, uz minimalnu promenu servisa za identifikaciju i autentifikaciju austrijske *eID*, i omogućava sigurnu upotrebu *eID* u nesigurnom okruženju [14, 15].

Grupa autora [16] je uočila i prikazala pretnje koje su opisane kao napad "oslušivanja" (engl. *sniffing*) terminala koji očitava pametnu karticu i napad kojim se vrši promena poruke neposredno pre potpisivanja digitalnim potpisom. Svoje istraživanje su završili predlogom novog protokola koji koristi osnove protokola za vremensko označavanje (engl. *timestamping protocol*).

Sigurna šema za autentifikaciju zasnovana na španskim *eID* prikazana je na primeru automobilske *Ad hoc* mreže (engl. *Vehicle Ad Hoc Networks* – *VANETs*) [17]. Autori su predstavili siguran protokol koji omogućava vozilima vlasti (policija, i tome sl.) da brzo i na zahtev preko *VANET* mreže dobiju stvarni identitet vozača. Evaluacija predloženog protokola je izvršena na simulacionom modelu koji je pokazao da je predloženi protokol imao 60–70% uspešnih detekcija identiteta vozača vozila. Grupa autora [18] je takođe koristila španski *eID* kako bi predstavila sistem za potvrdu identiteta pomoću bežične *NFC* (*Near Field Communication*) tehnologije uz pomoć kriptografskih metoda.

Federativno upravljanje identitetom je metoda koja je predstavljena sa ciljem lakšeg upravljanja entitetima koji sarađuju međusobno bez centralizovane kontrole. Ovo se odnosi pre svega na Evropsku uniju koja ima nasleđene *eID* sisteme svojih članica. Predstavljeno je objedinjeno evropsko rešenje za *eID* koje ima za cilj da opslužuje oko 500 miliona ljudi, a u planu je i proširenje na izdavanju *eID* za kompanije. Nakon evaluacije koja je podrazumevala proveru performansi i skalabilnosti predloženog rešenja, došlo se do zaključka da je predloženo rešenje izvodljivo uzimajući u obzir i sigurnosna ograničenja [19]. Pomenuta metoda i kreiranje *eIDAS* (*electronic IDentification, Authentication, and trust Services* – *eIDAS*) bila je predmet istraživanja grupe autora [20] koja je posmatrala scenario u kome se zahteva da se prvo sprovede

servis autorizacije, a nakon toga autentifikacija. Ovo se odnosi prevashodno na kontrolu pristupa nekom mrežnom servisu, gde pružalac usluge vodi računa o kontroli pristupa pre nego što se izvrši autentifikacija korisnika. Ponuđena su rešenja koja se primenjuju na aplikativnom i transportnom mrežnom sloju, respektivno. Mnoge zemlje, koje su uvele *eID*, koriste rešenja koja za potvrdu o identitetu vrše obelodanjivanje svih podataka koji se nalaze na *eID* [21, 22]. Naravno ovo predstavlja problem koji zalazi u domen zaštite privatnosti građana, pa su autori predložili jedan model koji selektivno otkriva potrebne podatke po potrebi.

Veliki broj evropskih zemalja počela je da koristi *eID* za aplikacije koje su izdate od strane državne uprave i od strane privatnih kompanija. Jedan od takvih primera je nemački *eID* koji predstavlja pametnu karticu mogućnošću beskontaktnog očitavanja, koja ima za cilj da zaštiti privatnost korisnika koristeći jaku kriptografsku autentifikaciju između korisnika i pružaoca usluga. Predloženo je korišćenje pseudonimne autentifikacije za pristup servisu usluga uz očitavanje samo potrebnih podataka, što je predstavljeno kao mera zaštite privatnih podataka korisnika [23]. Rad [24] koji takođe uzima u razmatranje austrijski *eID* ali ovoga puta u segmentu mobilnih tehnologija prikazuje kako se jedan novi postupak autentifikacije koristi kao sredstvo da se premosti jaz između različitih vrsta uređaja i usluga. Prikazana je evaluacija rešenja, u toku probnog korišćenja komponente, koje donosi sigurnu autentifikaciju na "pametnim" telefonima.

Slabosti i ranjivost sistema koji primenjuju *eID* razmatran je na slučaju estonske *eID* [25]. 2017. godine je otkriven sigurnosni rizik na estonskom *eID*, tj. u algoritamska greška unutar *RSA* biblioteke koja se nalazi na čipu *eID*. Preko 800000 estonskih *eID* i više od 200000 čipova koje je proizvela kompanija *Infineon* je bilo od 2014. godine pod rizikom. Ažuriranje digitalnih sertifikata na daljinu je omogućilo Estoniji da prevaziđe ovu krizu.

Mnogi autori su za prikrivanje informacija koristili različite tehnike steganografije [26]. S obzirom da napadač nije svestan postojanja komunikacije u nekom komunikacionom kanalu učinilo se kao vrlo interesantno za istraživanja. Grupa autora [27] je koristila steganografski metod zasnovan na diskretnim kosinusnim transformacijama u cilju skrivanja tajnih informacija u najmanje bitnim bitovima. Oni su koristili niske i srednje frekvencije za analizu njihovih performansi pomoću *PSNR* (engl. *Peak Signal to Noise Ratio*) i *MSE* (*Mean Square Error*) metoda. Istraživanja su pokazala da srednja frekvencija ima veću sposobnost prikrivanja, kao i bolji odnos signala i šuma, na osnovu čega su zaključili da predloženi steganografski alat omogućava relativno visok kapacitet ugradnje, bez bitnog vizuelnog izobličenja slike i da se pri tom održava tačnost skrivenih podataka. Autori [28] su predložili steganografsku tehniku za poboljšanje kvaliteta stego slike kao i povećanje steganografske sposobnosti. Predložena metoda se oslanja na minimiziranje tajne poruke što je više moguće pre ugradnje. Algoritam, nazvan od strane autora *DCT-M3*, koristi razlike između dva *DCT* (engl. *discrete cosine transform*) koeficijenata za ugradnju tajne poruke u *JPEG* sliku.

Dobijeni rezultati su pokazali da predloženi algoritam znatno smanjuje broj promena na *JPEG* slici tokom ugradnje poruka različite dužine. Na osnovu sprovedenih analiza zaključili su da algoritam *DCT-M3* daje bolje rezultate u poređenju sa najčešće korištenom *LSB* (engl. *least significant bit*) tehnikom steganografije.

Steganografija koja primenjuje *JPEG* sliku za sigurnost vizuelnih sadržaja na mrežnim društvenim mrežama je veoma aktuelno polje istraživanja, gde su osetljivi sadržaji ugrađeni u *JPEG* slike, zadržavajući svoj vizuelni kvalitet. Istraživači su do sada koristili korelacioni prostor boja, kao što je *RGB*, gde promena jednog parametra utiče na ukupni kvalitet stego slika, smanjujući na taj način njegovu pogodnost za steganografske algoritme. Adaptivni metod *LSB* supstitucije upotrebom nekorelisanog prostora u boji smanjuje šanse otkrivanja pomoću sistema ljudskog vida. U predloženoj šemi, ulazna slika prolazi kroz program za kodiranje slika, što kao rezultat daje šifrovanu sliku, koja se zatim se konvertuje u *HSV* prostor boja pogodan za dalju obradu. Ideja za korišćenje *HSV* prostora boja za skrivanje podataka potiče iz njegovih svojstava koja se ogledaju u dekorelaciji, ekonomičnosti u obradi, boljem kvalitetu slike i pogodnosti za steganografiju. Kvantitativni i kvalitativni eksperimentalni rezultati predloženog modela i njegove primene, kao i sigurnost i privatnost vizuelnih sadržaja na mrežnim društvenim mrežama, potvrđuju njegovu efikasnost za razliku od najsavremenijih (*state-of-the-art*) metoda [29].

Grupa autora [30] je dala novu i efikasnu metodologiju korišćenjem *JPEG* slika u steganografiji, primenom metode *LSB*. Ovaj sistem steganografije se kombinuje sa *RSA* algoritmom. Prema tvrdnji autora, korišćenje steganografske metode štiti prenete podatke od "curenja" u komunikacionom kanalu, pogotovo kada se koristi višestruki prenos podataka koji se odnosi na deljenje stego nosača između većeg broja korisnika.

Kombinovanje reverzibilnog skrivanja podatak i šifrovanja, kako bi se dobila maksimalna sigurnost, predstavljeno je kao nov pristup za ostvarivanje servisa poverljivosti, integriteta i autentifikacije [31]. Predloženi metod koristi steganografiju sa A-S [32] sekvencijalnim algoritmom za šifrovanje. Predloženi metod je veoma brz i pruža visoku sigurnost. Rezultat ispitivanja pokazuje da je predložena metoda vrlo efikasna i dobro izvedena.

U radu [33] predstavljen je steganografski alat *CrypSteg* za umetanje podataka u slike koji kombinuje kriptografiju i steganografiju u jednom algoritmu. Ova metoda pokazuje svoj veći kapacitet za skrivanje podataka od ostalih metoda jer ugrađuje 4 bita informacija u blok od 4 h 4 piksela. Ovaj alat se primenjuje na onim slikama čiji su pikseli homogeno raspršeni i koristan je za utiskivanje male količine podataka. Eksperimentalni rezultati pokazuju da je metoda veoma efikasna naročito kada se primenjuje na one binarne slike čiji su pikseli u boji raspoređeni vrlo jednoliko.

Analiza aktuelnih steganografskih tehnika i metoda primenjenih na različitim multimedijalnim fajlovima, sa akcentom na primeni steganografije u *JPEG* slikama, prikazana je uz primenu različitih transformacionih tehnika [34]. Pored metoda za

prikrivanje informacija dat je pregled metoda za detekciju utisnutih informacija, tj. stegoanaliza. Grupa autora je [35] predložila korišćenje alata *StegApp* s kojim bi se skrivala tajna poruka, čime bi se dobila *JPEG* slika kao stego nosač, koja bi nakon toga bila smanjena na veoma malu veličinu i kao takva bila umetnuta u *Microsoft Word* dokument.

3. Teorijske osnove istraživanja

Potreba da se razmena informacija učini bržom i efikasnijom podstakla je razvoj informaciono-komunikacionih tehnologija. Razvoj sve većeg broja telekomunikacionih i internet servisa, doveo je do porasta broja korisnika tih usluga, a samim tim povećala se i količina razmenjenih informacija. Informacije koje se razmenjuju putem javnog komunikacionog kanala mogu biti kompromitovane ukoliko nisu zaštićene na adekvatan način. Uporedo sa razvojem informaciono-komunikacionih tehnologija razvijaju se i načini za zaštitu razmenjenih informacija.

Razmena informacija na siguran način, koji podrazumeva da iste budu dostupne samo onome kome su i poslate, oduvek je predstavljala potrebu, još od vremena starih civilizacija. Poznato je da izraz "Kriptografija" potiče iz grčkog jezika i da predstavlja nauku o "tajnom pisanju" [36]. Gledano kroz istoriju kriptografija se u početku isključivo koristila u vojne i diplomatske svrhe. Ljudi su se na razne domišljate načine trudili da razmena poruka bude nerazumljiva nekoj trećoj strani koja bi bila u mogućnosti da presretne poslatu poruku. U vreme antičke države Sparte zabeleženo je korišćenje sistema za šifrovanje zvanog Skitale. Nakon toga, za vreme Rimljana koristio se šifarski sistem Cezarova šifra, nazvan po Gaj Julije Cezaru. Hronologija pojavljivanja i korišćenja šifarskih sistema je zabeležena u mnogim knjigama i udžbenicima, a među prvima koja se pojavila je knjiga Dejvida Kana¹ "Razbijači šifara" (engl. *The Codebreakers*), za koju se smatra da je podstakla nove autore da pišu i izdaju nove radove o kriptografiji iako je američka Nacionalna agencija za bezbednost (engl. *National Security Agency – NSA*) pokušavala to da suzbije [37].

Pored klasičnih kriptografskih metoda koje se koriste za razmenu informacija uz pomoć šifrovanja, za prikrivenu razmenu informacija razvijene su steganografske metode kojima se skrivaju informacije unutar neke datoteke. Steganografija se suštinski razlikuje od kriptografije iako se obe nauke koriste kako bi se sačuvala tajnost podataka. Korišćenjem steganografije moguće je izbeći napad "čovek u sredini" [38] jer se napadačima znatno otežava proces razotkrivanja tajne komunikacije time što se od njih skriva informacija da je do komunikacije uopšte i došlo. Kao i kriptografija, steganografija se takođe koristi od davnina kada su se ljudi koristili raznim trikovima za prikrivanje poruka, npr.: korišćenje nevidljivog mastila, razne oznake na samim slovima koja su napisana, i tome sl. U današnje vreme, upotrebom računara, moguće je poruke sakrivati tako što se one utiskuju u različite digitalne datoteke.

¹ Dejvid Kan (David Kahn) američki pisac, istoričar i novinar koji je napisao hronologiju kriptografije od starog Egipta pa sve do 1967. godine kada je knjiga i objavljena.

3.1. Kriptografija

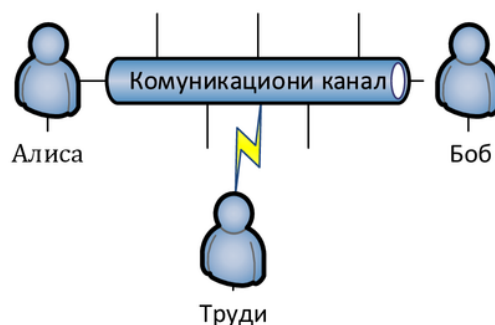
Godinama unazad kriptografija je predstavljala sredstvo za zaštitu koja se primenjivala uglavnom u vojnim okvirima, koja je bila pod direktnim nadzorom državnih organa. Razvojem računara i interneta kriptografija je, možemo reći, postala sveprisutna u javnim okvirima, iako je i dalje ostala dominantno vojna tehnologija [39].

Bez obzira u koju svrhu se koristi, osnovna svrha korišćenja kriptografije je da obezbedi tajnost. Međutim, primenom kriptografije možemo da zadovoljimo i druge zahteve koji se postavljaju ispred pojma bezbedna komunikacija: autentifikacija, integritet i neporecivost.

3.1.1. Osnovna pravila

U cilju predstavljanja kriptografskih principa u literaturi se definišu određeni pojmovi kao što su: pošiljalac (engl. *sender*), primalac (engl. *receiver*), komunikacioni kanal, otvoren tekst (engl. *plaintext*), šifrovan tekst (engl. *ciphertext*), ključ (engl. *key*), uljez (engl. *intruder*), itd.

Veoma često se u literaturi, u cilju jednostavnijeg predstavljanja problema, pošiljalac i primalac predstavljaju kao Alisa i Bob, a uljez kao Trudi, međutim, to ne mora da znači da se radi o ljudima već to mogu biti bilo koji uređaji (računari, mobilni telefoni, i tome sl.) ili pak procesi na samim tim uređajima. Ovo se može i predstaviti grafički, slika 3.1:



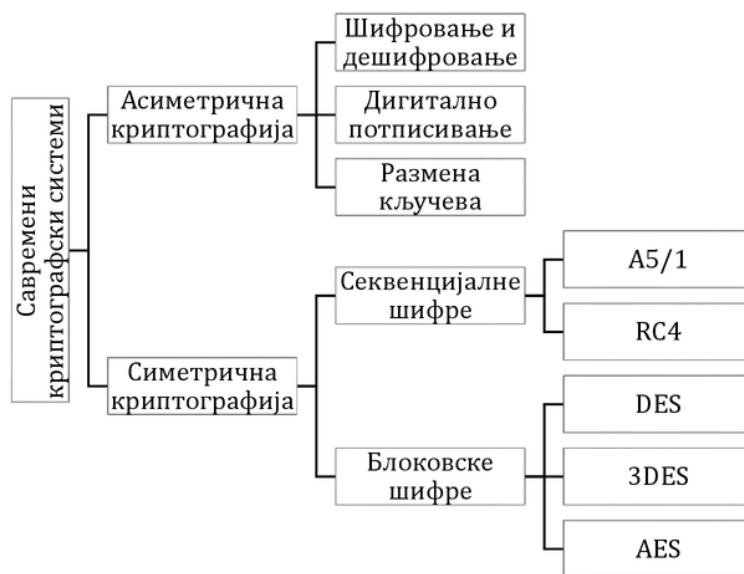
Slika 3.1. Komunikacija između Alise i Boba uz prisustvo uljeza Trudi

Tajnost poruke koju Alisa šalje Bobu može da se obezbedi šifrovanjem iste pomoću nekog kriptografskog algoritma i odgovarajućeg ključa. Autentifikacija ili provera identiteta treba da obezbedi da Bob bude sasvim siguran da je poruka koju je dobio stigla od Alise, tj. da Trudi nije uspjela da se umeša u komunikaciju i predstavi kao Alisa, a samim tim i prevari Boba. Integritet je servis od veoma velike važnosti jer se s njim garantuje da poruka koju je Alisa poslala Bobu nije u međuvremenu promijenjena, tj. da Trudi nije presrela poruku, izmenila njen sadržaj i tako izmenjenu poruku poslala

Bobu. Nemogućnost poricanja, tj. neporecivost, je servis koji treba da zaštiti Boba u slučaju da se Alisa predomisli i nakon nekog vremena počne da tvrdi da ona poruku uopšte nije ni poslala Bobu.

Da bi navedene servise Alisa i Bob mogli da sprovedu u delo moraju da to urade uz pomoć odgovarajućeg kriptografskog protokola. Kriptografski protokol predstavlja jedan algoritam ili niz koraka koji precizno opisuju interakciju između korisnika, bilo da se radi o dva ili više učesnika u komunikaciji [40]. Pre nego što uspostave komunikaciju Alisa i Bob se dogovaraju i biraju odgovarajući kriptografski protokol, način na koji će da razmene ključeve koji se koriste u kriptografskom algoritmu i druge korake koji će da im omoguće zaštićenu komunikaciju. Izbor kriptografskog protokola zavisi, pre svega, od načina na koji Alisa i Bob žele da ostvare sigurnu komunikaciju i oni se mogu definisati kao:

- Komunikacija uz primenu simetrične kriptografije.
- Komunikacija uz primenu kriptografije sa javnim ključem – asimetrična kriptografija.



Slika 3.2. Podela savremenih kriptografskih sistema

Na slici 2. je prikazana podela savremenih kriptografskih sistema sa nabrojanjem nekih od poznatijih realizacija tih sistema. Pobrojani su neki od praktično sigurnih kriptografskih algoritama. Poznato je, matematički dokazano, da apsolutno sigurni kriptografski sistem predstavlja jednokratna beležnica (engl. *one-time pad* - *OTP*) koji se i koristio u bližoj istoriji ali koji nije praktičan za većinu današnjih situacija u kojima se odvija komunikacija između dva korisnika [41].

Jednokratna beležnica je nepraktična za primenu u većini današnjih komunikacionih tehnologija iz razloga što dužina ključa za šifrovanje mora da bude iste

dužine kao i tekst (poruka) koji se šifruje. Drugo ograničenje je izbor samih ključeva za šifrovanje koji mora da zadovolji određene standarde po pitanju slučajnosti i jedinstvenosti, a nije ni jednostavno upravljati s njima jer se, po pravilu, jedan ključ može upotrebiti samo jednom nakon čega se uništava. Upotrebom jednokratne beležnice nije moguće proveriti identitet pošiljaoca, a takođe se mora voditi računa da pošiljalac i primalac budu savršeno sinhronizovani jer u suprotnom poruka koju primalac bude dobio neće imati nikakvog smisla. Primena jednokratne beležnice danas ima smisla jedino u komunikacionim kanalima koji zahtevaju veoma visok nivo bezbednosti.

Kako je apsolutnu sigurnost veoma teško ostvariti u današnje vreme se, u većini slučajeva, koriste kriptografski algoritmi koji obezbeđuju visok nivo zaštite ali koji ne zadovoljavaju pretpostavku apsolutne sigurnosti. Takvi sistemi su dovoljno dobri i pouzdani da se ostvari praktična bezbednost komunikacionog kanala i pogodni su da se koriste u računarskim sistemima. Njih drugim rečima nazivamo računarski sigurni šifarski sistemi i njihova sigurnost se zasniva na pretpostavci da protivnik ne raspolaže sa dovoljno računarske snage i vremena da bi u realnom vremenu mogao na neki način da naruši njihovu bezbednost i obezbedi sebi otkrivanje tajne poruke, delom ili u celosti, ili pak da dođe do otkrivanja kriptografskog ključa.

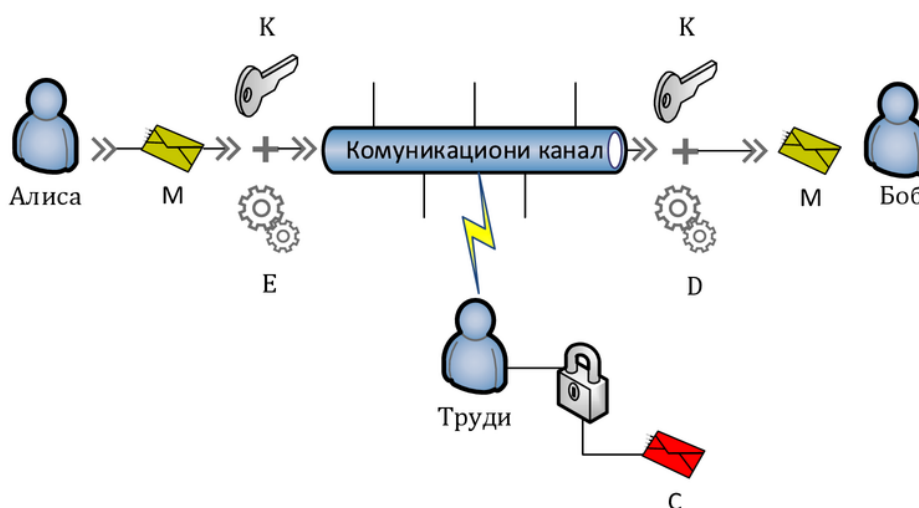
Pretpostavlja se da državne agencije, npr. *CIA*, *NSA*, *BND*, *SIS (MI6)* i njima slične svoje kriptografske algoritme drže u tajnosti. Međutim, osnovni princip kriptanalize, koji je postavio holandski kriptograf i lingvista *Auguste Kerckhoffs* još u XIX veku, glasi da sigurnost jednog kriptografskog sistema treba da zavisi isključivo od tajnosti kriptografskog ključa, a da je kriptografski algoritam, koji se koristi u postupku šifrovanja, opšte poznat. Ovaj fundamentalni princip se danas koristi u savremenoj kriptografiji, osim mogućih izuzetaka koji se odnose na državne agencije, i pouzdanost modernih kriptografskih algoritama je višestruko proveravana i dokazivana. Kada se kriptografski algoritam predstavi na takav način da bude javno dostupan svima on postaje predmet naučnih analiza stručnjaka iz celog sveta, od vojnih do akademskih, i na taj način se vrlo lako otkriva koliko je određeni postupak pouzdan i da li je otporan na razne napade iz domena kriptanalize. Na ovaj način se zapravo verifikuje njegova sigurnost.

Pojam kriptanaliza se odnosi na postupke koji se sprovode nad šifrovanim tekstom ili porukom u cilju otkrivanja teksta ili poruke, dela teksta ili poruke, otkrivanje postupka kojim je izvršeno šifrovanje, otkrivanje tajnog ključa ili bilo kakve druge informacije vezane za šifrovani tekst ili poruku. Uvek se polazi od pretpostavke da protivnik koji vrši kriptanalizu ima neograničene resurse na raspolaganju (novac, znanje, računarske resurse, ...) i da ima neograničeno vreme da sprovodi razne tehnike kriptanalize. Ono što mi jedino možemo da tvrdimo da je naš kriptografski sistem siguran ukoliko je najbolji poznati napad na njega napad pod nazivom potpuna pretraga ključeva. Potrebno je još naglasiti da se dešifrovanje razlikuje od kriptanalize jer

dešifrovanje podrazumeva akciju koju preduzima primalac kako bi pročitao šifrovanu poruku, dok kriptanaliza podrazumeva napad na kriptografski sistem [42].

3.1.2. Simetrična kriptografija

Savremeni kriptografski sistemi koji koriste algoritme za šifrovanje simetričnim ključem koriste ideje koje su se koristile u klasičnoj kriptografiji: transpozicija (premeštanje) i supstitucija (zamena). Prednosti koje je donela savremena tehnologija, pogotovo s razvojem savremenih računara, omogućila je kriptografima da kreiraju daleko složenije algoritme koji se daleko brže izvršavaju od onih koji su se koristili u klasičnoj kriptografiji. Princip po kome se izvršava jedan algoritam za šifrovanje simetričnim ključem prikazan na slici 3:



Slika 3.3. Algoritam za šifrovanje simetričnim ključem prikazan

Pretpostavićemo da Alisa i Bob dele tajni ključ (K) i da Alisa želi da pošalje poruku (M) Bobu putem otvorenog komunikacionog kanala [43]. Trudi ima mogućnost i odgovarajuće resurse da presretne šifrovanu poruku (C) koju Alisa šalje Bobu, međutim, Trudi nema tajni ključ i nije u mogućnosti da vidi šta je u poruci napisano. Ukoliko su Alisa i Bob ispoštovali fundamentalne principe kriptografije, sigurnost njihove tajne komunikacije zavisi od tajnog ključa koji su koristili za šifrovanje (E) i dešifrovanje (D) poruke. Matematički zapisano:

$$E_K(M) = C$$

$$D_K(C) = M$$

tj. ove funkcije imaju sledeće svojstvo:

$$D_K(E_K(M)) = M$$

Pored očiglednih prednosti koje donosi primena simetrične kriptografije u vidu brzine izvršavanja kriptografskog algoritma, količine podataka koji mogu da se šifruju i sigurnosti koji pružaju, postoji i nekoliko nedostataka na koje Alisa i Bob moraju da misle unapred, pre nego što uspostave tajnu komunikaciju. Ukoliko se Alisa i Bob nalaze na udaljenim lokacijama, npr. Evropa i Amerika, dogovor oko uspostavljanja sigurnog komunikacionog kanala je veoma komplikovan, pogotovo ako uzmemo i Trudi u obzir.

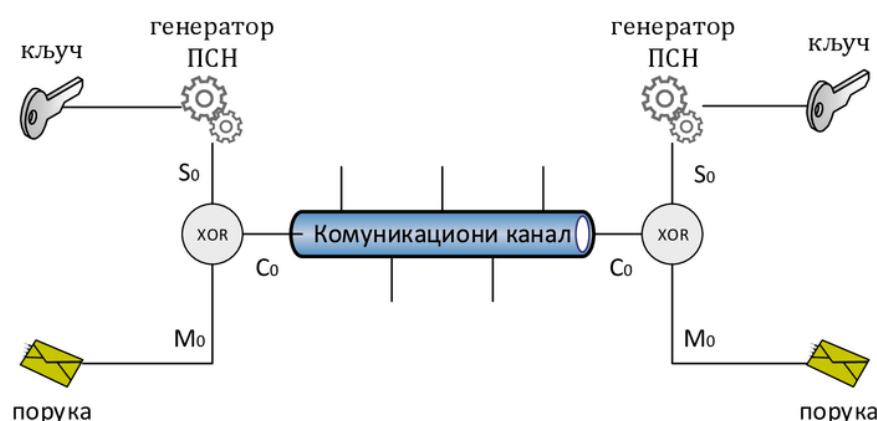
Pre svega, Alisa i Bob moraju da se dogovore u vezi kriptosistema koji će da koriste, nakon toga se dogovaraju o ključu i načinima kako će isti u tajnosti da razmene. Treba imati na umu da se ovde ne razmenjuje samo jedan ključ, već veći broj ključeva koji ne smeju biti kompromitovani. Ukoliko se radi o više korisnika, ne samo o Alisi i Bobu, problem razmene ključeva se dodatno usložnjava. Ovaj problem se rešava na različite načine, ličnom dostavom, uvođenjem centra za distribuciju ključeva (engl. *Key Distribution Center – KDC*) koji u celu priču uvodi i "treću stranu od poverenja" (engl. *Trusted Third Party – TTP*), korišćenjem kriptografije sa javnim ključem, itd. Pored razmene ključeva veoma bitna stvar u njihovoj tajnoj komunikaciji su servisi autentifikacije u cilju sprečavanja napada "čovek u sredini" i eventualno, ukoliko za tim ima potrebe, neporicanja.

Na osnovu načina na koji obrađuju podatke savremene algoritme za šifrovanje simetričnim ključem delimo na dve grupe:

- Algoritmi koji šifruju tokove podataka, tj. sekvencijalni šifarski sistemi (engl. *stream ciphers*).
- Algoritmi koji šifruju blokove podataka, tj. blokovski šifarski sistemi (engl. *block ciphers*).

3.1.2.1. Sekvencijalni šifarski sistemi

Karakteristika sekvencijalnih šifarskih sistema je da sa tajnim ključem K inicijalizuje niz pseudoslučajnih znakova $S = [s_0, s_1, s_2, \dots, s_i]$ koje generiše generator pseudoslučajnih nizova. Sa tako dobijenim pseudoslučajnim nizom S šifruje se XOR operacijom tok podataka $M = [m_0, m_1, m_2, \dots, m_i]$ koji predstavlja niz karaktera poruke koja se šalje. Tako generisani karakteri predstavljaju niz šifrovanih karaktera $C = [c_0, c_1, c_2, \dots, c_i]$, koji se drugim imenom zove šifrat [44]. Dešifrovanje se vrši na identičan način obrnutim postupkom od šifrovanja. Za svaku uspostavu veze između pošiljaoca i primaoca koristi se novi sesijski ključ koji se koristi zajedno sa tajnim ključem za dobijanje pseudoslučajnog niza.



Slika 3.4. Sekvencijalni šifarski sistem – početno stanje

Sekvencijalni šifarski sistemi nude znatno bolje performanse u poređenju sa blokovskim šifarskim sistemima, bar za faktor 4 – 5 ako se taj faktor meri brzinom. Međutim, sigurnost modernih sekvencijalnih šifarskih sistema nije toliko dobra kao kod algoritama koji šifruju blokove podataka. Većina sekvencijalnih šifarskih sistema koji su široko rasprostranjeni, poput *RC4* i *A5/1*, imaju sigurnosne slabosti [45, 46].

Algoritmi koji šifruju tokove podataka, iako imaju određene sigurnosne slabosti, koriste se najčešće za specijalne namene, poput *RC4* u računarskim mrežama ili *A5/1* u mobilnim *GSM* mrežama.

3.1.2.2. Blokovski šifarski sistemi

Algoritmi koji šifruju blokove podataka dele poruku na blokove tačno određene veličine i šifruje ih tajnim ključem koji je iste veličine kao i generisani blok podataka. Zapravo, blokovski algoritam koristi dva ulaza, ključ i blok bita koji su iste veličine čime se dobija šifrovan blok, takođe iste veličine. Na izlazu se šifrovan blok transformiše tajnim ključem ponovo u otvoren tekst [47].

Dva opšte prihvaćena principa za dizajniranje praktičnih šifarskih sistema, prema sugestiji Kloda Šenona², su principi konfuzije (engl. *confusion*) i difuzije (engl. *diffusion*). Blokovski šifarski sistemi kombinuju ta dva osnovna principa čime se dobija zadovoljavajuća kompleksnost algoritma. Svojstvo konfuzije treba da obezbedi minimalnu statističku vezu između poruke i šifrata, dok svojstvo difuzije treba da obezbedi da svaki bit poruke utiče na što veći deo šifrata. Blokovski šifarski sistemi, u zavisnosti od izbora algoritma koji se koristi, zadovoljavaju svojstva i ciljeve vezano za sigurnost i efikasnost, a najčešće se realizuju softverski [38, 40].

Najzastupljeniji algoritmi koji se koriste u blokovskim šifarskim sistemima su DES (engl. *Data Encryption Standard*), njegova poboljšana verzija 3DES (engl. *Triple*

² Američki naučnik i inženjer koji je postavio osnovne principe o teoriji informacija.

Data Encryption Standard) i AES (engl. *Advanced Encryption Standard*). Iako je izbor *DES* algoritma za šifrovanje pratio niz kontraverznih situacija u koje je bila umešana američka agencija *NSA*, koja je bila odgovorna za to da se inicijalna veličina ključa za šifrovanje smanji na 56 bita čime je sam algoritam znatno oslabljen, *DES* je postao opšte prihvaćeni standard za šifrovanje sredinom '70-ih i '80-ih godina HH veka. Što se tiče same umešanosti *NSA* agencije u kreiranje *DES* algoritma, postoje određena mišljenja da je *NSA* zapravo ojačala *DES* algoritam zamenom tzv. *S*-kutija koje su nudile zaštitu protiv do tada nepoznatih kriptanalitičkih napada. U svakom slučaju, *DES* algoritam je uspešno odolevao 30-ak godina intenzivnim kriptanalitičkim napadima čitave naučne zajednice, a danas je postao ranjiv samo zbog male dužine ključa (56 bita) koji se koristi.

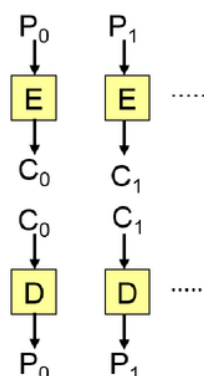
Krajem '90-ih ¹³ američki Nacionalni institut za standarde i tehnologiju (engl. *National Institute of Standards and Technology – NIST*) pokrenuo je proces za izbor novog kriptografskog standarda. Ovoga puta sam proces izbora novog standarda je bio transparentan i uključivao je veliki broj predloga poslatih od strane naučne i stručne javnosti širom sveta. *NSA* je i ovoga puta učestvovala u izboru novog standarda ali ovoga puta samo kao jedan od sudija. Izabran je kriptografski algoritam koji su razvili Joan Dajmen (*Joan Daemen*) i Vinsent Rejmen (*Vincent Rijmen*), belgijski kriptografi, koji je prvobitno po njihovim imenima bio nazvan *Rijndael*. *NIST* je 2001. godine proglasi ovaj algoritam pobednikom koji je nazvan *AES*. O ovom algoritmu je dostupno puno informacija i može se tvrditi da u istoriji nijedan kriptografski algoritam nije bio ispitivan kao *AES*. Otporan je na sve poznate napade i šifruje blokove veličine 128 bita ključevima od 128, 192 i 256 bita, što znači da *AES*-om možemo šifrovati blok od 128 bita ključem od 256 bita.

Veoma bitan parametar koji koriste svi algoritmi koji šifruju blokove podataka je način na koji to rade. Način rada blokovskog sistema za šifrovanje direktno utiče kako će se šifrovani blokovi spajati u konačan šifrat. Takođe, odabir ovog parametra direktno utiče na brzinu rada blokovskog šifarskog sistema. Postoje mnogi režimi koji se koriste u blokovskim šifarskim sistemima, a među njima se izdvajaju:

- Režim "elektronske kodne knjige" (engl. *Electronic CodeBook – ECB*).
- Režim ulančavanja blokova (engl. *Cipher Block Chaining – CBC*).
- Režim brojača (engl. *CounTeR mode – CTR*).

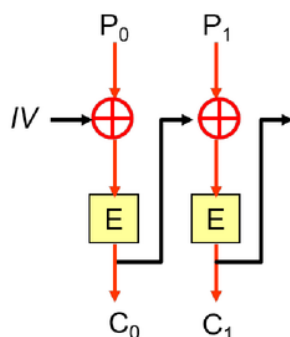
Režim *ECB* je jednostavan i popularan način primene blokovske šifre. U ovom režimu rada jedan blok otvorenog teksta se pretvara u isti blok šifrata. Takav način šifrovanja je identičan šifrovanju sa kodnom knjigom, koji se ranije koristio kroz istoriju, pa odatle i potiče naziv "elektronska kodna knjiga", slika 3.5. Blokovi otvorenog teksta se šifruju nezavisno, moguće je šifrovati prvo blokove u sredini, zatim na kraju teksta, pa tek onda one na početku teksta. Međutim, postoji ozbiljan nedostatak u primeni ovog režima koji navodi na to da se ovaj režim šifrovanja ne bi trebao primenjivati u praksi. Možemo da pretpostavimo da napadač zna deo otvorenog teksta i da poseduje nekoliko šifrovanih blokova. Napadač sada može da pokrene napad

prevođenja kodne knjige iako ne zna tajni ključ jer svako podudaranje šifrovanog bloka sa blokom otvorenog teksta otvara novi blok [37, 38].



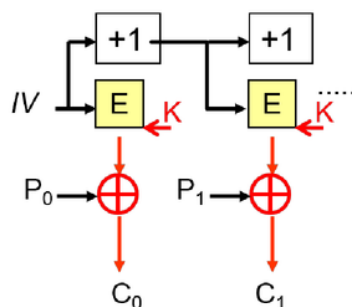
Slika 3.5. *ECB* režima rada

Režim *CBC* je najčešće korišćeni režim šifrovanja koji blokovskoj šifri dodaje mehanizam povratne sprege čime se dobija da je rezultat šifrovanja prethodnog bloka zapravo ulazna vrednost za šifrovanje narednog bloka. Početni blok u *CBC* režimu šifrovanja se sabira (*XOR*) sa inicijalnim vektorom *IV* koji se generiše na potpuno slučajnan način, a njegova dužina odgovara veličini bloka i koristi se samo za generisanje prvog bloka šifrata. Prednost ovakvog načina korišćenja blokovske šifre se ogleda u tome da isti blok otvorenog teksta neće odgovarati istom bloku šifrata. Ova osobina *CBC* režima šifrovanja daje dodatni nivo složenosti šifrovanim podacima. *CBC* režim šifrovanja je bezbedniji od *ECB* režima šifrovanja.



Slika 3.6. *CBC* režima rada

Režim *CTR* je specifičan po tome što omogućava potpunu nezavisnost između blokova. Pošto su svi blokovi nezavisni jedni od drugih mogu se paralelno obrađivati što ubrzava izračunavanje šifrata iz bloka otvorenog teksta i obrnuto. Kao i kod *CBC* režima i ovde se upotrebljava inicijalni vektor *IV* koji se šifrjuje, a zatim sabira (*XOR*) sa blokom otvorenog teksta. Početna vrednost brojača je broj jedan i za svaki naredni blok vrednost brojača i inicijalnog vektora se uvećava za jedan [48].



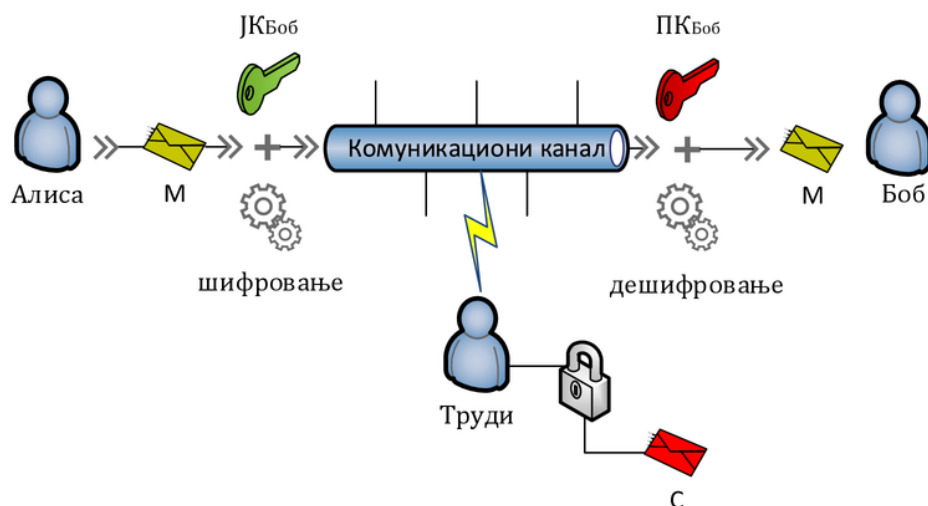
Slika 3.7. CTR režima rada

Može se zaključiti da se CTR režim ponaša kao sekvencijalna šifra.

3.1.3. Asimetrična kriptografija

1 Rad koji su *Whitfield Diffie* i *Martin Hellman* objavili 1976. godine predstavljao je ideju kriptografije u kojoj nije bilo neophodno da dve strane u šifrovanoj komunikaciji posедуju isti ključ [48]. Dve godine kasnije *Kohnfelder* je u svom diplomskom radu [50] predstavio pojam sertifikata kao digitalno potpisanog podatka koji vezuje javni ključ sa osobom kojoj taj ključ pripada, dok su *Rivest, Shamir* i *Adleman* pronašli metod praktične realizacije asimetrične kriptografije [51], po kojima je nazvan najpoznatiji algoritam asimetrične kriptografije – *RSA*. Ovo su bile osnovne ideje koje su uz pojavu interneta dovele do razvoja asimetričnih šifarskih sistema, koji se smatraju za jedno od najvećih istorijskih dostignuća u kriptografiji.

Princip korišćenja dva ključa, javnog i privatnog, je prikazan na primeru komunikacije između Alise i Boba, slika 3.8:



Slika 3.8. Princip slanja šifrovane poruke u asimetričnoj kriptografiji

Karakteristika i osnovna razlika asimetrične kriptografije u odnosu na simetričnu kriptografiju je ta da se u asimetričnoj kriptografiji koriste različiti ključevi za šifrovanje i dešifrovanje podataka. Često se za asimetričnu kriptografiju u literaturi navodi da je to kriptografija sa javnim ključem (engl. *Public Key Cryptography*). Objavljivanjem jednog ključa koji postaje javni podatak ne ugrožava se tajnost drugog ključa. Suština je u tome da se javni ključ koristi za šifrovanje, a privatni ključ, koji se uvek čuva u tajnosti, koristi za dešifrovanje. Koristeći notaciju koja je navedena za šifrovanje i dešifrovanje kod simetričnih kriptografskih sistema, matematički zapisano asimetrična kriptografija, uz dodatak da javni ključ obeležavamo sa JK, a privatni ključ sa PK, se koristi na sledeći način:

$$E_{JK}(M) = C_1$$

$$D_{PK}(C_1) = M$$

Šifrovanje privatnim ključem, što se isključivo koristi kod digitalnog potpisivanja matematički može da se prikaže kao:

$$E_{PK}(M) = C_2$$

$$D_{JK}(C_2) = M$$

Prvi korak u komunikaciji je da Alisa zatraži od Boba njegov javni ključ (JK_{Bob}). Bob bez ikakve bojazni svoj javni ključ može da objavi ili da ga pošalje Alisi putem otvorenog komunikacionog kanala. Alisa sada može da šifrue poruku Bobovim javnim ključem sa odgovarajućim asimetričnim algoritmom i da tako šifrovanu poruku pošalje Bobu. Trudi je mogla da preuzme Bobov javni ključ i da presretne Alisinu šifrovanu poruku, međutim, Trudi ne može da dođe do otvorenog teksta jer Bobov javni ključ služi samo za šifrovanje poruka. Kada Bob primi šifrovanu poruku od Alise on će uz pomoć svog privatnog ključa (PK_{Bob}) i odgovarajućeg asimetričnog algoritma da dešifruje i pročita poruku. Alisa u svakom trenutku može da traži od Boba da se predstavi kako bi se uverila da se Trudi nije umešala u njihovu komunikaciju. Bob to radi na vrlo jednostavan način tako što šifrue poruku, npr. "*Ja sam Bob*", svojim privatnim ključem i šalje je Alisi. Alisa tu poruku može da dešifruje samo sa Bobovim javnim ključem čime se potvrđuje Bobov identitet. Trudi to takođe može da uradi ali ona sem činjenice koju već zna, da je Bob poslao tu poruku, ne može da dođe ni do kojeg drugog bitnog podatka vezanog za šifrovanu poruku ili ključa kojim je ona šifrovana.

Samo je mali broj asimetričnih algoritama istovremeno i siguran i praktičan. Od sigurnih i praktičnih algoritama s javnim ključem neki su pogodni samo za šifrovanje, dok su pojedini pogodni samo za digitalne potpise. Samo tri algoritma dobro funkcionišu i za šifrovanje i za digitalne potpise: *RSA*, *ElGamal* i *Rabin*. Svi ovi algoritmi su spori, oni šifruju i dešifruju podatke mnogo sporije nego simetrični algoritmi, a to je obično presporo da bi se obavljalo masovno šifrovanje podataka [37].

Osobine asimetričnih algoritama koje proizilaze iz jednostavnosti korišćenja, omogućile su niz funkcionalnosti koje se teško ili nikako koriste u simetričnim šifarskim sistemima. Autentifikacija, integritet, tajnost i neporecivost su četiri ključne usluge koja na jednom mestu obezbeđuje asimetrična kriptografija. Rad asimetričnih kriptografskih algoritama se zasniva na matematičkim jednosmernim funkcijama sa zamkom. Ove funkcije imaju specifičnu osobinu da se lako izračunavaju u jednom smeru, dok je inverzna operacija, odnosno izračunavanje u suprotnom smeru praktično neizvodljivo. Zamka koja se pominje se odnosi na osobinu koja omogućava onome ko poseduje javni i privatni ključ da dešifruje šifrovane poruke.

Faktorizacija proizvoda veoma velikih prostih brojeva je pravi primer za jednosmernu funkciju. Lako se izračunava proizvod dva velika prosta broja p i q , $N = p \times q$, međutim, veoma je teško iz proizvoda N izračunati faktore p i q ukoliko su oni nepoznati onome ko pokušava da ih izračuna. [52, 38].

3.1.3.1 RSA asimetrični algoritam

Već je napomenuto da se u asimetričnoj kriptografiji koriste dva ključa, javni i privatni ključ. RSA privatni ključ se generiše uz pomoć dva nasumično izabrana velika prosta broja, npr. za ključ od 2048 bita biraju se prosti brojevi od 1024 bita [53, 54]. Sigurnost RSA algoritma se zasniva na pretpostavci da je nemoguće izvršiti faktorizaciju proizvoda dva velika nasumično izabrana prosta broja na činioce. Radi se dakle o pretpostavci jer ne postoje matematički dokazi koji bi proces faktorizacije jednog tako velikog broja skratio i učinio bržim.

Za izračunavanje privatnog ključa se koristi modularna aritmetika. U literaturi parametri za izračunavanje ključeva se najčešće označavaju sa p i q . Preporuka je da se prosti brojevi za ova dva parametra izaberu tako da imaju određene osobine koje njihov proizvod, koji se inače označava sa n , čini teškim za faktorisanje. Zbog uprošćenog prikaza se najčešće biraju mali prosti brojevi s kojima se prikazuje postupak izračunavanja privatnog ključa [38, 55, 56, 57]. Važno je napomenuti da parametri p i q nikada ne smeju da budu razotkriveni i da je zbog toga dobra praksa da se oni unište nakon izračunavanja jer se sigurnost privatnog ključa zasniva na tajnosti ova dva parametra.

Proces izračunavanja se može prikazati na jednostavan način, uz činjenicu da se javni ključ obeležava sa e , a privatni ključ sa d . Prilikom izračunavanja privatnog ključa potrebno je izabrati javni ključ na taj način da bude zadovoljen uslov da su e i proizvod φ uzajamno prosti. Najmanji zajednički delilac brojeva e i φ obeležavamo sa gcd (engl. *greatest common divisor* – gcd). Uporedo sa teoretskim, biće prikazan i praktičan deo izračunavanja.

Za pokazni primer biramo da je $p = 11$, a $q = 47$.

$$n = p \times q$$

$$n = 11 \times 47 = 517$$

$$\varphi = (p - 1) \times (q - 1)$$

$$\varphi = (11 - 1) \times (47 - 1) = 460$$

$$e = 13$$

$$\gcd(e, \varphi) = 1$$

$$\gcd(13, 460) = 1$$

$$d = e^{-1} \bmod \varphi$$

$$d = 13^{-1} \bmod 460 = 177$$

Sada e i n mogu da se javno objave, d se čuva u tajnosti, a p i q se uništavaju.

Algoritmi za faktORIZACIJU se stalno unapređuju, međutim, ne tolikom brzinom da bi se moglo reći da je *RSA* ključ dužine od 2048 bita ugrožen. Ova dužina ključa je u velikoj meri još uvek u komercijalnoj upotrebi i po preporukama, koje je objavio *NIST* u 2019. godini [58], on zadovoljava minimalnu bezbednosnu snagu.

RSA algoritam je veoma spor jer se koriste veoma veliki brojevi što u znatnoj meri usporava proces šifrovanja i dešifrovanja. Ova činjenica u praksi znači da se sa *RSA* algoritmom neće šifrovati poruke koje sadrže mnogo teksta, već kratke poruke koje bi mogle da budu nosioci tajnih ključeva simetrične kriptografije. *RSA* algoritam je pogodan i za digitalno potpisivanje, čime se obezbeđuju servisi autentifikacije, integriteta i neporecivosti. Potrebno je napomenuti da se digitalno potpisivanje vrši sa privatnim ključem. Komercijalna upotreba *RSA* algoritma podrazumeva upotrebu infrastrukture javnih ključeva, što u celu priču uvodi i "treću stranu od poverenja".

3.1.3.2 Sertifikaciona tela

Složeni sistem uz pomoć koga se odvija sigurna komunikacija naziva se Infrastruktura javnih ključeva (*Public Key Infrastructure – PKI*). Osnova svakog *PKI* sistema je sertifikaciono telo (*Certification Authority – CA*). Sertifikaciono telo je najvažniji modul i osnova poverenja svakog *PKI* sistema [59].

PKI sistem je izgrađen kao kombinacija hardverskih i softverskih rešenja, kriptografskih algoritama i usluga koje u potpunosti omogućavaju državnim organizacijama, kompanijama i pojedincima da obezbede sigurnost svojih komunikacija i poslovnih transakcija. Ovakav sistem integriše digitalne sertifikate, kriptografiju javnog ključa i sertifikaciona tela u kompletnu mrežnu sigurnosnu arhitekturu koje obuhvata izdavanje digitalnih sertifikata pojedinim korisnicima [60].

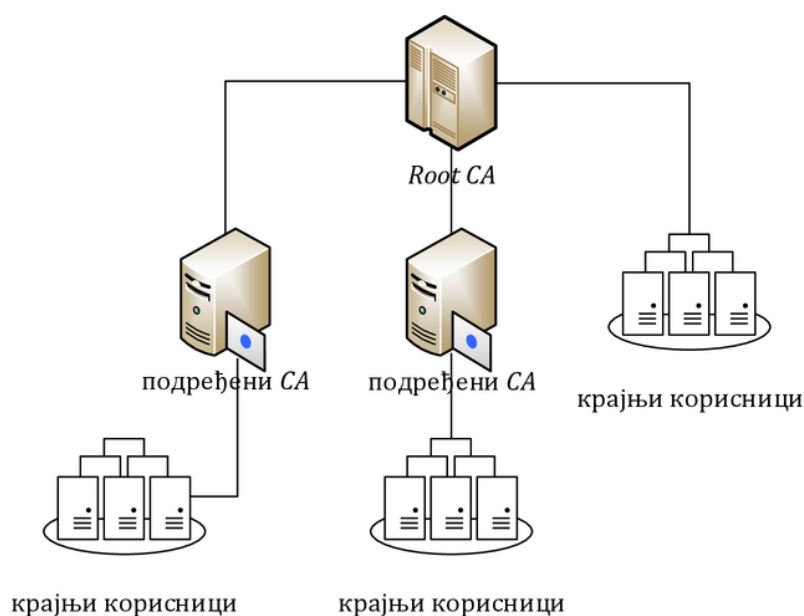
Sertifikaciono telo je neophodno u procesu izdavanja digitalnih sertifikata jer predstavlja instituciju od poverenja. Poverenje je osnova sigurnih komunikacija. Zapravo, svaka vrsta identifikacije, koja je prvi kriterijum sigurnih komunikacija, je zasnovana na poverenju. Ljude i predmete koje neposredno poznajemo identifikujemo direktno. Ljude i predmete koje ne poznajemo direktno identifikujemo preko nekog

1 drugog. Potpune strance u službenim kontaktima identifikujemo preko identifikacionih dokumenata. O 1 m dokumentima verujemo jer ih je izdala ustanova kojoj verujemo. Ista ta ustanova je izdala i naše identifikacione dokumente. Mi verujemo i identifikacionim dokumentima koje je izdala neka druga ustanova, a ne naša, na osnovu toga što je naša ustanova kojoj verujemo rekla da veruje toj drugoj ustanovi (npr. pasoši). Navedeni primeri predstavljaju modele poverenja 1. Postoji više formalnih podela modela poverenja u svetu digitalnih sertifikata ali bi se osnovna podela mogla napraviti na direktno i indirektno poverenje [61, 62].

Model direktnog poverenja odnosi se, pre svega, na to da digitalnom sertifikatu verujemo jer znamo kome pripada, odnosno na neki način smo se uverili 1 da digitalni sertifikat pripada svom navedenom vlasniku. Ovakav model poverenja nema veliku praktičnu primenu osim za uži krug ljudi koji se međusobno poznaju. Asimetrična kriptografija omogućava ljudima koji se ne poznaju sigurnu i poverljivu elektronsku komunikaciju. Ovakav vid komunikacije 1 implicira model indirektnog poverenja. Model indirektnog poverenja se deli u dve glavne grupe [61] koje zapravo predstavljaju modele poverenja koje ljudi koriste u privatnim i poslovnim kontaktima.

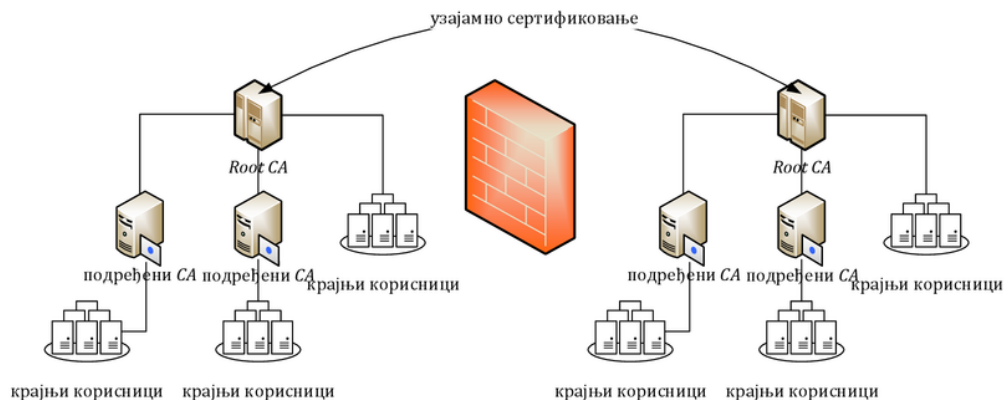
Kada komuniciraju međusobno ljudi često veruju u preporuke drugih ljudi koje vrlo dobro poznaju. Ako ovakav vid poverenja prenesemo na digitalnu sertifikaciju mogli bi smo da uspostavimo mrežu poverenja (*Web of Trust*). Međutim, u ovakvo uspostavljenoj mreži poverenja digitalne sertifikate ne potpisuje CA već korisnici ovakve mreže se uzajamno sertifikuju. Naravno, odmah se uočava i ograničenje u korišćenju ovakvog sistema jer nije primenljiv van okvira uskog kruga ljudi koji se međusobno poznaju i veruju jedni drugima. Za razliku od ovakvog modela, u poslovnim i njima sličnim komunikacijama, servisi državne elektronske uprave, korisnici se oslanjaju na neku organizaciju koja garantuje za identitet svojih članova.

1 Klasičan hijerarhijski model poverenja je zasnovan na jednoj vrhovnoj sertifikacionoj ustanovi (*Root CA*) od koje potiču svi sertifikati unutar jedne mreže poverenja, slika 3.9.



Slika 3.9. Hijerarhijski model poverenja

Root CA, kao vrhovno telo od poverenja, kome svi korisnici te mreže veruju, u najčešćem broju slučajeva izdaje sertifikate podređenim sertifikacionim ustanovama, koje dalje mogu da izdaju sertifikate ustanovama koje su podređene direktno njoj ili pak krajnjim korisnicima. Međutim, *Root CA* može takođe, što je zapravo ređi slučaj, da digitalne sertifikate izdaje direktno krajnjim korisnicima. Izdavanje sertifikata na ovaj način, unutar mreže poverenja za koju je nadležna *Root CA* predstavlja jedan lanac povezivanja u kome korisnici ovakve mreže od poverenja mogu da budu sigurni i identitet drugih korisnika iste te mreže. Jedni način da se korisnici ove mreže od poverenja povežu sa korisnicima druge mreže od poverenja je da se ostvari uzajamno sertifikovanje vrhovnih sertifikacionih tela (*cross-certification*), slika 3.10 [62].

Slika 3.10. Uzajamno sertifikovanje - *cross-certification*

Root CA po pravilu ne bi trebalo da bude povezan na mrežnu infrastrukturu – internet. Potrebno je da se nalazi u posebno zaštićenoj prostoriji koja je otporna i na elektro-magnetno zračenje i postoji niz strogih pravila po kojima radi. Sertifikaciono telo mora da podržava različite hardverske elemente kao što su "pametne" (*smart*) kartice, *HSM* moduli (*hardware security module*), *USB* tokeni, itd. Sertifikaciono telo, takođe, mora da podržava različite algoritme za simetrično i asimetrično šifrovanje, a neophodno je da podrži sledeće algoritme za digitalno potpisivanje: *RSA*, *DSA* i *ECDSA*.

Tehnički gledano sertifikaciono telo treba da obavlja sledeće zadatke:

- registraciju korisnika (može to da radi i registraciono telo),
- inicijalizaciju korisnika (može to da radi i registraciono telo),
- sertifikaciju korisnika,
- međusobno sertifikovanje,
- pothranjivanje ključeva,
- ažuriranje ključeva,
- opozivanje sertifikata i
- vođenje evidencije o opozvanim sertifikatima.

3.1.3.3. Princip rada sertifikacionog tela

CA najčešće predstavlja državnu instituciju ili kompaniju koje zaduženo za izdavanje digitalnih sertifikata krajnjim korisnicima. Što se tiče samih korisnika, *CA* predstavlja tzv. "treću stranu od poverenja" (engl. *Trusted Third Party – TTP*) kojoj svi korisnici veruju. *CA* poverenje gradi na principu piramide, na čijem se samom vrhu nalazi *Root CA*. Jedino *Root CA* može samom sebi da potpiše digitalni sertifikat i ono najčešće sertifikuje podređene *CA* (*Intermediate CA – ICA*) koja pod određenim uslovima izdaju i povlače digitalne sertifikate krajnjim korisnicima.

Prilikom izdavanja digitalnog sertifikata krajnjem korisniku *CA* mora da izvrši potpunu proveru podataka o krajnjem korisniku kako bi isti bili upisani u korisnikov digitalni sertifikat potpisan od strane *CA* čime se garantuje tačnost podataka. Sve postupke vezane za proveru i registraciju novih korisnika *CA* može da prepusti telu pod nazivom registracioni telo (engl. *Registration Authority – RA*). Izdati digitalni sertifikat garantuje da je javni ključ koji je zapisan u digitalnim sertifikatu i koji može biti javno objavljen u vlasništvu korisnika kome je digitalni sertifikat i izdat. Ovom se uspostavlja poverenje između krajnjih korisnika ove mreže od poverenja jer svi korisnici znaju da je garant *Root CA* [64].

Važna karika u lancu poverenja koje stvara jedno sertifikaciono telo i lista opozvanih sertifikata (*Certificate Revocation List – CRL*). Digitalnim sertifikatima izdatim od strane *CA* može da istekne rok važenja, da korisnik sam podnese zahtev za ukidanje digitalnog sertifikata, da dođe do kompromitacije privatnog ključa koji je zapisan u digitalnom sertifikatu i da zbog toga digitalni sertifikat mora da bude opozvan, itd. Svi ti razlozi dovode do toga da sertifikaciono telo mora da napravi jednu listu ili elektronski

repozitorijum koji će da sadrži listu svih opozvanih sertifikata i da je javno objavljuje kako bi bila dostupna svim učesnicima u njegovoj mreži poverenja.

Sertifikaciono telo najčešće javno objavljuje dokumente koji regulišu njegov rad i odnose se na razna pravila iz ⁸mena njegovog rada. Ti dokumenti se po pravili zovu Politika sertifikacije (engl. *Certificate Policy – CP*) i Praktična pravila rada sertifikacionog tela (*Certificate Practice Statement – CPS*).

PKI sa pripadajućim sistemima korisnicima obezbeđuje pouzdan servis za prenos informacija u distribuiranim sistemima time što obezbeđuje [65]:

- Autentifikaciju učesnika u komunikaciji.
- Integritet razmenjenih poruka.
- Neporecivost jer niko ne može da tvrdi da poruku nije poslao.
- Tajnost jer poruke mogu da se šifruju ključevima zapisanim na digitalnom sertifikatu.

Iako je dosta stvari regulisan prema strogim pravilima opšti standard koji se odnosi na podelu *PKI* sistema ne postoji.

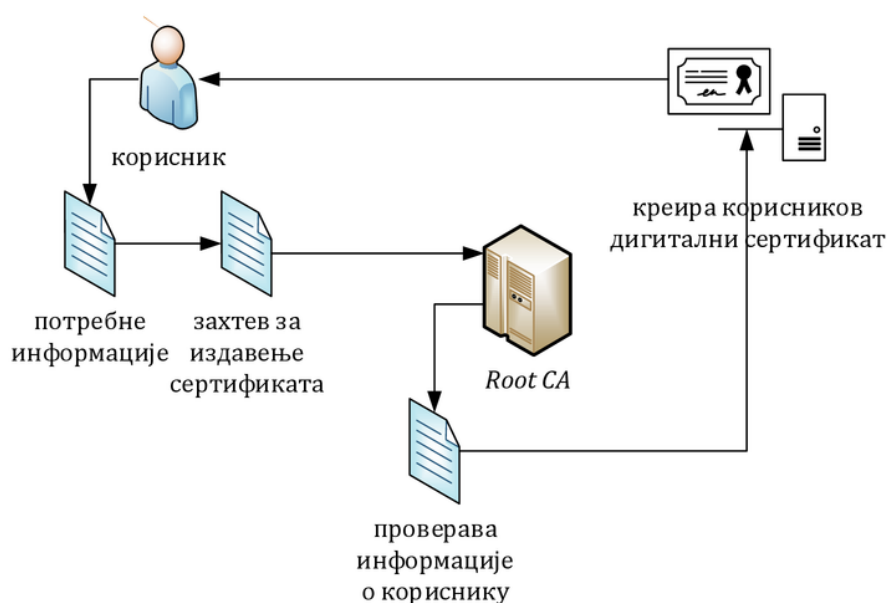
3.1.3.4. Digitalni sertifikat

¹⁰ Digitalni sertifikat je digitalno potpisan dokument koji povezuje javni ključ sa osobom kojoj taj ključ pripada (vlasnikom javnog ključa). Kao što svojim ličnim identifikacionim dokumentom dokazujemo svoj identitet na raznim mestima kao što su državna uprava, banke ⁷pošte, i tome sl., digitalnim sertifikatom dokazujemo svoj identitet na internetu. Sertifikat se digitalno potpisuje da bi se obezbedio njegov integritet. Integritet digitalnog sertifikata garantuje potpisnik, a potpisnik je u ovom slučaju *CA*.

⁵ Digitalni sertifikat najčešće sadrži:

- podatke o vlasniku sertifikata,
- javni ključ vlasnika sertifikata,
- period važenja sertifikata,
- ime izdavača (sertifikaciono telo koje je izdalo sertifikat),
- serijski broj sertifikata i
- digitalni potpis izdavača.

Dobijanje sertifikata od *CA*:



Slika 3.11. Šematski prikaz izdavanja digitalnog sertifikata

CA je ustanova koja skladišti informacije o identitetu fizičkih i pravnih lica. Korisniku koji počinje sa komunikacijom prvo zahteva od drugog učesnika da mu potvrdi svoj identitet. Njemu je dovoljno da proverí preko ustanove koja je izdala sertifikat da li je on još uvek validan i da li on zaista pripada onome s kim želi da komunicira. Iz digitalnog sertifikata lako može da preuzme javni ključ i da započne sa tajnom komunikacijom. [66].

Digitalni sertifikati prema nameni izdavanja se dele na: lične – za građane, poslovne – pravne subjekte i tela državne uprave. Prema nivoima sigurnosti svrstavaju se u 3 kategorije:

- Standardna – nivo koji je prikladan za rizike i posledice koji nemaju veću važnost. To može biti pristup tajnim podacima za koje verovatnoća zlonamernog pristupa nije velika. Za ovaj sigurnosni nivo se podrazumeva da je verovatnoća da korisnici budu zlonamerni mala.
- Srednja - ovaj nivo je prikladan za okoline u kojima su rizici i posledice kompromitovanja podataka umereni. Može se koristiti u transakcijama koje imaju znatnu novčanu vrednost ili rizik od falsifikovanja, ili u onima u koje je uključen pristup tajnim informacijama za koje je verovatnoća zlonamernog pristupa znatna.
- Visoka - nivo prikladan za upotrebu u transakcijama u kojima je ugroženost podataka visoka ili su posledice propusta u sistemu zaštite velike. To su transakcije vrlo visoke vrednosti ili sa velikim rizikom od falsifikovanja.

3.1.3.5. Struktura digitalnog sertifikata

Najzastupljeniji format sertifikata koji se koristi u *PKI* sistemima je *X.509*. Ovaj format definišu *ISO* i *ITU-T* [67]. *X.509* format podržavaju vodeći *PKI* -omogućeni protokoli i aplikacije kao što su *SSL*, *IPSec*, *S/MIME*, *Privacy Enhanced Mail (PEM)* i *SET*. Drugi format sertifikata koji nije standardizovan od strane zvaničnih institucija ali je dovoljno zastupljen da ga je neophodno spomenuti je *PGP* [68]. Ovaj format se koristi u vrlo raširenom softverskom paketu istog naziva *PGP (Pretty Good Privacy)*.

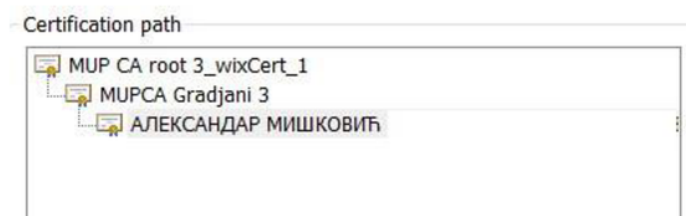
Field	Value	Field	Value
Version	V3	Public key	RSA (2048 Bits)
Serial number	0b 7c ad 5f 69 1d 72 bd	Basic Constraints	Subject Type=End Entity, P...
Signature algorithm	sha512RSA	Enhanced Key Usage	Secure Email (1.3.6.1.5.5...
Signature hash algorithm	sha512	Authority Key Identifier	KeyID=66 2d c5 52 9e 23 0...
Issuer	MUPCA Gradjani 3, MUPCA...	Subject Key Identifier	94 1d d7 e3 7f 78 01 fd 45 ...
Valid from	Thursday, November 26, 2...	CRL Distribution Points	[1]CRL Distribution Point: D...
Valid to	Thursday, November 26, 2...	Qualified Certificate Sta...	30 14 30 08 06 06 04 00 8...
Subject	АЛЕКСАНДАР МИШКОВИЋ...	Authority Information A...	[1]Authority Info Access: A...

Slika 3.12. *X.509* ver3 standardni sertifikat

Sertifikati izdati od strane *PKI* sistemima po formatu *X.509* definišu format i polja u kojima se upisuju informacije o izdatom sertifikatu, slika 3.12.

Polja od posebnog značaja su:

- Verzija: U ovom primeru se radi o sertifikatu verzije 3.
- Serijski broj sertifikata: *CA* izdaje jedinstveni serijski broj.
- Algoritam potpisivanja i kriptografska heš funkcija: Identifikacija digitalnog potpisa koji koristi *CA*.
- Izdavač: *CA* koje je izdalo digitalni sertifikat, zapisan po standardu *X.500*, koji definiše stablo ili strukturu direktorijuma čime se definiše lanac sertifikacije, slika 3.13.
- Period važenja: U ovim poljima je zapisan datum izdavanja i prestanka važenja digitalnog sertifikata.
- Ime korisnika: Ime i prezime korisnika kome je izdat digitalni sertifikat, takođe zapisan po standardu *X.500*.
- Javni ključ: U prikazanom primeru radi se o *RSA* ključu za digitalno potpisivanje.
- Proširenja: Ova polja sadrže dodatne informacije o *CA*, korisniku, ekstenzije koje sadrži digitalni sertifikat, listi opozvanih sertifikata itd.



Slika 3.13. Lanac sertifikacije

U svetu postoji veliki broj kompanija koje koriste *X.509 ver3* standardni sertifikat. Među njima su i svetski poznate *VISA* i *MasterCard*.

3.1.3.6. Izdavanje digitalnog sertifikata

Da bi sertifikaciono telo izdalo digitalni sertifikat korisniku moraju da se izvrše sledeće procedure:

- preuzimanje ličnih podatke od korisnika,
- preuzimanje javnog ključa korisnika ili generisanje istog od strane *CA* (češći slučaj),
- formatiranje preuzetih podataka na standardan način (npr. *X.509 ver3* format),
- digitalno potpisivanje formatiranih podataka.

CA javni ključ može da dobije od samog korisnika i da ga sertifikuje ili da generiše par asimetričnih ključeva (javni i privatni ključ) za svakog korisnika pa da ih distribuira zajedno sa sertifikatom. Ukoliko korisnik sam generiše par asimetričnih ključeva može da zahteva od *CA*, samo u određenim slučajevima koji se mogu retko sresti u praktičnoj promeni, da mu izda digitalni sertifikat koji sadrži njegov javni ključ. Ovaj metod je dobar sa stanovišta bezbednosti korisnika jer se privatni ključ uvek čuva samo na jednoj lokaciji tj. kod samog korisnika. Međutim, pomenuti razlozi mogu se opravdati samo sa stanovišta korisnika. Sa stanovišta *CA* sigurnije je da samo *CA* bude nadležno za generisanje parova asimetričnih ključeva jer se jedino na taj način može kontrolisati i održati kvalitet generisanih ključeva kao i sprovođenje procedura za bezbedno čuvanje istih.

Korisnik se obraća *CA* zahtevom za izdavanje sertifikata (engl. *certification request*). Kako se sve u vezi *PKI* sistema radi po odgovarajućim standardima i procedurama, tako postoji i standard koji propisuje kako će korisnik da podnese zahtev za izdavanje sertifikata. Najčešće korišćeni standard za podnošenje zahteva nosi oznaku *PKCS#10*.

Prvi korak u procesu prijavljivanja je registracija pri kojoj se proverava identitet krajnjeg korisnika koji podnosi zahtev za sertifikatom. Nivo provere identiteta zavisi od tipa sertifikata za koji se podnosi zahtev. Za svaki tip sertifikata definisan je odgovarajući dokument koji se naziva politika sertifikacije. Inicijalizacija je sledeći

korak u registraciji u okviru koga krajnji korisnik i sertifikaciono telo razmenjuju neophodne informacije za dalju komunikaciju [64]:

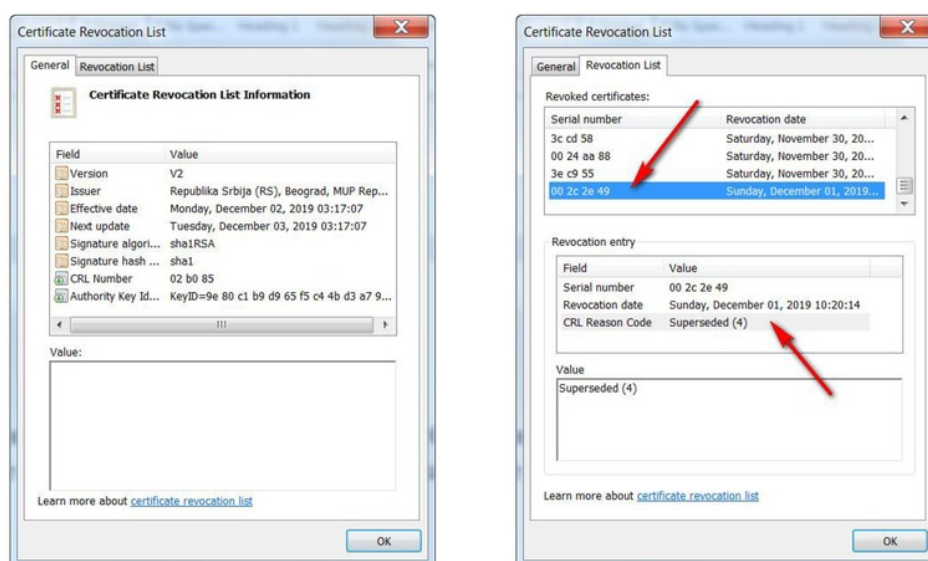
- kako će se odvijati sama komunikacija,
- kako će se distribuirati sertifikati,
- na koji način se uspostavlja sigurna komunikacija između krajnjih korisnika i sertifikacionog tela,
- kako se generiše i dostavlja par asimetričnih ključeva itd.

3.1.3.7. Lista opozvanih sertifikata

Kao što je već napomenuto, digitalni sertifikat ima datum izdavanja i datum kada istom ističe validnost. Koliko dugo će jedan sertifikat da važi zavisi od unutrašnje politike koju CA sprovodi prema odgovarajućim, unapred propisanim, pravilima. Već je napomenuto da postoje različite situacije kada digitalnom sertifikatu prestaje upotreba. CA je dužan da sve opozvane sertifikate čuva i javno objavljuje u vidu CRL preko odgovarajućeg digitalnog repozitorijuma. CRL mora da bude digitalno potpisana od strane CA koje je dužno da je redovno ažurira i objavljuje. Način na koji to CA radi i u kojim vremenskim okvirima nije na precizan način standardizovano i zavisi isključivo od unutrašnje politike koju sprovodi CA. Nizom pravila [69] definisan je način izdavanja CRL, odgovarajući upravljački protokol i niz operacionih protokola (HTTP, LDAP,...) za dostavljanje CRL do klijenata. [66].

Proveru digitalnih sertifikata, a samim tim i javnih ključeva, korisnici PKI sistema rade preko CA tela ili preko nekog drugog tela koje je autorizovano od strane CA tela. CRL omogućuje entitetima koji komuniciraju u datom PKI sistemu proveru validnosti digitalnih sertifikata druge strane u komunikaciji [70].

PKI sistemi koji koriste X.509 ver3 sertifikat, CRL svojim korisnicima dostavlja najčešće korišćenjem LDAP (Lightweight Directory Access Protocol – LDAP) protokola. slika 3.14. Takođe su zastupljeni metodi slanja CRL od strane CA tela ili povlačenja CRL od strane korisnika sa repozitorijuma na kome se ona objavljuje. CRL je koji korisnicima omogućava da vide niz podataka, a među bitnije se ubrajaju datumi objavljivanja CRL i datum objavljivanja nove CRL, slika 3.14.



Slika 3.14. Prikaz CRL liste

Postoje i razni drugi načini za proveru opozvanih sertifikata, a koji će da se koristi najviše zavisi od propisa i pravila kojima se definiše rad jednog *PKI* sistema. Poznati su protokoli koji korisnicima mogu u realnom vremenu da da ju odgovor da li je digitalni sertifikat povučen ili ne. Jedan od takvih protokola je *OCSP (Online Certificate Status Protocol)* protokol koji koristi dve metode za dobijanje informacije o validnosti digitalnog sertifikata. *OCSP* server takođe periodično preuzima ili prima informacije od *CA* tela o validnosti digitalnih sertifikata koji se dalje korisnicima prosleđuje u realnom vremenu [71]. Načini na koji ovaj protokol može biti implementiran u *PKI* sistem je definisan i odobren od strane *IESG (Internet Engineering Steering Group – IESG)*[72].

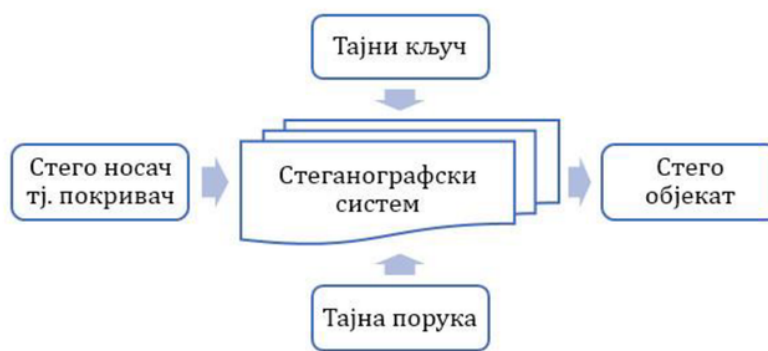
3.2. Steganografija

Istorijski gledano steganografija i kriptografija imaju istu vremensku liniju. Postoje istorijski zapisi u kojima je navedeno da se steganografija koristila od davnina, oko 500. godine pre nove ere. Kako što je to slučaj kod kriptografije i steganografija se koristila u gotovo svim ratnim sukobima kroz istoriju. Njena primene nije bila ograničena samo na vojnu upotrebu u ratnim sukobima, već se može reći da se steganografija koristila tamo gde se slanje šifrovanih poruka zabranjeno i kažnjivo. Mnogo je takvih primera i danas u svetu, tako da se steganografija i dalje koristi. Na žalost, svrha skrivanja poruka nema uvek plemenitu misiju, kao što je to npr. borba protiv ugnjetavanja i tiranije.

Razvoj moderne steganografije se, kao i kod kriptografije, poklapa sa razvojem računara. Moderna steganografija se danas koristi ne samo za skrivanje informacija od

potencijalnih napadača, već je svoju primenu našla i u oblastim zaštite intelektualne svojine, marketinškim aktivnostima koje se posebno oslanjaju na korišćenje multimedije (npr. plasiranje reklama putem video prenosa nekog važnog događaja, sportske manifestacije, i tome sl.). Sa rastom popularnosti i upotrebe moderne steganografije razvijaju se i tehnike stegoanalize, čiji je cilj da skrivanje informacija otkriju.

Steganografija se suštinski razlikuje od kriptografije iako se obe nauke koriste kako bi se sačuvala tajnost podataka. Međutim, za steganografiju se može reći da je to nauka o "nevidljivoj" komunikaciji, slika 3.15. U odnosu na kriptografiju čiji je cilj da tajna komunikacija ostane bezbedna čak i ako je otkrivena, steganografija ima za cilj da sakrije samo prisustvo tajne komunikacije od potencijalnih napadača ili posmatrača uopšte [73].



Slika 3.15. Model steganografskog sistema

Koncept steganografije, tj. skrivanja tajne poruke, se može opisati pomoću tzv. pojma "problem zatvorenika", kojim je opisana tajna komunikacija uz posredovanje "treće strane" koja je za taj vid komunikacije veoma zainteresovana [74]. Tajnost poruke koja je utisnuta u stego nosač se obezbeđuje tajnim ključem koji se koristi u određenom steganografskom algoritmu. Kada krajnji korisnik preuzme stego objekat, isti se raspakuje uz pomoć prethodno definisanog tajnog ključa i steganografskog algoritma. Na taj način, krajnji korisnik dolazi do tajne poruke. Postoje tri vrste steganografskih sistema:

- Steganografski sistemi koji ne koriste tajne ključeve ili lozinke.
- Steganografski sistemi koji koriste tajni ključ za zaštitu.
- Steganografski sistemi koji koriste javni ključ za zaštitu.

Steganografske tehnike koje se danas koriste moraju da zadovolje određene kriterijume kako bi tajna poruka zaista bila skrivena u nekom stego objektu. Pre svega se mora voditi računa o kapacitetu koji stego nosač, odnosno pokrivač, poseduje. Jednostavno rečeno, postoji mogućnost da u stego nosač umetnete poruku veoma velike dužine ali će takav postupak znatno izmeniti izgled originalnog fajla koji biti uočljiv i vizuelnim pregledanjem istog. Tehnike koje se koriste u steganografiji su brojne,

međutim, postoji nekoliko koje se svojom popularnošću, brzinom transformacije, robusnošću i tome sl. izdvajaju od ostalih. Nijedna od ovih tehnika ne garantuje potpunu bezbednost, tj. funkcionalnu metodu koja će utisnuti tajnu informaciju tako da ona sa sigurnošću bude "nevidljiva" brojnim alatima koji su razvijeni za stegoanalizu. S obzirom na iznete činjenice mogu se izdvojiti sledeće steganografske tehnike[75]:

- Najmanje značajan bit (engl. *Least Significant Bit – LSB*). Tehnika menja najmanje značajne bitove u stego nosaču sa bitovima tajne poruke, slika 3.16. Najčešće se koristi za menjanje digitalnih slika. Međutim ovaj metod ne pruža visok nivo sigurnosti jer se menjaju statistička svojstva korišćenih datoteka za stego nosače.

```

01011101  11010000  00011100  10101100
11100111  10000111  01101011  11100011

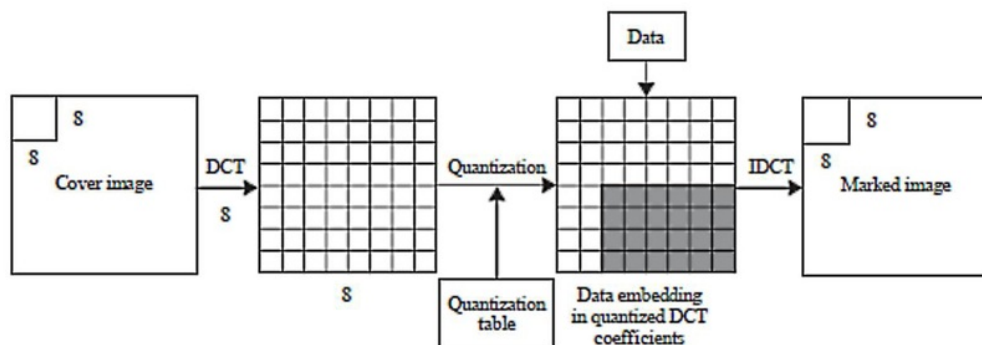
A -> ASCII => 65 => 01000001

01011100  11010001  00011100  10101100
11100110  10000110  01101010  11100011

```

Slika 3.16. Umetanje slova "A" u 8 bajtova stego nosača

- Diskretna kosinusna transformacija (engl. *Discrete Cosine Transformation – DCT*). *DCT* koeficijenti se koriste za kompresiju koja se bazira na Furijeovoj transformaciji, tj. na diskretnoj Furijeovoj transformaciji, transformišući ih iz prostornog domena u frekventni domen. *DCT* može da razdvoji sliku na komponente visoke, srednje i niske frekvencije [76]. Najčešće se koristi za umetanje tajne poruke u *JPEG* slike, slika 3.17 [77].



Slika 3.17. *DCT* pomoću *JPEG* modela kompresije pomoću bloka veličine 8 x 8 piksela

Kao što je već napomenuto iako je upotreba steganografije, kao i kriptografije, potpuno legalna i legitimno je pravo svakog pojedinca da te tehnike koristi, postoje određene situacije kada su ove tehnike bile i zloupotrebljavane u cilju izvršavanja terorističkih i dugih vrsta napada na objekte i ljude. Kao rezultat toga, potreba za otkrivanjem steganografskih podataka postala je važno pitanje za agencije koje su

zadužene za bezbednost u okviru svojih država. Pokušaj da se otkrije upotreba steganografije naziva se steganalizom gde se otkriva prisustvo skrivenih podataka. Zbog ogromnog broja tehnika skrivanja podata upotrebom steganografije, otkrivanje svih skrivenih podataka je veoma težak zadatak. Detektovanje skrivenih podatak u nekoj multimedijalnoj datoteci može biti veoma dug proces, koji neće uspeti da u vremenskom intervalu važnog za bezbednost otkrije skrivenu poruku.

Uprkos svemu, može se reći da steganografija ima više nego korisnu ulogu u današnjem društvu koje je usmereno na korišćenje multimedijalnih izvora podataka (televizija, radio, internet, ...). Shodno tome, najznačajnija i najčešća upotreba steganografije je upotreba digitalnih vodenih pečata kojima se štite autorska prava[38].

4. Pregled postojećih rešenja

Kriptografija u oblasti zaštite podataka ima veoma dugu istoriju korišćenja. Opšte je poznato da je kriptografija dominantno vojna tehnologija koja se s razvojem interneta, pre svega, a u novije vreme i pametnih telefona svoju primenu proširila na poslovne ali i servise javne uprave. Kriptografiju više ne koriste samo određene državne strukture, obaveštajne pre svega, već je ona postala lako dostupna za korišćenje i običnim ljudima, tj. pojedincima koji imaju potrebu da primene jedan od servisa koje kriptografija nudi.

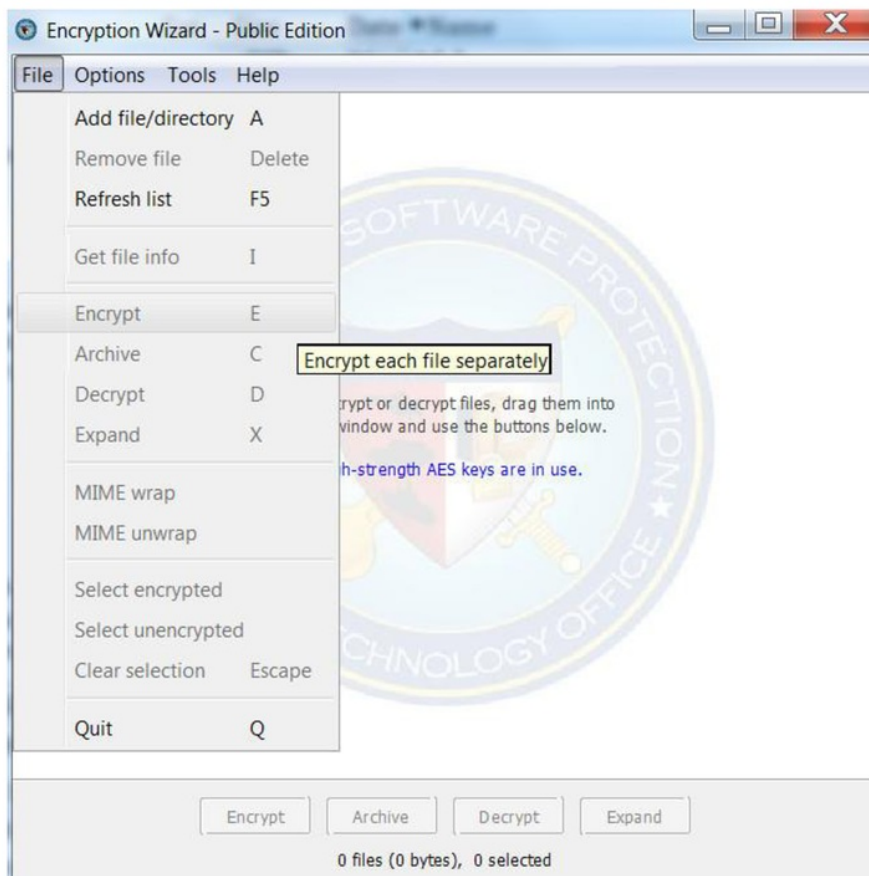
Steganografija, koja takođe ima dugačku istoriju kao i kriptografija, se takođe koristi kako bi se ostvarila zaštita informacija. Međutim, sam koncept zaštite koje se koristi u steganografiji se razlikuje od principa na kojima funkcioniše kriptografija. Dok se u kriptografiji teži ka ostvarivanju servisa tajnosti podataka, steganografija ima za cilj da postojanje informacije o nečemu sakrije na određeni način od oka posmatrača. Jedan od napada na komunikacione kanale kojim se razmenjuju tajne poruke ili informacije uopšte, a koji se odnosi na prekidanje komunikacionog kanala ili onemogućavanje korisnika da razmenjuju informacije, steganografija uspešno rešava.

Uporedo sa razvojem kriptografije, razvijala se i steganografija. To je dovelo do spajanja kriptografskih metoda sa metodama steganografije u višenamenske sisteme za tajnu komunikaciju. Cilj kreiranja ovakvih sistema je više nego očigledan jer postoji potreba ka servisu koji bi mogao da obezbedi tajnost, integritet i autentifikaciju i koji pri tom ne oдаje nikakve informacije o tome da su se pobrojani servisi uopšte i koristili. Najčešće se u ovakvim hibridnim rešenjima koriste servisi simetrične kriptografije kojima se obezbeđuje tajnost, dok se nekom od steganografskih metoda vrši utiskivanje tajne poruke ili informacije u stego nosač. Stego nosači u današnje vreme su najčešće multimedijalne datoteke ili datoteke koje se lako prenose i dele preko javnog komunikacionog kanala kao što je to internet. Od svih multimedijalnih datoteka najviše se primenjuju digitalne fotografije koje se kodiranjem transformišu na takav način da vizuelno ne izgledaju drugačije od originala. Međutim, kao što postoje tehnike za kriptanalizu, postoje i tehnike kojima se vrši stegoanaliza, tj. detekcija anomalija u stego nosaču.

U ovom poglavlju će biti opisani samo neki od brojnih alata koji pružaju servise iz domena oblasti istraživanja ove doktorske disertacije. Odabrani alati su se koristili kako bi se izvršila validacija predloženog protokola za razmenu kriptografskih ključeva na bazi ličnih identifikacionih dokumenata.

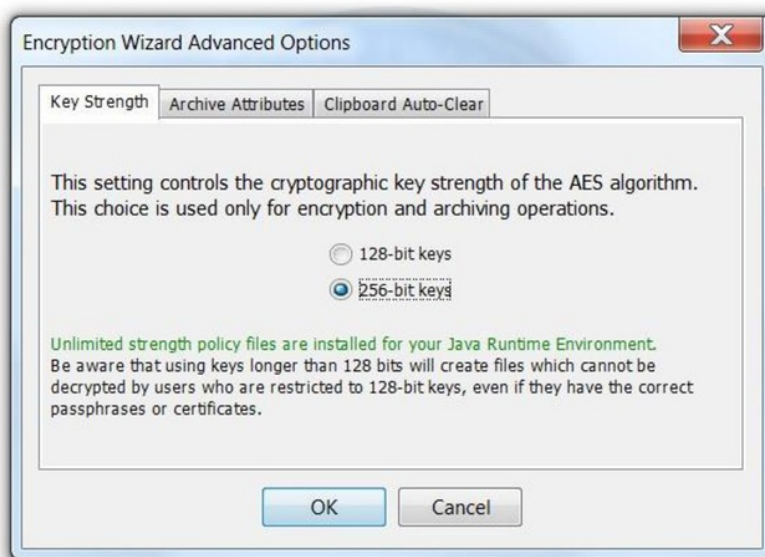
4.1. Encryption Wizard

Encryption Wizard kao i ostale alate koji su razvijeni od strane AFRL (engl. *Air Force Research Laboratory*), koji je deo Ministarstva odbrane SAD (engl. *Department of Defence – DoD*), bi trebalo da koriste američko Ministarstvo odbrane i ostatak savezne vlade, međutim, ponuđena je i javna verzije ovog softvera zajednici otvorenog koda (u ograničenoj verziji), slika 4.1.



Slika 4.1. Izgled *Encryption Wizard* aplikacije

Encryption Wizard je alat koje je razvijen korišćenjem Java programskog jezika za jednostavno, lako i brzo šifrovanje fajlova (datoteka) i programskih fascikli (foldera) u celini. Java programski jezik je korišćen kako bi se razvila multiplatformska aplikacija koja može da radi na gotovo svim poznatim operativnim sistemima. Program se uz minimalno predznanje kriptografskih pojmova veoma lako koristi. Na vrlo jednostavan način korisnici ovog programa mogu da izaberu željene dužine, 128 ili 256 bita, AES ključa, slika 4.2.



Slika 4.2. Odabir dužine AES ključa u *Encryption Wizard* aplikaciji

Ukoliko korisnik želi da koristi servis autentifikacije u okviru aplikacije može da generiše sopstveni digitalni sertifikat, slika 4.3.



Slika 4.3. Odabir parametara za formiranje digitalnog sertifikata

Ponudene su različite opcije za izbor dužine *RSA* ključa i *SHA* heš funkcije. Na slici su odabrani isti parametri koji se nalaze na kvalifikovanom digitalnom sertifikatu izdatom od strane *MUPCA*, koji se koristi u sistemu za tajnu komunikaciju opisanom u poglavlju 5.

Encryption Wizard alat može da se upotrebi za jedan od dva predložena načina za korišćenje predloženog rešenja za tajnu komunikaciju, koji su opisani u poglavlju 5 ove doktorske disertacije.

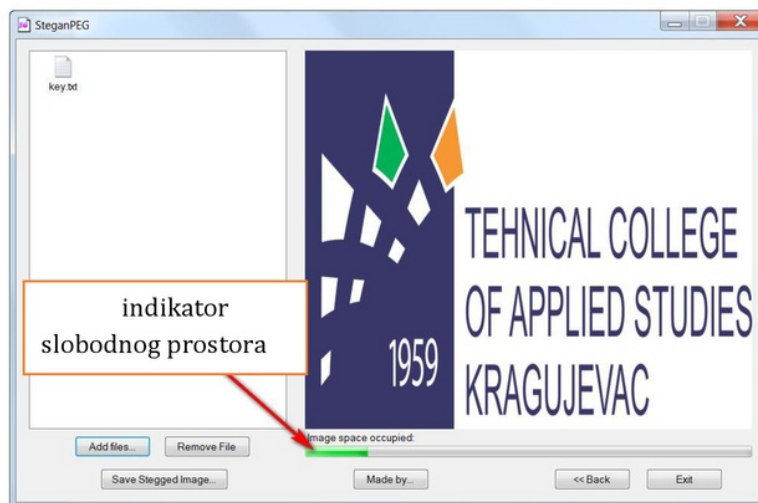


Slika 4.4. Verzija *Encryption Wizard* aplikacije

Verzija softvera koji je korišćen tokom istraživanja sprovedenih u okviru ove doktorske disertacije prikazana je na slici 4.4.

4.2. SteganPEG

SteganPEG je aplikacija koja koristi diskretnu kosinusnu transformaciju (*DCT*) za sakrivanje odabrane datoteke u *JPEG* sliku bez bitnije promene same u *JPEG* slike, slika 4.5.

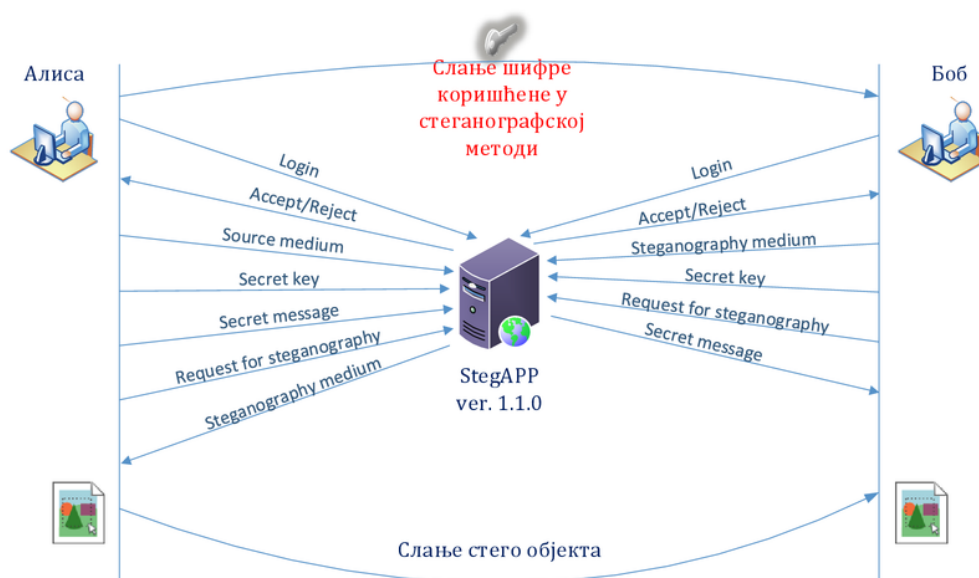


Slika 4.5. Izgled *SteganPEG* aplikacije nakon postavljenih ulaznih datoteka

Softver je jednostavan za upotrebu i ne zahteva od korisnika nikakvo predznanje vezano za kriptografiju. Podržava rad samo sa u *JPEG* slikama i softver može da sakrije više datoteka u jednoj *JPEG* slici. Postoji indikator koji označava koliko je još prostora preostalo za utiskivanje u odabranoj *JPEG* slici. Zaštita se svodi na jednostavno ukucavanje lozinke i ovaj softver je pogodan samo za skrivanje manje bitnih datoteka. Autor je dao izvorni kod tako da svako može slobodno da nastavi razvoj ovog softvera i da ga prilagodi svojim potrebama.

4.3. StegApp tool

StegApp tool je kreiran kao jedna Veb aplikacija koja se zasniva na zaštiti tajne poruke skrivanjem u slikama formata *JPEG*, *PNG*, *BMP*, *GIF* i *TIF*. Autor je predstavio svoj program u istaknutom naučnom međunarodnom časopisu (po kategorizaciju KoBSON-a) [35]. Aplikacija radi na principu *DCT* i zahteva prethodnu prijavu na Veb stranici aplikacije putem email-a. Nakon dobijanja autorizacije od administratora sajta korisnik može da vrši skrivanje tajne poruke koja je zapisana u *.txt* formatu. Princip rada same aplikacije je prikazan na slici 4.6.



Slika 4.6. Šematski prikaz tajne komunikacije pomoću *StegApp* aplikacije

Koraci koje Alisa preduzima da bi poslala tajnu poruku su:

1. Prijavljivanje na *StegApp* Veb aplikaciju;
2. Dodavanje datoteke koja će biti stego nosač na server Veb aplikacije;
3. Upisivanje tajne lozinke (šifre) koja se koristi u *StegApp* aplikaciji pri zaštiti stego nosača;

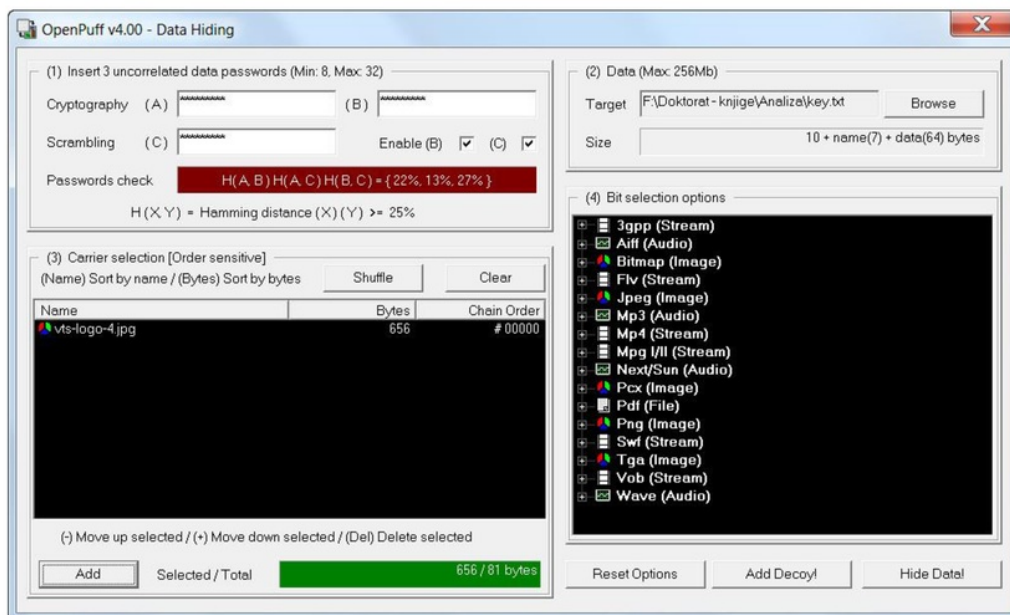
4. Dodavanje tekstualne poruke koja će biti utisnuta u stego nosač;
5. Preuzimanje stego nosača sa *StegApp* Veb stranice na svoj računar;
6. Slanje stego nosača (stego objekat) putem interneta Bobu.

Koraci koje Bob preduzima da bi pročitao tajnu poruku su:

1. Preuzimanje stego nosača (stego objekat) od Alise;
2. Prijavljivanje na *StegApp* Veb aplikaciju;
3. Dodavanje stego nosača na server Veb aplikacije;
4. Upisivanje tajne lozinke (šifre) radi otkrivanja tekstualne poruke;
5. Preuzimanje tekstualne poruke sa *StegApp* Veb stranice na svoj računar.

4.4. OpenPuff

OpenPuff je veoma moćan i sveobuhvatan alat koji je publikovan pod licencom otvorenog koda. Ovaj alat obuhvata veliki broj digitalnih datoteka koje je moguće koristiti kao stego nosač. Moguće je kombinovati više digitalnih datoteka kako bi se utisnula veoma velika datoteka slika 4.7.



Slika 4.7. Korišćenje steganografije u *OpenPuff* aplikaciji

Inicijalnim pokretanjem nudi se odabir načina korišćenja *OpenPuff* aplikacije. Postoje tri izbora, a u skladu sa predmetom istraživanja u ovoj doktorskoj disertaciji je korišćen deo softvera namenjen za steganografiju.

Program dozvoljava korišćenje tri lozinke, minimalne i maksimalne vrednosti za iste se kreću od 8 do 32 karaktera, ali korisnik može da izabere da koristi samo jednu lozinku. Maksimalna veličina datoteke koja može biti utisnuta zavisi od veličine stego nosača ali je ona projektovana tako da ne može da pređe granicu od 256 MB. *OpenPuff* je jedina aplikacija koja kombinuje simetričnu kriptografiju sa steganografskom tehnikom koja se koristi adaptivnim nelinearnim kodiranjem bitova stego nosača.

4.5. Sertifikaciono telo MUP-a Republike Srbije

Sertifikaciono telo *MUPCA* izgradilo je infrastrukturu javnih ključeva na bazi implementacije rešenja koje je projektovala kompanija *NetSeT*. *MUPCA* izdaje kvalifikovane digitalne sertifikate građanima Republike Srbije na ličnim identifikacionim dokumentima sa čipom. Standardi kojih se pridržava *MUPCA* prilikom izdavanja kvalifikovanih digitalnih sertifikata su¹:

- **9** *ETSI ESI TS 101 862 „Qualified Certificate Profile”,*
- *RFC 3739 „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile”,*
- *RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”,*
- *ETSI TS 102 280 „X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons”*

9 *MUPCA* izdaje sertifikate u formatu *X.509v3*. Kriptografski parametri, tj. asimetrični parovi ključeva se generišu pomoću hardverskih generatora slučajnih brojeva koji su realizovani na kriptografskim hardverskim uređajima tzv. *HSM* (engl. *hardware security module*) modul. Sopstveni sertifikat *MUPCA* potpisuje *RSA* ključem dužine 4096 bita, dok se građanima Republike Srbije izdaju kvalifikovani digitalni sertifikati koji u sebi sadrže dva para *RSA* ključeva od 2048 bita.

Detaljni propisi koji propisuju rad *MUPCA*, Politika sertifikacije i Praktična pravila rada sertifikacionog tela, su dostupni na Veb stranici sertifikacionog tela *MUPCA*.

¹ Dostupno na: <http://ca.mup.gov.rs/>

5. Model predloženog rešenja

Do danas je razvijen veliki broj kompletnih servisa kojima se štiti privatnost i koji garantuju visok stepen zaštite razmenjenih informacija. Postoji više poznatih načina za razmenu tajnih ključeva putem nesigurnog komunikacionog kanala.

Nov pristup koji će biti predstavljen u ovoj disertaciji unapređuje sigurnost protokola za razmenu tajnih kriptografskih ključeva tako što se dodaje još jedan sigurnosni korak u tajnoj komunikaciji korisnika. Steganografija, koja se koristi u predloženom sistemu, treba da sakrije od potencijalnog napadača informaciju da je do bilo kakve komunikacije između dva korisnika došlo. Potencijalni napadač pored stegoanalize, kako bi utvrdio da nekakva tajna komunikacija postoji, mora da izvrši i kriptooanalizu kako bi došao do otvorenog teksta poslate poruke koja u sebi sadrži tajni ključ. Primenom predloženog sistema se pored prikrivene komunikacije uz pomoć steganografije, vrši i bezbedna distribucija tajnih ključeva korišćenih za šifrovanje poruke ali i autentifikacija korisnika, respektivno.

Bezbedna distribucija tajnih ključeva i autentifikacija korisnika se vrši pomoću asimetrične kriptografije, korišćenjem kvalifikovanih digitalnih sertifikata koji se nalaze na ličnim identifikacionim dokumentima građana Republike Srbije. Predloženim unapređenjem korisnici dobijaju kompletan sistem za tajnu komunikaciju koji se, kao takav, po prvi put koristi.

5.1. Opis problema

Prisluškivanje komunikacionih kanala, pogotovo interneta, više ne predstavlja nepoznat pojam i u današnje vreme je to postala javno poznata činjenica o kojoj se u više navrata pisalo i govorilo u javnosti.

Aktuelni slučajevi poput portala "Wikileaks"¹ (engl. *WikiLeaks*), za koji se smatra da ga je osnivao Julijan Asanž (engl. *Julian Assange*), a pogotovo polemika koju je izazvao Edvard Snouden (engl. *Edward Snowden*) iznošenjem činjenica o postojanju velikog broja tajnih projekata nadziranja od strane SAD² (*United States of America*) su dovoljni

¹ Nefitna međunarodna organizacija preko koje su uzbunjivači širom sveta objavljivali, i još uvek objavljuju, tajna dokumenta i materijale koji su na drugi način nedostupni široj svetskoj javnosti. Na portalu *WikiLeaks* mogu se pronaći i dokumenta i tajne depeše vezano za našu zemlju.

² Glenn Greenwald, novinar britanskog dnevnog lista *The Guardian*, prvi je objavio niz članaka, prema tvrdnjama i dokumentima koje mu je prezentovao Edvard Snouden, da su SAD pokrenule i koristile niz tajnih projekata za nadzor gotovo čitavog interneta ali i drugih svetskih institucija

razlozi da se tvrdi kako slobodna komunikacija u svetu, bez nečijeg nadzora, ne postoji. Ukoliko je važno da komunikacija bude tajna, makar se to odnosilo i za neki kraći period, upotrebiće se neki od servisa koji to mogu obezbediti. Svaki od tih servisa podrazumeva upotrebu kriptografije.

Verovatnoća da neko nadzire i prisluškuje komunikacioni kanal je velika, a razmena šifrovanih informacija može da skrene pažnju na iste. Nakon otkrivanja šifrovane komunikacije i presretanja šifrovanih poruka, postoji verovatnoća da će neko pokušati da izvrši kriptanalizu istih. U svrhu smanjivanja verovatnoće otkrivanja šifrovane komunikacije najčešće se koristi neka od opšte poznatih steganografskih metoda. Upotrebom steganografije potencijalnim napadačima se znatno otežava proces razotkrivanja tajne komunikacije jer se poruka koja sadrži informaciju utiskuje u stego objekat čime se originalna datoteka, tj. stego nosač, tek neznatno menja.

S obzirom na činjenicu da se u današnje vreme razmenjuje velika količina multimedijalnog sadržaja putem raznih društvenih mreža, servisa za razmenu fotografija i video fajlova, internet foruma, i tome sl., potencijalni napadač koji prisluškuje komunikacioni kanal mora da prikupi sav razmenjeni multimedijalni sadržaj i da izvrši stegoanalizu svih datoteka kako bi eventualno otkrio tajnu komunikaciju između dva korisnika.

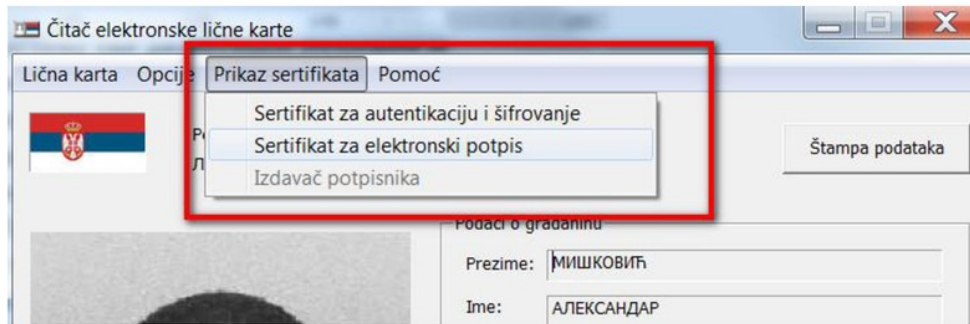
S druge strane, razvojem i unapređivanjem informacionih sistema postali smo svedoci primene elektronskih dokumenata u državnoj administraciji, bankarstvu, pravosuđu i ostalim sferama društva, a komuniciranje u otvorenim mrežama bez direktnog ličnog kontakta je postala svakodnevica. Ovo su samo neki od primera primene savremenih komunikacionih tehnologija koji zahtevaju nove oblike utvrđivanja identiteta i zaštite podataka. Zaštita poverljivih informacija veoma se uspešno sprovodi uz pomoć simetričnih šifarskih sistema, dok se za utvrđivanje autentičnosti i integriteta najčešće koriste asimetrični šifarski sistemi. Ovi servisi će biti osnov za korišćenje predloženog sistema za tajnu komunikaciju, dok će se korišćenjem steganografije prikrivati da je do tajne komunikacije uopšte i došlo čime se otežava proces razotkrivanja tajne komunikacije, a samim tim umanjuje se i verovatnoća da će doći do kriptanalize šifrovanih informacija.

5.2. Predloženo rešenje i njegova primena

Jedan od najvećih problema koji se javlja prilikom uspostavljanja tajne komunikacije je sigurna razmena kriptografskih ključeva. Problem koji nastaje kada korisnici treba da razmene tajni ključ putem javnog komunikacionog kanala kao što je to npr. internet, u predloženom sistemu ove disertacije razrešen je upotrebom

i organizacija. Objavljeni su kodni nazivi tajnih projekata zapisanih u preko 9000 tajnih dokumenata. Pored američke agencije NSA, u objavljenim dokumentima se pominju se i britanske, nemačke i izraelske tajne službe.

asimetrične kriptografije. Naime, korišćenjem Java programskog jezika, razvijen je metod koji pristupa kvalifikovanim digitalnim sertifikatima koji se nalaze na ličnim identifikacionim dokumentima sa čipom građana Republike Srbije. Kvalifikovani digitalni sertifikati koji se koriste u predloženom sistemu sadrže dva para *RSA* ključeva veličine 2048 bita, slika 5.1, jedan za šifrovanje i autentifikaciju, a drugi za digitalno potpisivanje. Kvalifikovane digitalne sertifikate građanima republike Srbije besplatno izdaje sertifikaciono telo *MUPCA*³.



Slika 5.1. Očitavanje kvalifikovanih digitalnih sertifikata koji se nalaze na ličnom identifikacionom dokumentu

Predloženi sistem za tajnu komunikaciju svoju sigurnost zasniva na šifrovanju tajnog ključa, koji se koristi u simetričnoj kriptografiji, sa *RSA* javnim ključem za šifrovanje koji se nalazi na kvalifikovanom digitalnom sertifikatu. Pre operacije šifrovanja dokument, koji sadrži tajni ključ, se digitalno potpisuje čime se vrši autentifikacija korisnika predloženog sistema za tajnu komunikaciju, a samim tim se potvrđuje i integritet razmenjenih poruka kojima se distribuiraju tajni ključevi. Utiskivanjem ove šifrovane i digitalno potpisane poruke u stego objekat, koji se kasnije postavlja na neki od servisa javne komunikacije, se prikriva da je do razmene tajnih poruka između korisnika uopšte i došlo. Na ovaj način korisnici tajne komunikacije mogu na efikasan i siguran način da razmenjuju tajne poruke, uvereni da one nisu u međuvremenu promenjene od strane nekog trećeg lica i da su tajni ključevi koji se koriste za šifrovanje poruka razmenjeni na siguran način.

Korisnici predloženog sistema mogu da izaberu neka od steganografskih rešenja koja u sebi integrišu i simetrične algoritme za šifrovanje, koji su opisani u poglavlju 4 ove disertacije. Tada bi se predloženi sistem za razmenu tajnih ključeva pomoću ličnih identifikacionih dokumenata koristio za prenos tajnih ključeva koji se koriste u tim steganografskim rešenjima. Mana ovakvih gotovih rešenja je u tome što korisnici nemaju mogućnost izbora algoritma za simetrično šifrovanje. Takođe, u nekim

³ Na osnovu uvida u registar sertifikacionih tela za izdavanje kvalifikovanih digitalnih sertifikata Republike Srbije, može se utvrditi da je sertifikaciono telo MUP RS (*MUPCA*) jedno od pet sertifikacionih tela koje izdaju kvalifikovane digitalne sertifikate. Takođe, MUP RS je jedino sertifikaciono telo koje izdaje kvalifikovane digitalne sertifikate na elektronskim identifikacionim dokumentima građana Republike Srbije.

sistemima nemaju mogućnost izbora dužine tajnog ključa, već moraju da se zadovolje onim što nudi jedan takav hibridni sistem.

Međutim, predloženi sistem za razmenu tajnih ključeva pomoću ličnih identifikacionih dokumenata ne uslovljava korisnike da koriste takve hibridne sisteme, već im dozvoljava da sami odaberu algoritam za simetrično šifrovanje. Na ovaj način korisnici bi mogli, pored izbora sistema za simetričnu kriptografiju, da sami generišu ključeve koji će da se koriste u simetričnom algoritmu za šifrovanje, a steganografske alate da koriste za prikrivanje i prenos poruka koje sadrže informaciju o tajnom kriptografskom ključu korišćenom u simetričnoj kriptografiji.

5.2.1. Primena i implementacija steganografije

Potrebno je napomenuti da karakteristike steganografskih alata nisu uzimane u ozbiljnu evaluaciju s obzirom na činjenicu da oni, u ovoj doktorskoj disertaciji, služe za predstavljanje predloženog koncepta distribucije tajnih ključeva i autentifikacije korisnika tajne komunikacije pomoću ličnih identifikacionih dokumenata.

Steganografski alati koji su trenutno dostupni za besplatnu upotrebu nude vrlo jednostavne i efikasne načine za skrivanje tajnih poruka unutar *JPEG* slika. *JPEG* format je odabran da bude stego nosač kao jedan od najpopularnijih formata za prikazivanje slika (fotografija) na internetu. Međutim, postoje različite metode koje se koriste za stegoanalizu, kojima se može otkriti prisustvo tajne poruke u na izgled običnoj *JPEG* slici. U tu svrhu se koriste vizuelna detekcija, statistička detekcija ili analiza histograma, strukturna detekcija ili detekcija neobičnih struktura.

Promenu *JPEG* slike korišćenjem frekventnog domena prikazali su u svom radu Cheddad et al. [78] Oni su u svom radu dali pregled različitih softvera koji se mogu koristiti u tu svrhu i kritički analizirali performanse istih. Jedan od zaključaka do koga su došli dovodi u spregu steganografske tehnike i njihovu otpornost na moguće napade sa veličinom poruke koja se skriva u *JPEG* slici. Ovaj rad je poslužio kao ideja da se sprovede slična analiza u ovoj disertaciji. Analizom rezultata dobijenih korišćenjem steganografskih alata koji su dostupni za slobodnu upotrebu, a koji su opisani u poglavlju 4, dobijeni su rezultati koji pokazuju da je kapacitet *JPEG* slike za skrivanje podataka u direktnoj vezi sa veličinom same *JPEG* slike, slika 5.2 i 5.3.



300 × 100 px, 23,7 KB

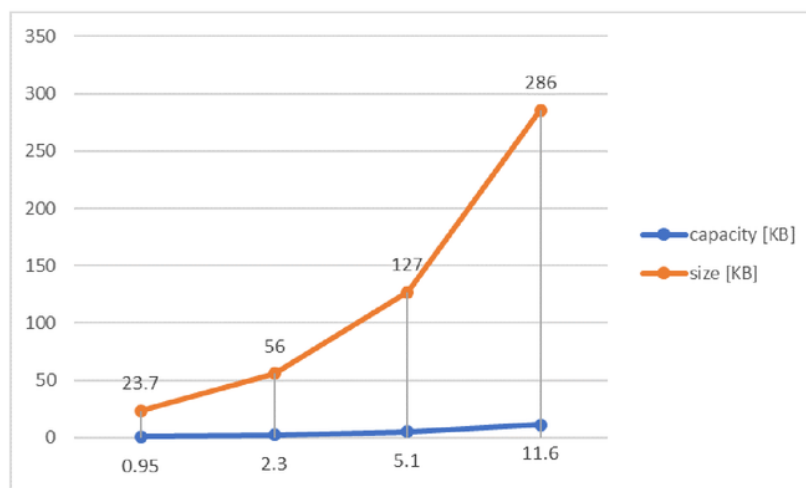
600 × 200 px, 56 KB



2400 × 800 px, 286 KB

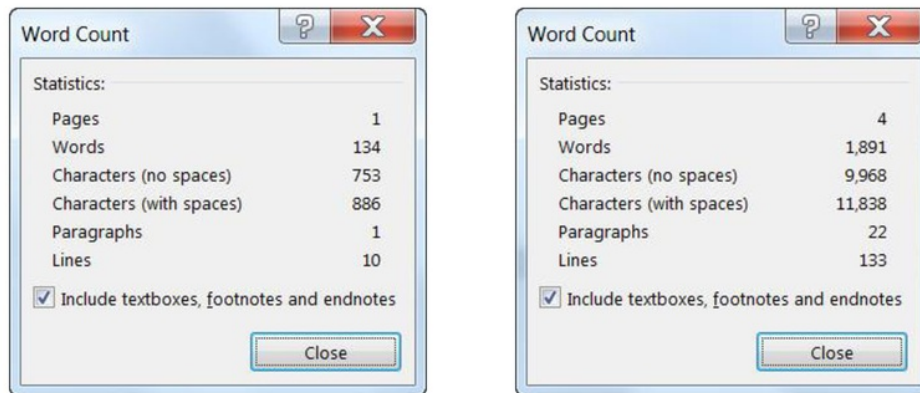
Slika 5.2. Aproksimacija *JPEG* slike nad kojom je vršena analiza kapaciteta za skrivanje podataka

Međutim, ova analiza je pokazala da porast veličine *JPEG* slike ne utiče puno na vrednost koja predstavlja kapacitet *JPEG* slike za skrivanje podataka. Kapacitet za skrivanje poruke neznatno raste u odnosu na porast veličine same *JPEG* slike, slika 3. Uzimajući u obzir da je *JPEG* slika stego nosač mora se voditi računa da se ona ne sme promeniti tako da svojim izgledom, statističkim svojstvima i strukturom ukazuje na činjenicu da u sebi sadrži skrivenu poruku.



Slika 5.3. Dijagram zavisnosti kapaciteta za skrivanje tajnih podataka i veličine *JPEG* slike u KB

Analiza je započeta sa *JPEG* slikom veličine 23.7 KB (što odgovara slici veličine 300 × 100 piksela), a završena je sa *JPEG* slikom veličine 286 KB (što odgovara slici veličine 2400 × 800 piksela). Dužina tekstualne poruke koja je upisivana u *JPEG* sliku najmanje veličine je 134 reči ili 886 karaktera sa razmacima, dok se u najveću *JPEG* sliku, veličine 286 KB, upisivala poruka od 1891 reč ili 11838 karaktera sa razmacima. Broj reči i karaktera sa razmacima koji su navedeni je dobijen brojačem iz *Microsoft Word* dokumenta, slika 5.4.



Slika 5.4. Statistički prikaz poruka zapisanih u najmanjoj i najvećoj slici

Ako se uzme u obzir da korisnik može da bira simetrični algoritam za šifrovanje i da se pretpostavi da je izabrao *AES* ključ od 256 bita, na osnovu predstavljenih podataka o veličini tekstualne poruke može se reći da se ovaj izabrani ključ može utisnuti u najmanji stego nosač, veličine 23,7 KB, bez ikakvog uticaja na izgled, statistička svojstva i strukturu odabrane *JPEG* slike. Ovaj zaključak proizilazi iz činjenice da poruka najmanje veličine konvertovana u *Base64* kodni format sadrži 1184 karaktera bez razmaka, dok *AES* ključ od 256 bita predstavljen u istom tom kodnom formatu sadrži 44 karaktera bez razmaka. Kada se *AES* ključ od 256 bita, sačuvan u *Base64* kodnom formatu, šifrjuje *RSA* ključem od 2048 bita koji se nalazi na ličnom identifikacionom dokumentu broj karaktera onda iznosi 344, slika 5.5.

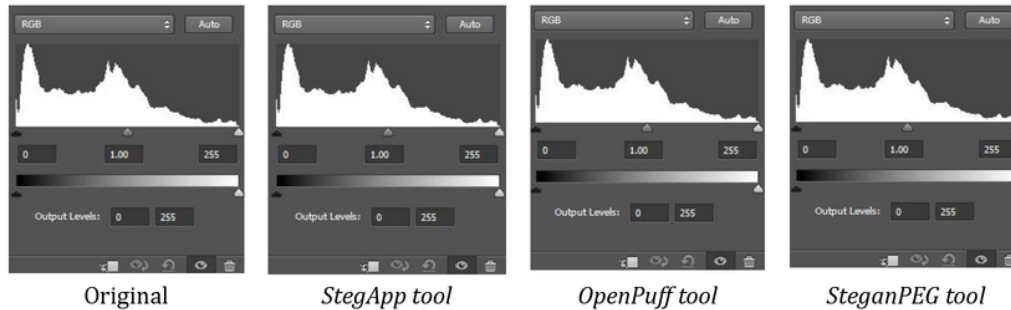
```
ANBdWqyHV4HhCOYBKXSP2Im0A7F3gQ9DzTUZP+VEtrRceaB/IAP8cRbD9ppUwGVi4QPgGYNj0v9j8Fj
WZ4zMTct6XdqB7G9ZcshtYI9hXUO8Bgwue5N4vn+p9SvNQkipwiUtGFV8zffQmjl8y8AiShbQmmJFQvK
xwrpZk9gNUDB0otNY3y/ccjwbZLL11upliNoElLxy1D6gnAecMYXnmHeDizcqkErqO6Vc6+7rDjuzYnox4u
Vb1gOLpE3+IE025IDzots7pXZ9fzln1cakNK/jRqQ/mWZCSBUIfpf8HhLT/mEPA/k4AleKOz07P0Sdw2w71
t20utn8iFo7L29Bw==
```

Slika 5.5. *AES* ključ u šifrovanom obliku

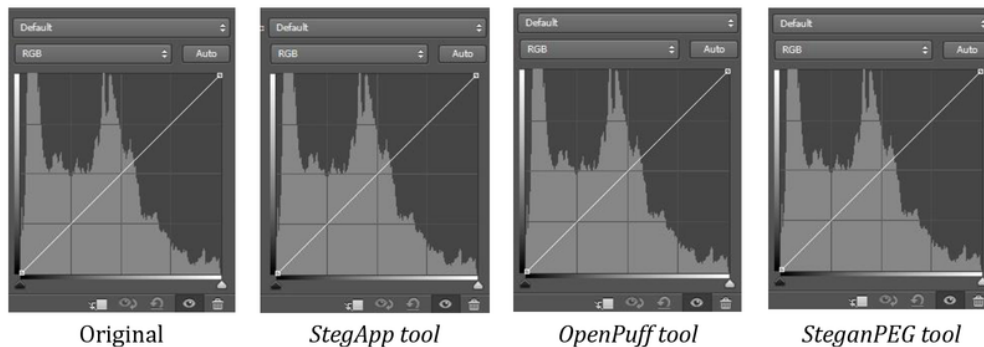
Upotrebom nekoliko javno dostupnih steganografskih alata, koji se mogu besplatno koristiti, došlo se do zaključka da su ovi alati vrlo efikasni prilikom utiskivanja relativno kratkih poruka u *JPEG* slike većih dimenzija. Npr. slika koja je korišćena u gore pomenutom eksperimentu je veličine 286 KB tj. 2400 × 800 piksela prema prikazanim podacima iz analize je mogla da se upotrebi za utiskivanje šifrovanog *AES* ključa od 256 bita. Ova slika je poslužila kao stego nosač, a za utiskivanje tajne poruke koja sadrži šifrovani *AES* ključ upotrebljeni su sledeći steganografski alati: *StegApp tool*, *OpenPuff tool* i *SteganPEG tool*. Kao što je već napomenuto karakteristike ovih steganografskih alata nisu uzimane u ozbiljnu evaluaciju, a oni su detaljno predstavljeni u poglavlju 4 ove disertacije.

Prema prikazanim rezultatima, slika 5.6 i 5.7, može se zaključiti da kvalitet originalne *JPEG* slike nije nimalo promenjen utiskivanjem poruke koja u sebi sadrži 344

karaktera. Potrebno je napomenuti da prema analizi kapaciteta za skrivanje podataka izabrana *JPEG* slika može da posluži kao stego nosač za poruku od 9968 karaktera bez razmaka, što je i prikazano na slici 4. Ovo je veoma bitna napomena jer se šifrovanjem *RSA* ključem od 2048 bita broj reči koji mogu da stanu u takvu poruku smanjuje, što se vidi na primeru šifrovanog *AES* ključa čijih se 44 karaktera bez razmaka, šifrovanjem *RSA* ključem dobija 344 karaktera bez razmaka.



Slika 5.6. Grafički prikaz kvaliteta *JPEG* slike putem opcije *Curves* u programu *Photoshop*



Slika 5.7. Grafički prikaz kvaliteta *JPEG* slike putem opcije *Levels* u programu *Photoshop*

Za analizu *JPEG* slike, originala i stego nosača korišćen je program *Photoshop* i njegove opcije *Curves* i *Levels*. Upoređivan je originalna *JPEG* slika sa *JPEG* slikom nakon steganografskog postupka utiskivanja poruke u istu. Kao krajnji zaključak ove analize nameće se činjenica da je kapacitet *JPEG* slike za skrivanje tajne poruke od velikog značaja za utiskivanje tajne poruke u *JPEG* sliku. Od njega u velikoj meri zavisi koliko podataka, izraženih u *KB*, može da se sakrije u nekoj *JPEG* slici, a da se njen izgled ne promeni. O ovoj činjenici korisnici steganografije moraju posebno da vode računa kako tajna komunikacija ne bi bila razotkrivena.

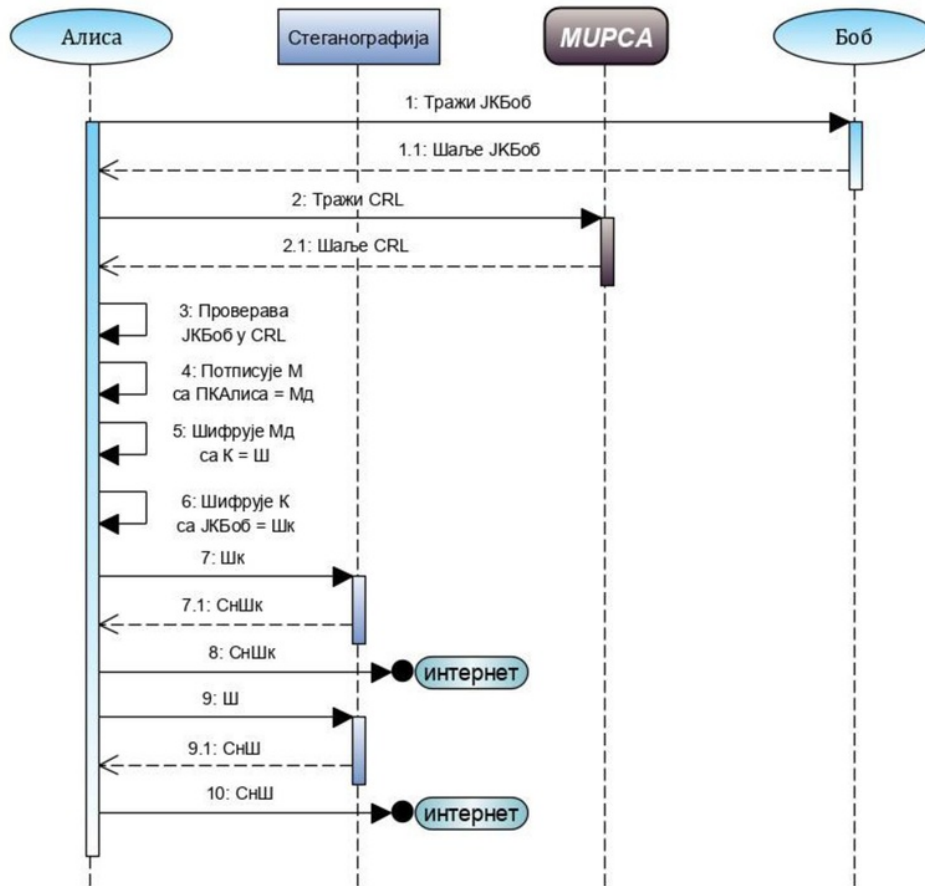
5.2.2. Predloženo rešenje i njegova implementacija

Razmena tajnih ključeva koja podrazumeva da se korisnici tajne komunikacije susretnu na nekoj lokaciji i da ih lično razmene se smatra dobrom praksom. Međutim, ovakav način razmene tajnih ključeva iako je dobar nije uvek i praktičan, pogotovo ako

korisnici koji žele tajno da komuniciraju ne žive u istom gradu, državi ili pak na istom kontinentu. Slanje tajnih ključeva javnim komunikacionim kanalom, kao što je to internet, se smatra nebezbednim jer uvek postoji verovatnoća da je javni komunikacioni kanal prisluškivan od neke treće strane. Pitanje koje se nameće je: "Kako Alisa i Bob mogu na siguran način da razmene tajne ključeve?". Dodatan problem je i to što Bob mora biti uveren da komunicira sa Alisom, i obrnuto, a ne sa nekom nepoznatom osobom koja se predstavlja kao neko od njih.

Organizacije koje pripadaju raznim državama, npr. ambasade, tajne službe, vojska, pa čak i velike internacionalne korporacije koje imaju neograničena ili velika novčana sredstva, infrastrukturu, obučene pojedince za ovakve poslove, i tome sl., nemaju problem da tajne ključeve razmene na bilo koji način. Pojedinci, male organizacije, u koje spadaju i neprofitne organizacije, i njima sl. mogu lično da razmenjuju tajne ključeve ukoliko im lokacijski uslovi pogoduju za to. Međutim, ukoliko je udaljenost među korisnicima koji žele da tajno komuniciraju velika ili se korisnici u ovakvom vidu komunikacije nikada pre nisu ni sreli, pružena im je mogućnost da koriste neki od javno dostupnih servisa za razmenu tajnih ključeva, koji pri tom obezbeđuju i servis autentifikacije. Na ovu činjenicu se ukazuje u ovoj doktorskoj disertaciji, a predloženo rešenje za razmenu tajnih ključeva treba to da im i omogući.

Šema predloženog sistema tajne komunikacije, sekvencijalni dijagram, koja uključuje lična identifikaciona dokumenta građana Republike Srbije, prikazana je na slikama 5.8 i 5.9 – koraci koje preuzimaju Alisa i Bob. Predloženi sistem tajne komunikacije koristi lična identifikaciona dokumenta sa čipom, na kojima su upisana dva kvalifikovana digitalna sertifikata izdata od strane *MUPCA*. Na ovim sertifikatima se nalaze dva para *RSA* ključeva, što je prikazano na slici 5.1. Ovi ključevi se mogu koristiti za digitalno potpisivanje i šifrovanje, respektivno, a u predloženom modelu oni se koriste za šifrovanje tajnih ključeva korišćenih u simetričnim algoritmima za šifrovanje i autentifikaciju korisnika tajne komunikacije.



Slika 5.8. Koraci koje preduzima Alisa u predloženom rešenju

Koraci koje Alisa preduzima u ovakvom sistemu su sledeći:

1. Alisa preuzima digitalni sertifikat od Boba, na kome je zapisan Bobov javni ključ (JK_{Bob}), i vrši proveru njegove validnosti preko *CRL*⁴ izdate od strane *MUPCA*. Provera se vrši kako bi Alisa bila siguran da je Bobov digitalni sertifikat validan.

2. Tekstualnu poruku (M), koju želi da pošalje Bobu, Alisa prvo digitalno potpisuje čime se dobija digitalno potpisana poruka (M_D). Alisa ne želi da Bob na bilo koji način posumnja da ona nije imala uvid u poruku pre šifrovanja iste ili da je M na neki način izmenjen bez Alisinog znanja. Potpisivanje poruke Alisa radi sa svojim privatnim ključem (PK_{Alisa}) koji se nalaz na njenom ličnom identifikacionom dokumentu. Šifrovanje M_D Alisa obavlja algoritmom simetrične kriptografije čime se dobija šifrat ($\check{S}$).

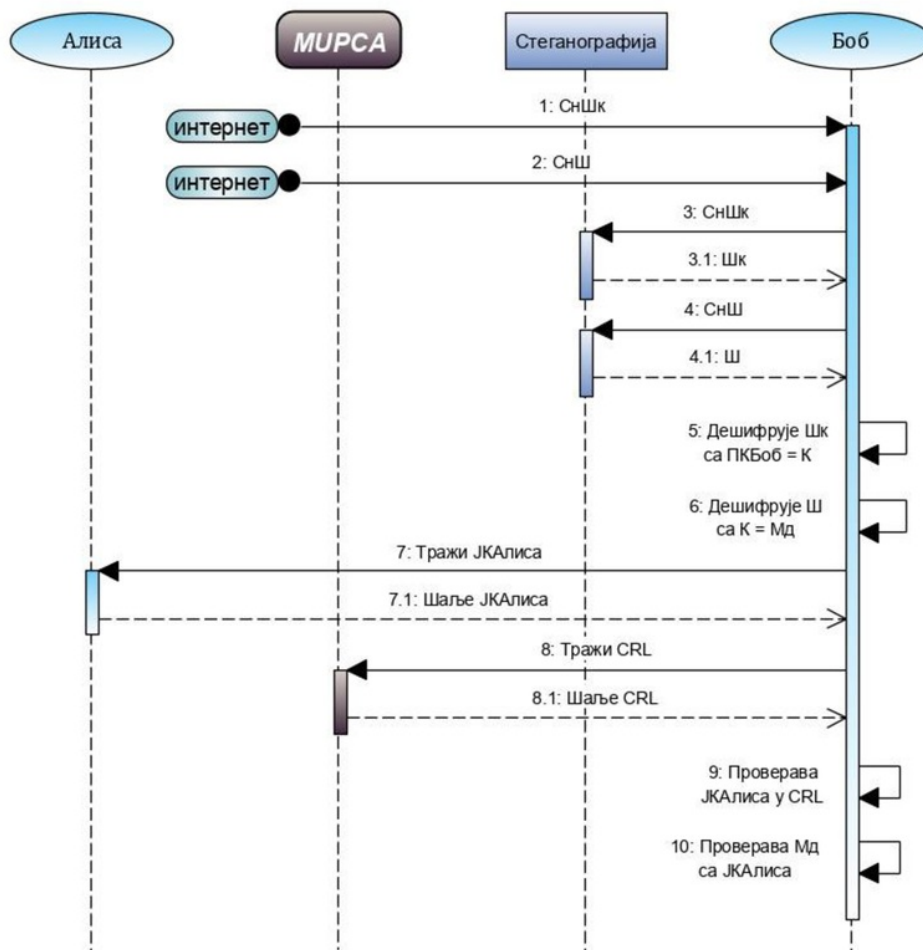
3. Tajni ključ (K) koji se koristio za šifrovanje M_D , Alisa šifruje sa JK_{Bob} čime se dobija šifrovana poruka u kojoj je zapisan tajni ključ ($\check{S}_K$). Na taj način Alisa je uverena

⁴ Lista povučenih sertifikata: <http://ca.mup.gov.rs/CRL.html>

da samo Bob može da dešifruje $\hat{S}_K$ jer samo Bob poseduje privatni ključ koji se nalazi na njegovom ličnom identifikacionom dokumentu (PK_{Bob}).

3. Alisa koristi steganografiju radi utiskivanja $\hat{S}_K$ u odabranu *JPEG* sliku. Takva slika postaje stego nosač ($S_N\hat{S}_K$) i Alisa je postavlja na svoju Veb stranicu ili je distribuira na neki drugi način, vodeći računa o tome da koristi portale koji ne vrše dodatnu kompresiju prilikom slanja *JPEG* slika (npr. *Facebook*).

4. Šifrovanu poruku, tj. $\hat{S}$, Alisa može Bobu da pošalje direktno putem komunikacionog kanala, međutim, Alisa može da ponovi treći korak sa nekom drugom *JPEG* slikom čime bi ona postala novi stego nosač ($S_N\hat{S}$) i time u potpunosti prikrije da je do bilo kakve tajne komunikacije i došlo.



Slika 5.9. Koraci koje preduzima Bob u predloženom rešenju

Koraci koje Bob preduzima u ovakvom sistemu su sledeći:

1. Bob prati šta Alisa objavljuje na svojim Veb stranicama i preuzima *JPEG* slike od kojih jedna u sebi sadrži tajnu poruku, tj. preuzima $S_N\check{S}_K$, a druga sadrži tajni ključ, tj. preuzima $S_N\check{S}_K$.

2. Kako bi dobio $\check{S}$ i $\check{S}_K$ Bob mora da koristi isti steganografski alat koji je koristila Alisa.

3. Bob dešifruje $\check{S}_K$ sa PK_{Bob} kako bi došao do K . Sada kada ima K može da dešifruje $\check{S}$ i dođe do M_D . Kako bi se uverio da je poruka koju je dobio stigla od Alise u neizmenjenom obliku proverice da li je ispravan digitalni potpis kojim je Alisa potpisala poruku čime se sprovodi servis autentifikacije.

4. Bob preuzima Alisin digitalni sertifikat, na kome je zapisan Alisin javni ključ (JK_{Alisa}), i vrši proveru njegove validnosti preko *CRL* izdate od strane *MUPCA*. Ukoliko je digitalni potpis validan Bob može da bude siguran da je to zaista poruka koju mu je Alisa poslala jer je samo Alisa mogla M da potpiše sa PK_{Alisa} .

5.2.2.1. Implementacija predloženog rešenja

Jedan korisnik u ovakvom vidu komunikacije ne mora da poseduje bilo kakva prethodna saznanja o drugom korisniku komunikacije. Sve informacije, koje su mu potrebne da otpočne komunikaciju, nalaze se na kvalifikovanom digitalnom sertifikatu. Podrazumeva se da kvalifikovani digitalni sertifikati za obe strane u komunikaciji moraju da budu izdati od strane *MUPCA* i da obe strane u komunikaciji veruju "trećoj strani od poverenja", tj. sertifikacionom telu koje im je sertifikate i izdalo.

Uz pomoć programa razvijenog u Java programskom jeziku pristupa se kvalifikovanim digitalnim sertifikatima na kojima se nalaze dva para *RSA* ključeva. *RSA* algoritam se smatra sporim algoritmom, on šifrue i dešifrue podatke mnogo sporije nego simetrični algoritmi. Međutim, kako se u ovom slučaju on ne koristi za šifrovanje podataka većeg obima, u smislu veličine tekstualne poruke, on se smatra pogodnim i praktičnim za šifrovanje tajnih ključeva koji se koriste za simetrično šifrovanje. Takođe, važno je napomenuti da postoje programi koje nudi *MUPCA* u okviru svojih usluga, koji vrše digitalno potpisivanje i očitavanje elektronskog identifikacionog dokumenta.

Isto tako, važno je napomenuti da ne postoji javno dostupan alat ili program kojim bi se izvršilo šifrovanje *RSA* ključem koji se nalazi na elektronskom identifikacionom dokumentu građana Republike Srbije, čime se vrši proširivanje funkcionalnosti ličnih identifikacionih dokumenata sa čipom građana Republike Srbije. Program koji je razvijen u Java programskom jeziku uzima *RSA* par ključeva koji se nalaze na kvalifikovano digitalnom sertifikatu namenjenom za autentifikaciju i šifrovanje.

2

Korišćenjem standardne metodologije i alata za softversko modelovanje, radi proširivanja funkcionalnosti ličnih identifikacionih dokumenata sa čipom građana Republike Srbije, razvijen je program u Java programskom jeziku, slika 5.10. Algoritam koji je značajan za ovaj program prikazan je pseudo kodom u sledećim koracima:

```
1 function main(args):  
2     /* configuration */  
3     loadPkcs11ProviderIntoSystem(cfg)  
4     KeyStore keyStore = connectIDAndCreateKeyStore(pinCode, PKCS11)  
5     String alias = getAlias(KeyStore)  
6  
7     /* encryption */  
8     X509Certificate certificate = keyStore.getCertificate(alias)  
9     String text = readFileIntoText(fileLocation)  
10    byte[] encryptedData = encryptText("RSA", text)  
11    writeEncryptedTextIntoFile(encryptData, fileLocation)  
12  
13    /* decryption */  
14    PrivateKey privateKey = keyStore.getKey(alias);  
15    String encryptedText = readEncryptedFileIntoText(fileLocation)  
16    byte[] decryptedData = decryptText("RSA", encryptedText)  
17    writeDecryptedTextIntoFile(decryptedData, fileLocation)  
18
```

Slika 5.10. Pseudo kod predloženog rešenja

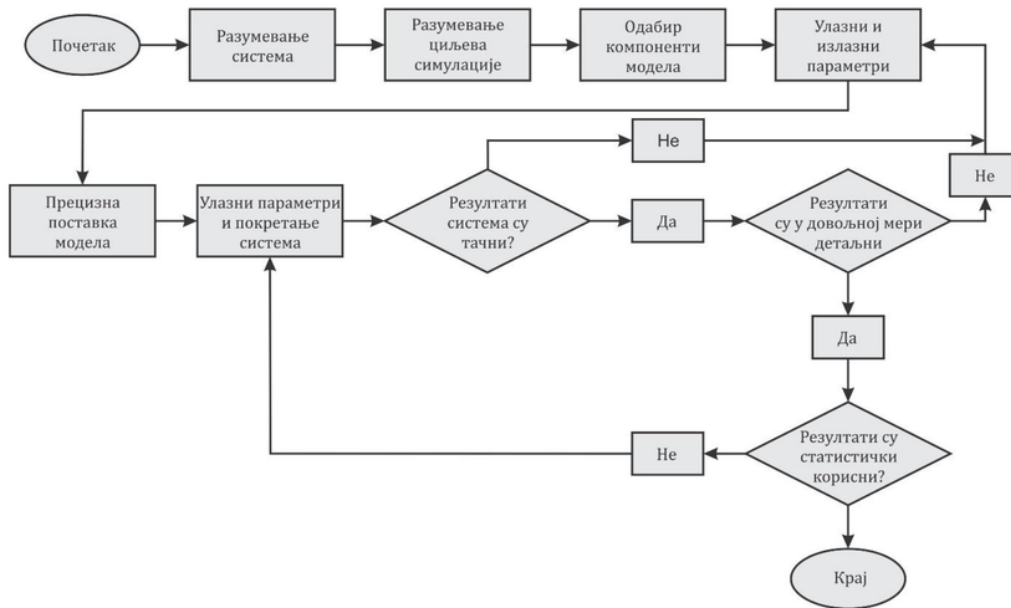
Detaljan prikaz koda razvijenog u Java programskom jeziku biće dat u prilogu ove doktorske disertacije.

6. Evaluacija predloženog rešenja

Pored evaluacije predloženog sistema za razmenu kriptografskih ključeva i njegove implementacije, izvršena je analiza faza planiranja i rezultata dobijenih preko simulacionih modela. Za potrebe ove doktorske disertacije, sa aspekta socijalnih aktivnosti, sprovedena je anketa koja je imala za cilj dobijanje odgovora vezanih za:

1. Opštu informisanost targetirane grupe ispitanika o pojmu kvalifikovani digitalni sertifikat.
2. Motivacija targetirane grupe ispitanika da koristi sisteme za zaštitu privatnosti.

Za izradu simulacionih modela, statističku obradu i prikazivanje dobijenih rezultata korišćen je softverski paket *OPNET IT Guru Academic Edition*, a u završnoj fazi istraživanja i *Riverbed Modeler Academic Edition*. Simulaciona metodologija koja je primenjivana i na osnovu koje su doneti određeni zaključci prikazana je na slici 6.1. Analizom literature [79, 80] izvršen je odabir komponenti simulacionog modela, ulazni i izlazni parametri, kao i način prikazivanja rezultata dobijenih na kraju simulacija.



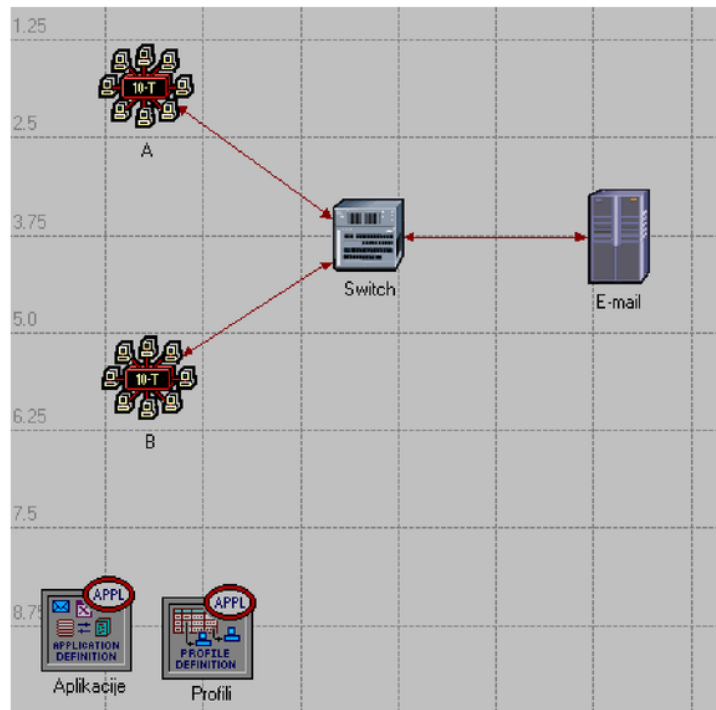
Слика 6.1. Дијаграм контроле тока одлучивања у симулационом моделу

6.1. Prikaz eksperimentalnih rezultata

Implementacija i primena jednog sistema za tajnu komunikaciju koji pri tom obezbeđuje i autentifikaciju korisnika ne predstavlja jednostavan proces. Šifrovanje i digitalno potpisivanje poruka uvećava njihovu veličinu, mereno u *KB*, što je i očekivano zbog samog načina na koji ovi procesi funkcionišu. Međutim, činjenica da su digitalno potpisane i šifrovane poruke koje se razmenjuju znatno veće od rutinski razmenjenih poruka je od bitne važnosti za razvoj jednog sistema za tajnu komunikaciju koji ima za cilj da tu činjenicu da sakrije od potencijalnog napadača.

6.1.1. Simulacija sistema za sigurnu razmenu *email* poruka

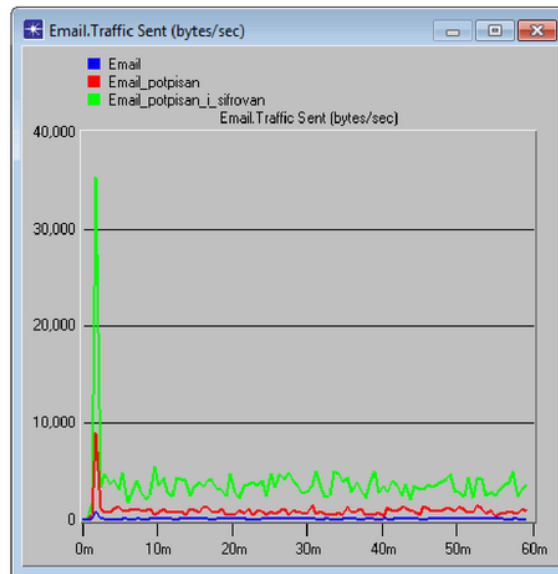
U prvom simulacionom modelu izvršena je aproksimacija tajne komunikacije na taj način što su se za razmenu šifrovanih i autentifikovanih poruka koristile *email* poruke, slika 6.2.



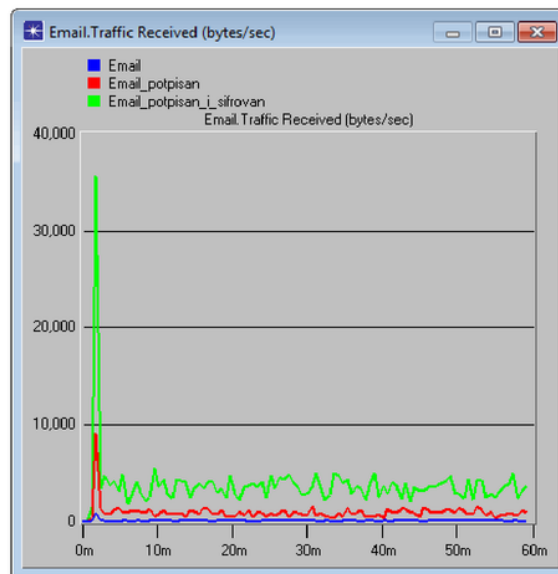
Slika 6.2. Simulacioni model za razmenu tajnih poruka

Ovim simulacionim modelom predstavljena je razmena *email* poruka između dve grupe korisnika preko jednog servera. Simulacija je izvedena korišćenjem tri ista scenarija sa različitim ulaznim parametrima u trajanju od 60 minuta. Za prvi simulacioni scenario korišćena je uobičajena razmena *email* poruka među korisnicima jedne mreže. Zatim je uveden parametar u vidu digitalnog potpisa koji je poslužio za

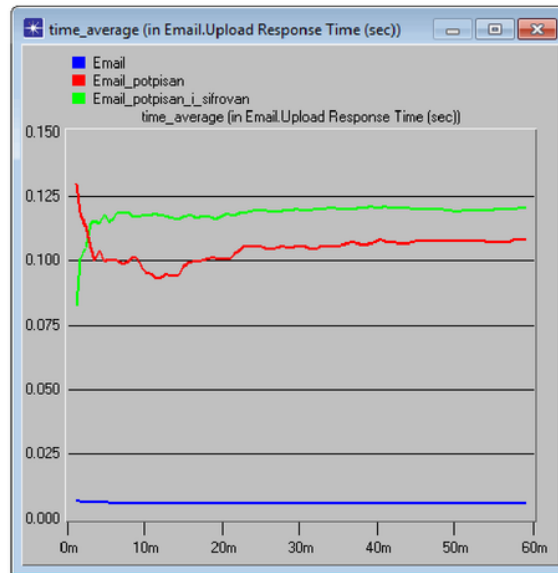
scenario broj dva u kome se simulira ista takva komunikacija. Nakon toga se za treći scenario, koji takođe koristi iste postavke kao i prethodna dva, dodaju dva parametra koji se odnose na digitalno potpisivanje i šifrovanje u isto vreme. Rezultati simulacije su prikazani na sledećim slikama:



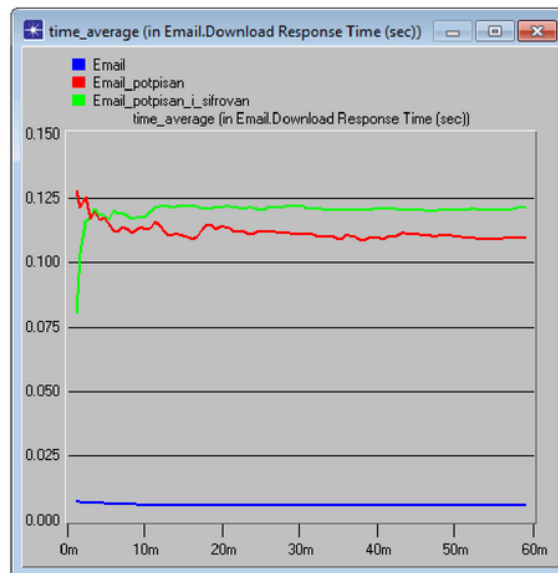
Slika 6.3. Prosečna vrednost odlaznog saobraćaja na mreži



Slika 6.4. Prosečna vrednost dolaznog saobraćaja na mreži



Slika 6.5. Prosečno vreme odgovora servera na zahtev klijenata za slanje *email* poruke predstavljen funkcijom *time_average*



Slika 6.6. Prosečno vreme odgovora servera na zahtev klijenata za preuzimanje *email* poruke predstavljen funkcijom *time_average*

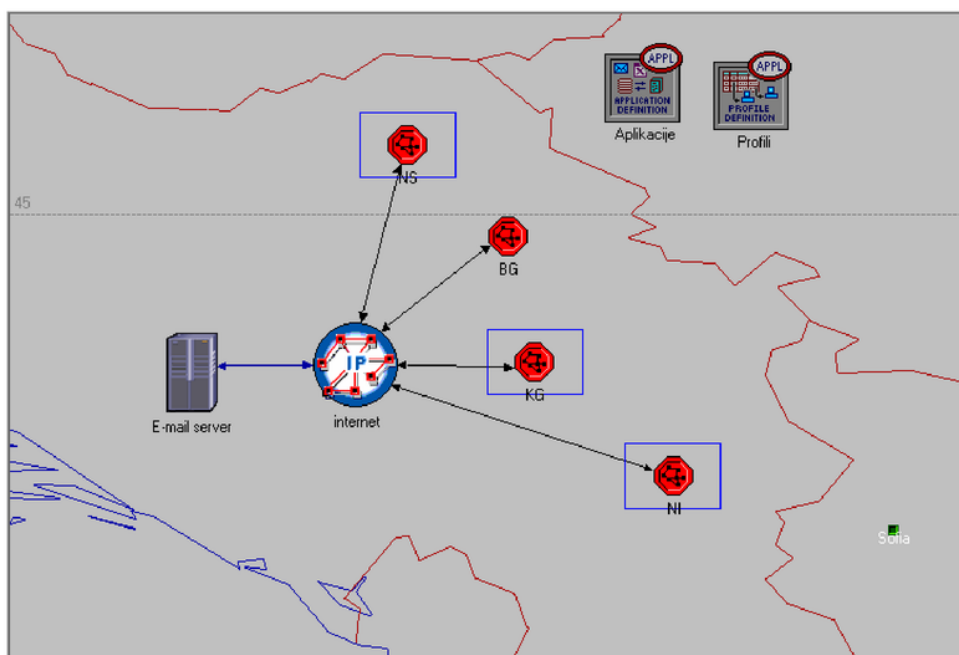
Iz priloženih rezultata se vidi da je generisani saobraćaj najveći prilikom razmene poruka koje su zaštićene i autentifikovane od strane korisnika. Rezultati simulacije su očekivani i potvrđuju činjenicu iznetu u uvodnom izlaganju da postoji potreba da se podatak o neuobičajenom korišćenju razmene poruka sakrije od potencijalnog napadača.

Shodno iznetim činjenicama i rezultatima koji su dobijeni u simulaciji, opravdanost uvođenja steganografskih tehnika u predloženi sistem za tajnu komunikaciju, koji je prikazan u poglavlju 5. ove doktorske disertacije, je potvrđena. Uvođenje steganografije u sistem za tajnu komunikaciju dodatno povećava bezbednost tajne komunikacije time što skriva informaciju da je do nekakve neuobičajene komunikacije uopšte i došlo.

6.1.2. Kritički osvrt na funkcionalnost *PKI* sistema

U ovom simulacionom modelu izvršena je aproksimacija *PKI* sistema koji se koristi u predloženom sistemu za tajnu komunikaciju, opisanom u poglavlju 5. Za korisnike jednog *PKI* sistema veoma je važno da imaju uvid u listu povučenih digitalnih sertifikata, a od posebne važnosti je da ta lista bude dostupna, ažurna i jednostavna za preuzimanje.

Ovim simulacionim modelom se vrši simulacija preuzimanje *CRL* od strane korisnika korišćenjem *pull* metode, što korisnici *MUPCA* inače moraju i da rade, slika 6.7.



Slika 6.7. Simulacioni modela interneta sa podrežama u kojima se koristi *PKI* sistem

Metod preuzimanja *CRL* od strane korisnika sa udaljenog servera se koristi u *PKI* sistemu kome pripada sertifikaciono telo *MUPCA*. Pošto je sertifikaciono telo *MUPCA* jedan od bitnih delova sistema za tajnu komunikaciju koji se koristi u ovoj disertaciji, bilo je potrebno ukazati na nedostatke ovakvog sistema koji se odnose na dinamiku objavljivanja i način distribuiranja *CRL* krajnjim korisnicima ovog sistema.

Nedostaci koji su prikazani ovom simulacijom mogu da utiču i na rad samog sistema tajne komunikacije koji je predložen u ovoj doktorskoj disertaciji. Ovaj nedostatak bi bio posebno izražen ako bi se posmatrao kroz rad jednog velikog *PKI* sistema koji se predlaže na nivou Evropske unije, čiji je cilj da opslužuje približno 500 miliona korisnika i koji je spominjan u poglavlju 2 ove disertacije.

Nakon analize dobijenih rezultata predloženi su načini za unapređenje rada sertifikacionog tela *MUPCA*. Predložena unapređenja utiču pozitivno na efikasnost rada sertifikacionog tela *MUPCA*, a samim tim i efikasnost korišćenja sistema za tajnu komunikaciju predloženog u ovoj doktorskoj disertaciji. Pored poboljšanja efikasnosti, predlozi za unapređenje rada sertifikacionog tela *MUPCA* treba da doprinesu većoj bezbednosti njihovih korisnika, a samim tim i predloženog sistema za tajnu komunikaciju.

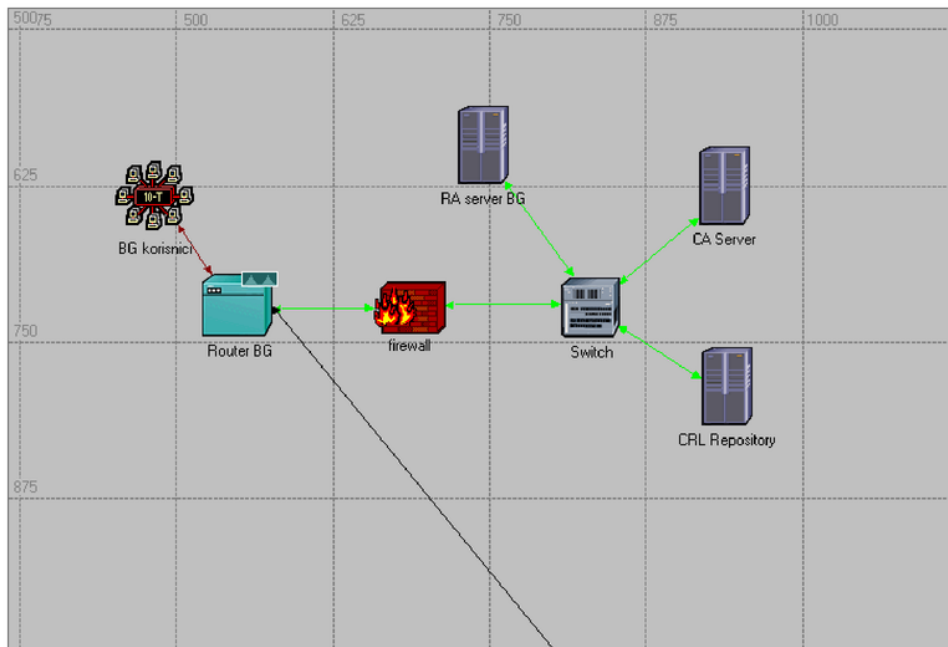
Server za slanje i primanje *email* poruka je postavljen kako bi se predstavila analogija komunikacije između korisnika putem internet mreže i može da se nalazi bilo gde u svetu. U simulacionom modelu nisu obuhvaćeni svi gradovi u kojima sertifikaciono telo *MUPCA* ima svoja registraciona tela, niti je to bio cilj ove simulacije.

Objekti koji se vide na simulacionom modelu koji je prikazan na prethodnoj slici su objašnjeni na slici 6.8.

Име објекта	Модел објекта
<i>E-mail server</i>	<i>ppp_server</i>
<i>internet</i>	<i>ip32_cloud</i>
<i>NS, BG, KG u NI</i>	<i>subnet</i>
комуникациони канали	<i>ppp_DS1 i ppp_DS3</i>
<i>Aplikacije</i>	<i>Application Config</i>
<i>Profili</i>	<i>Profile Config</i>

Slika 6.8. Imena i modeli objekata korišćeni u simulacionom modelu

Modeli objekta simulacionog modela koji predstavljaju gradove u Republici Srbiji su zapravo pod mreže koje koriste *PKI* sistem koji se nalazi u pod mreži *BG* (Beograd). Njihova struktura se razlikuje u nekoliko bitnih elemenata. Objekat simulacionog modela koji je nazvan *CA Server* predstavlja sertifikaciono telo *MUPCA*, slika 6.9.

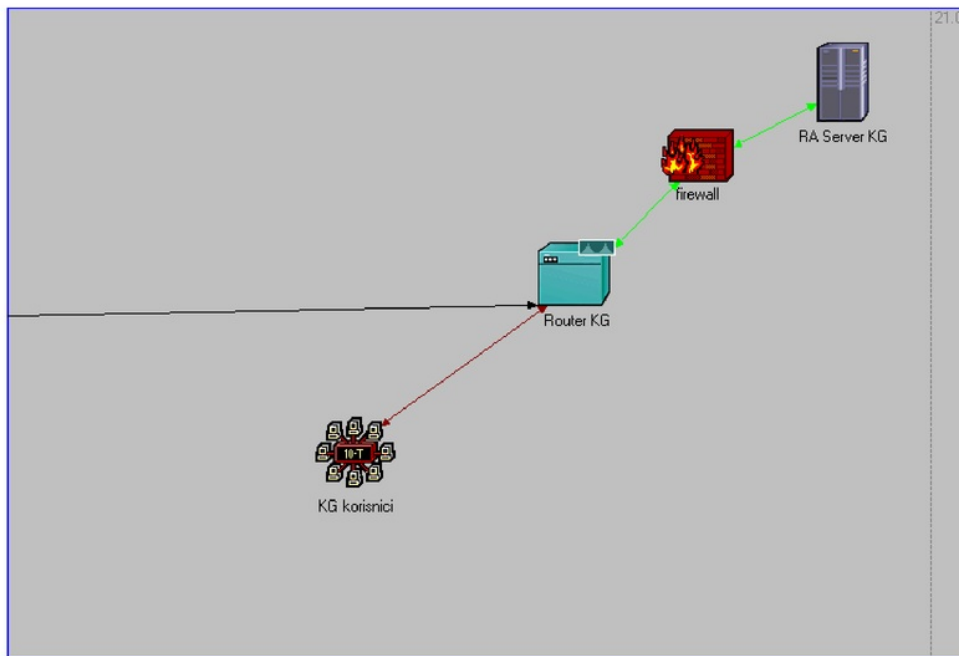


Slika 6.9. Simulacioni model pod mreže BG (Beograd)

CRL Repository je baza podataka ili direktorijum na kome se nalazi lista opozvanih sertifikata potpisana od strane *MUPCA*. Korisnici *PKI* sistema će periodično pristupati *CRL* serveru i preuzimati listu opozvanih sertifikata. Zbog ograničenja od strane simulacionog softvera, koja su već ranije navedena, *CRL* koja se preuzima od strane korisnika u ovoj simulaciji je konstantne veličine. To ne oslikava rad *PKI* sistema u stvarnosti, a ni sama *CRL* nije konstantne veličine, mereno u *KB*.

Međutim, parametri koji se prate u ovom simulacionom modelu odnose se na opterećenje *CRL* servera i beleže se na dva načina. Izvršena je simulacija preuzimanja *CRL* kada je server za preuzimanje centralizovan i smešten na jednoj lokaciji, a nakon toga izvršena je rekonfiguracija sistema tako što je način preuzimanja *CRL* decentralizovan. Performanse *CRL* servera su vrlo bitne za rad ovakvog tipa mreže i zbog toga su praćeni bitni parametri koji utiču na njihov rad. Simulacioni model pod mreže *KG* (Kragujevac), se preslikava i na ostale gradove u simulacionom modelu, tako da nije bilo neophodno da se prilažu na posebnim slikama, slika 6.10.

RA serveri koji se koriste u svim gradovima u ovom simulacionom modelu predstavljaju servere registracionih tela i zaduženi su za kreiranje zahteva za izdavanje digitalnog sertifikata koji se nakon obrade podataka prosleđuje *CA* telu i registraciju novih korisnika. Uloga ovih *RA* servera je ograničena na ove dve aktivnosti i ovi serveri nemaju veliki uticaj na parametre koji se prate.



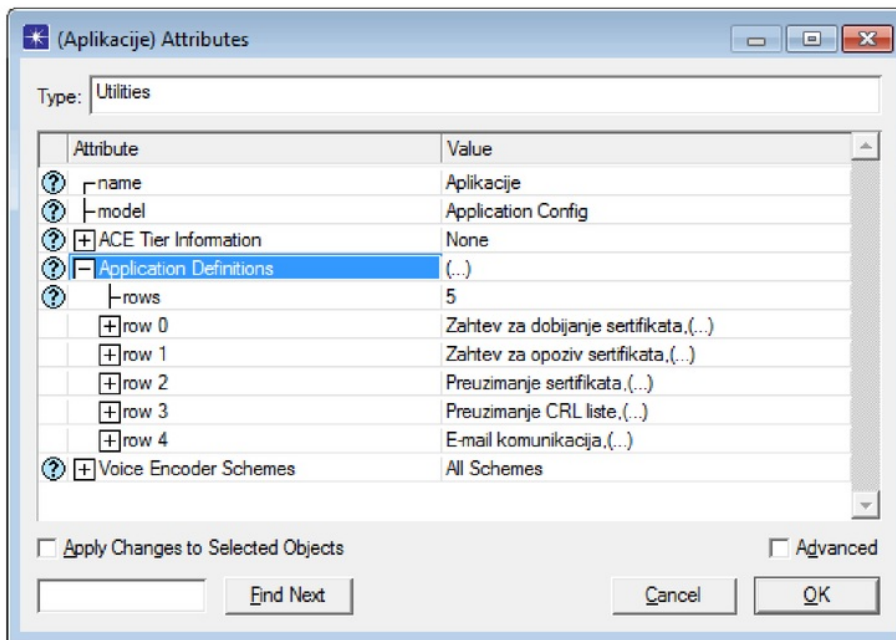
Slika 6.10. Simulacioni model pod mreže KG (Kragujevac)

Objekti koji se vide na simulacionom modelu svih pod mreža su objašnjeni na slici 6.11:

Име објекта	Модел објекта
Сервери	<i>ethernet_server</i>
Корисници	<i>10BaseT_LAN</i>
Рутери	<i>CISCO 7000</i>
Свичеви	<i>ethernet16_switch</i>
Заштитни зид	<i>ethernet2_slip8_firewall</i>
комуникациони канали	<i>10BaseT i 100BaseT</i>

Slika 6.11. Imena i modeli objekata korišćeni u pod mrežama simulacionog modela

Komunikacioni kanali koji omogućavaju komunikaciju između grupe korisnika jedne pod mreže koriste mrežu od 10 Mbps. Serveri PKI sistema međusobnu komunikaciju ostvaruju pomoću mreže od 100 Mbps. Definisanje aplikacija i protokola koji se koriste u ovom simulacionom modelu, koji je baziran na postavkama prethodno prikazanog simulacionog modela, prikazan je na slici 6.12.



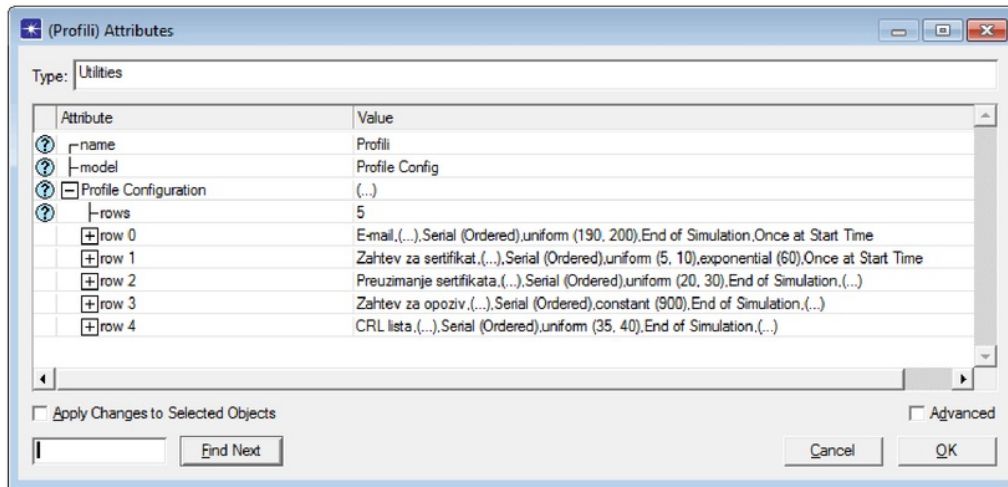
Slika 6.12. Konfigurisanje simulacionog objekta "Aplikacije"

Atributi modela i vrednosti tih atributa, koji se koriste u ovom simuliranom mrežnom okruženju, su prikazani na slici 6.13.

Име апликације	Атрибут модела	Вредност атрибута
Захтев за добијање сертификата	<i>HTTP</i>	<i>Light Browsing</i>
Захтев за опозив сертификата	<i>HTTP</i>	<i>Light Browsing</i>
Преузимање сертификата	<i>FTP</i>	<i>High load</i>
Преузимање CRL листе	<i>HTTP</i>	<i>1048576 bites</i>
E-mail комуникација	<i>Email</i>	<i>102400 bites</i>

Slika 6.13. Parametri aplikacionih modela

Parametri ovih aplikacija su korišćeni za simulaciju rada *PKI* sistema u prvom scenariju prikazane mrežne konfiguracije. U drugom scenariju vrednosti ovih parametara nisu menjane, već je izvršena rekonfiguracija mrežnog okruženja kako bi se prikazao i simulirao decentralizovan način preuzimanja *CRL*. Aktivnosti korisnika u ovakvom mrežnom okruženju definisani su na sledeći način, slika 6.14.



Slika 6.14. Konfigurisanje simulacionog objekta "Profilii"

Detaljan opis zadatih parametara predstavlja srž rada ovog simulacionog modela. Nazivi atributa i opis aktivnosti koje ti atributi realizuju u simulacionom modelu su prilagođeni ograničenjima koja su data od strane samog simulacionog softvera, slika 6.15.

Назив атрибута	Опис активности
E-mail	Апликација се покреће након 190-200 секунди од почетка симулације, што представља време потребно да корисници преузму сертификате и CRL. Извршава се до краја рада симулације.
Захтев за сертификат	Апликација се покреће након 5-10 секунди од почетка симулације, извршава се само једном у току симулације у трајању од 10 секунди.
Преузимање сертификата	Апликација се покреће након 20-30 секунди од почетка симулације, извршава се два пута током симулације у трајању од 180 секунди. Временски интервал рада је 900 секунди.
Захтев за опозив	Апликација се покреће након 900 секунди од почетка симулације у трајању од 60 секунди.
CRL листа	Апликација се покреће након 35-40 секунди од почетка симулације, извршава се шест пута у току симулације у трајању од 180 секунди.

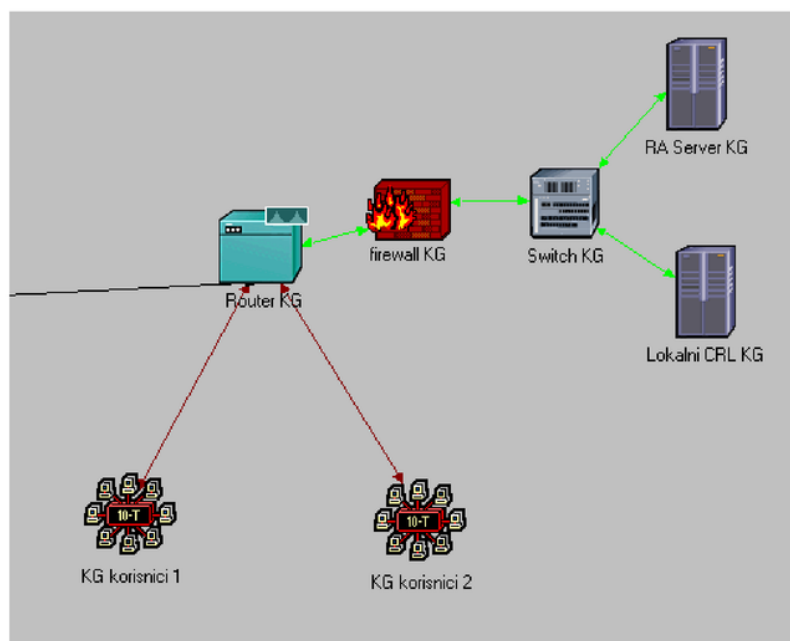
Slika 6.15. Nazivi atributa i opis njihovih aktivnosti

Mogućnost kreiranja različitih scenarija u ovom eksperimentu je iskorišćena da se kompletan simulacioni model posmatra u različitim okolnostima. Promena određenih parametara objekata, a u određenim slučajevima i samih objekata

simulacionog modela, omogućila praćenje izlaznih parametara, eventualnu ponovnu rekonfiguraciju simulacionog modela i poređenje dobijenih rezultata.

Za drugi scenario ovog simulacionog modela kreirana je još jedna aplikacija, pored postojećih, koja je nazvana "Lokalno preuzimanje *CRL* liste" i primenjuje se samo na lokalne korisnike i *CRL* servere. Atributi ove aplikacije su identični atributima već predstavljene aplikacije prvog scenarija pod imenom "Preuzimanje *CRL* liste".

Konfiguracija podmreže *BG* (Beograd) nije menjana, a rasterećenje centralnog *CRL* servera je izvršeno dodavanjem lokalnih *CRL* servera u lokalne podmreže. Konfiguracija podmreže *KG* (Kragujevac) je izmenjena, i ona je identična po pitanju modela objekata koji su promenjeni u podmrežama Novi Sad i Niš, slika 6.16. Podmreži Kragujevac je dodat jedan server, objekat tipa *ethernet_server* koji je imenovan kao "Lokalni *CRL KG*". 80% korisnika ove lokalne mreže je preusmereno na novi lokalni server. Preusmereni korisnici preko rutera su spojeni na mrežu linkom tipa *10BaseT* brzine 10 *Mbps*. Takođe, za 80% korisnika koji će koristiti ovu aplikaciju kreiran je i novi profil pod imenom "*CRL* lista lokalno" koji ima iste attribute kao već predstavljeni profil prvog scenarija pod imenom "*CRL* lista lokalno".



Slika 6.16. Rekonfigurisani simulacioni model podmreže *KG* (Kragujevac)

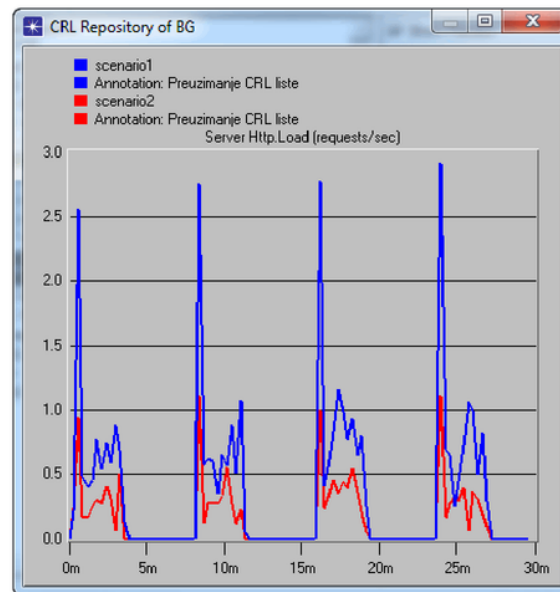
Pre pokretanja simulacije odabrani su statistički parametri koji će da se posmatraju i upoređuju. Simulaciona statistika predstavlja kolekciju jedne ili više vrednosti kojima se opisuju izvesni aspekti procesa ponašanja tokom simulacije. Statistički podaci koji su prikupljeni u ovoj simulaciji odabrani su shodno predmetu i cilju istraživanja postavljenog u predstavljanju ovog simulacionog modela. Praćene su

performanse glavnog *CRL* servera u oba scenarija i shodno tome odabrani su sledeći statistički parametri za praćenje:

- *Load (requests/sec)* - broj aktivnih sesija na serveru.
- *Task Processing Time (sec)* - vreme koje je potrebno da server obradi zahtev klijenta.
- *Traffic Received (bytes/sec)* - prosečna stopa dolaznog saobraćaja.
- *Traffic Sent (bytes/sec)* - prosečna stopa odlaznog saobraćaja.

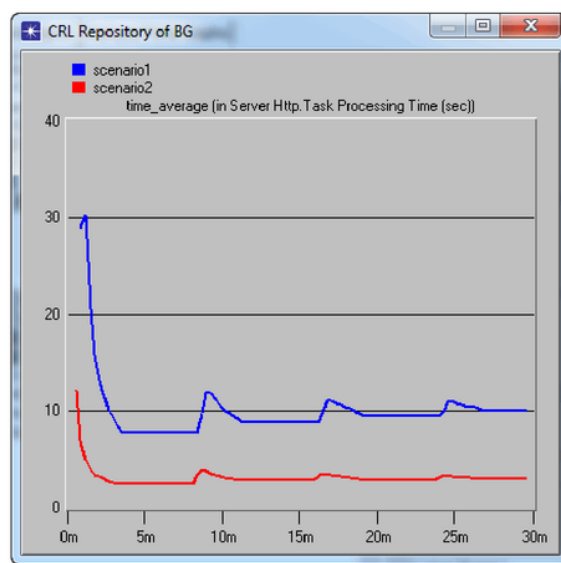
Za simulacioni model, u oba scenarija, vreme trajanja simulacije je postavljeno na 30 minuta. U oba scenarija simulacionog modela prikazan je rad 10 korisnika svake pod mreže, što u ukupnom zbiru iznosi 40 korisnika, s tim da je u drugom scenariju 80% korisnika lokalnih pod mreža preusmereno na lokalne servere.

Podaci za *CRL Repository* server koji se nalazi u pod mreži *BG* (Beograd) prikazani su na slikama 6.17 i 6.18. Na slici 6.17 se uočavaju zadati intervali po kojima korisnici aplikacije pod imenom "CRL lista" pristupaju ovom serveru. Sa slike se vidi da je broj aktivnih sesija na serveru manji primenom decentralizovane metode za distribuiranje *CRL*.



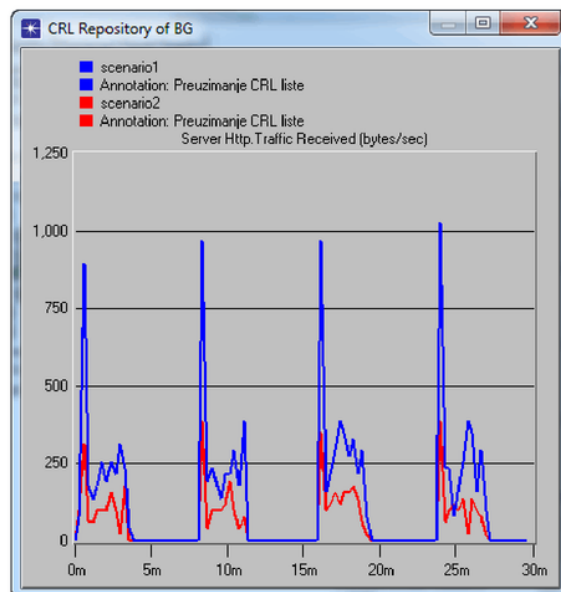
Slika 6.17. Broj aktivnih sesija na serveru u pod mreži *BG* (Beograd)

Decentralizacijom se *CRL Repository* server u pod mreži *BG* (Beograd) znatno rasterećuje, tj. vreme koje je potrebno da server obradi zahteve klijenata znatno manje nego kada je to u pitanju centralizovan metod, slika 6.18.

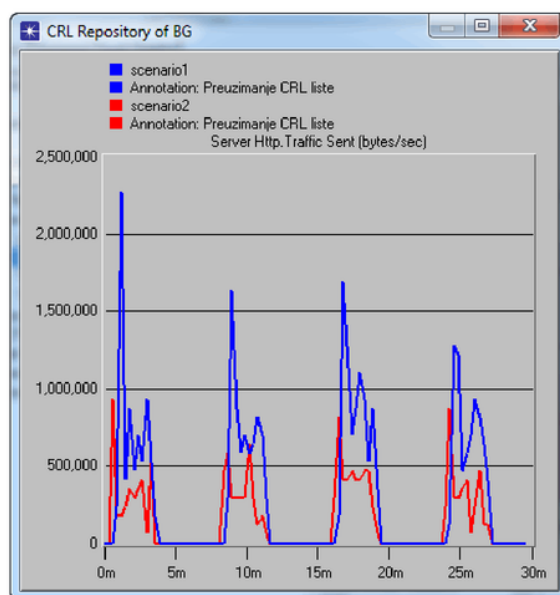


Slika 6.18. Vreme koje je potrebno da server obradi zahtev klijenta u pod mreži BG (Beograd)

Prosečna stopa dolaznog i odlaznog saobraćaja prikazana je na sledećim slikama.



Slika 6.19. Prosečna stopa dolaznog saobraćaja u pod mreži BG (Beograd)



Slika 6.20. Prosečna stopa odlaznog saobraćaja u pod mreži BG (Beograd)

Prosečna stopa dolaznog saobraćaja je očekivano manja po vrednosti jer veličina poruka koje predstavljaju zahteve serveru u pod mreži BG (Beograd) je manja u odnosu na CRL koju server šalje korisnicima u suprotnom smeru.

Na ovim slikama se takođe jasno uočavaju zadati intervali po kojima korisnici aplikacije pod imenom "CRL lista" pristupaju serveru. Takođe se sa slika vidi da je generisani saobraćaj manji primenom decentralizovane metode za distribuiranje CRL i može se zaključiti da je CRL Repository server znatno rasterećen upotrebom lokalnih servera za distribuiranje CRL.

Informacije o korišćenom softveru u eksperimentu:

- OPNET IT Guru Academic Edition 9.1.A PL1(Build 2000)
- Microsoft Windows 7 Professional x64, Service Pack 1

Informacije o korišćenom hardveru u eksperimentu:

- MB: Asus H77 P8H77-M
- CPU: Intel i5-3470, 3.20 GHz, 4 Core(s)
- RAM: 8.00 GB DDR3 1600 MHz
- HDD: SATA3 7200 2TB

Rezultatima simulacije je potvrđena pretpostavka da razmena CRL utiče na rad servera za distribuciju iste, samim tim utiče i na performanse PKI sistema, koje posredno utiču i na rad predloženog sistema za tajnu komunikaciju. Rezultati koji su prikazani su potvrdili da postoje razlike između centralizovanog i decentralizovanog metoda za distribuiranje CRL liste. Ukoliko bi MUPCA promenio način koji je trenutno u

upotrebi, povlačenje *CRL* od strane korisnika *PKI* sistema, uvođenjem decentralizovanih servera ili uvođenjem *OCSP* protokola bezbednosne karakteristike bi bile poboljšane. Takođe se nedostatkom ovog sistema može smatrati činjenica da se *CRL* objavljuje jednom u toku 24 časa. Poboljšanje ovih bezbednosnih parametara bi se direktno odrazilo i na poboljšanje bezbednosti korisnika predloženog sistema za taj komunikaciju, opisanog u glavi 5.

6.2. Anketa

Anketa o zaštiti privatnosti i doprinosu iste u društvu sprovedena je među studentima prve godine, Visoke tehničke škole strukovnih studija u Kragujevcu, na početku školske 2017. i 2018. godine. Pitanja su bila podeljena u dve grupe. Prva grupa pitanja odnosila se na informacije o posedovanje biometrijske lične karte i da li su upoznati sa činjenicom da ona može sadržati kvalifikovani digitalni sertifikat. Druga grupa pitanja se odnosila na zaštitu privatnosti na internetu i da li su zainteresovani uopšte da zaštite svoju privatnost. Anketa je imala za cilj da podstakne ispitanike na razmišljanje o pojmu privatnosti na internetu i jačanja svesti ispitanika o važnosti zaštite privatnosti na internetu.



Slika 6.21. Da li posedujete biometrijsku ličnu kartu (sa čipom)?

Profil anketiranih studenata: Od ukupnog broja ispitanika koje su odgovorile na anketu, više od polovine su studenti na odseku Informatika, starosne dobi 18 do 23 godina. Ovakav profil ispitanika odgovara pojmu "digitalno pismena osoba".

Evaluacija predloženog rešenja



Slika 6.22. Da li ste upoznati sa činjenicom da biometrijska lična karta (sa čipom) može da sadrži kvalifikovani digitalni sertifikat?

80% ispitanika poseduje biometrijsku ličnu kartu, 44% ispitanika ima saznanje da ona može sadržati kvalifikovani digitalni sertifikat, pri čemu samo trećina od njih je informisana da time može zaštititi svoju privatnost na internetu.



Slika 6.23. Da li ste upoznati sa činjenicom da upotrebom kvalifikovanog digitalnog sertifikata možete da zaštitite svoju privatnost na internetu?

To ukazuje na činjenicu da veliki deo ispitanika nije informisan adekvatno i ne poseduje znanja vezana za mogućnosti zaštite, pa samim tim i nije u mogućnosti da sa sigurnošću izrazi stav da li bi koristila biometrijsku ličnu kartu koja sadrži kvalifikovani digitalni sertifikat za zaštitu svoje privatnosti na internetu.



Slika 6.24. Da li bi ste koristili biometrijsku ličnu kartu (sa čipom) koja sadrži kvalifikovani digitalni sertifikat za zaštitu svoje privatnosti na internetu?

Sve ovo govori u prilog tome da podizanje svesti ispitanika o prednostima koje im donosi zaštita privatnosti na internetu i saznanje da upotrebom predloženog sistema za tajnu komunikaciju u ovoj disertaciji mogu tu privatnost i da ostvare. Takođe je bitno naglasiti da je saznanje ispitanika o mogućnostima koje im, kao krajnjim korisnicima predloženi sistem pruža, društveni doprinos ovog istraživanja u potpunosti ispunjen.

6.3. Poređenje s postojećim rešenjima i pravci daljih istraživanja

Predloženi sistem za tajnu komunikaciju krajnjih korisnika koji unapređuje protokol za razmenu kriptografskih ključeva na bazi ličnih identifikacionih dokumenata dokazao je svoj "*proof of concept*", tj. da je ovaj sistem, opisan u ovoj doktorskoj disertaciji, dokazao izvodljivost i pokazao da su teoretske pretpostavke iznete u hipotezama disertacije dokazane.

U poređenju sa predstavljanim sistemima i rešenjima, opisanim u poglavlju 4 ove disertacije, predloženi sistem za tajnu komunikaciju se pokazao kao kompletno rešenje koje korisnicima pruža odgovor kako da na siguran i jednostavan način razmene tajne ključeve korišćene u steganografskim alatima. Sistem koji objedinjuje steganografske alate, simetričnu kriptografiju i lične identifikacione dokumente građana Republike Srbije kao takav se do sada nije koristio. Postoje brojni primeri upotrebe ličnih identifikacionih dokumenata, koji su između ostalog navedeni u poglavlju 2 ove disertacije, međutim, nijedno od njih se nije odnosilo na razmenu kriptografskih ključeva.

Svi alati navedeni u poglavlju 4 pružaju određeni nivo zaštite, međutim, u svakom od tih sistema se postavlja pitanje kako i na koji način korisnici mogu da razmene tajne ključeve ili lozinke koje se koriste u tim aplikacijama.

Postoje razni sistemi za razmenu kriptografskih ključeva koji se koriste u profesionalnoj praksi i koji su dokazano sigurni. Predloženi sistem za tajnu komunikaciju nije preporučljivo koristiti u svrhe profesionalne zaštite, prvenstveno jer se bazira na korišćenu digitalnih sertifikata izdatih od "treće strane od poverenja". Međutim, iako *MUPCA* predstavlja "treću stranu od poverenja" kojoj korisnici njihovog *PKI* sistema veruju, može se tvrditi da su tajni ključevi u predloženom protokolu razmenjeni na siguran način. Tajni ključevi koji se koriste u ovom rešenju prvenstveno imaju za cilj da zaštite privatnost pojedinca kao individue na internetu, a ne velikih korporacija i državnih službi koji bi štitili poverljiva dokumenta sa oznakom "državna tajna". Masovna upotreba i lakoća korišćenja predloženog sistema su dve činjenice koje bi ovaj predloženi sistem mogao vrlo lako da ostvari.

Dalji razvoj na predloženom sistemu tajne komunikacije bi bio razvoj jedne sveobuhvatne mrežne ili *Cloud* aplikacije koja bi primenu ovog sistema približila korisnicima pametnih telefona i aplikacijama koje oni koriste. Ovaj sistem je razvijen u Java programskom jeziku što mu garantuje modularnost i primenu na gotovo svim operativnim sistemima. Takođe je potrebno razviti novi način za proveru povučenih sertifikata jer činjenice koje su iznete u ovoj disertaciji ukazuju da je to jedan od većih nedostataka. Međutim, to ne zavisi direktno od predloženog sistema već od izdavača kvalifikovanih digitalnih sertifikata, tj. od sertifikacionog tela *MUPCA*. Vremenski period od 24 časa, tj. period koji se odnosi na objavljivanje *CRL* liste, je predugačak s obzirom na činjenicu da se transakcije bilo koje vrste putem internet i mobilne mreže izvršavaju gotovo trenutno. U takvom jednom sistemu činjenica da korisnik nema trenutnu informaciju o validnosti digitalnog sertifikata ne doprinosi bezbednosti, već naprotiv, otvara razne mogućnosti za zloupotrebu.

7. Zaključak

Analizom i sistematizacijom postojećih znanja, iskustava i naučnih rezultata iz oblasti istraživanja ove doktorske disertacije, definisan je predmet i cilj istraživanja.

Cilj istraživanja doktorske disertacije je unapređenje protokola za razmenu tajnih kriptografskih ključeva koji se koriste u simetričnoj kriptografiji. Izvršena je analiza aktuelnih problema vezanih za bezbednu elektronsku razmenu tajnih ključeva koji se koriste u simetričnoj kriptografiji i autentifikaciju korisnika sistema za tajnu komunikaciju, kao i analiza postojećih rešenja u oblasti istraživanja.

Razvijanje sistema za komunikaciju, koji se danas većinom oslanjaju na internet, bežičnu komunikaciju i komunikaciju putem mobilnih mreža u kojima brzine prenosa podataka neprestano rastu, povećava se i broj novih korisnika, kako i broj novih usluga sa intuitivnim interfejsima. Analizom iznetih činjenica u doktorskoj disertaciji i donošenjem zaključka da elektronska distribucija tajnih simetričnih ključeva postaje sve više "usko grlo", predstavljeno je unapređeno rešenje koje se zasniva na simetričnim i asimetričnim šifarskim sistemima, i na korišćenju jedinstvenih kriptoloških parametara koji se nalaze na ličnim identifikacionim dokumentima građana Srbije.

Praktični cilj ovog istraživanja ogleda se u razvoju i primeni jednog novog sveobuhvatnog modela za tajnu komunikaciju. Novo rešenje se zasniva na korišćenju jedinstvenih parametara koji se nalaze na identifikacionim dokumentima građana i na primeni steganografskih tehnika za sakrivanje i utiskivanje kratkih sekvenci u različite standardne medije za komunikaciju (slika, tekst, govor, video, elektronska pošta i sl.). Razvijeno rešenje nema teorijsku podlogu za profesionalne sisteme zaštite, ali je veoma upotrebljivo za komercijalnu upotrebu i lako se može realizovati i koristiti u svakodnevnom radu velikog broja standardnih korisnika servisa na internetu.

Sprovedena anketa među studentima prve godine Visoke tehničke škole strukovnih studija u Kragujevcu, odmah nakon upisa u prvu godinu studija, ukazuje na to da razvoj predloženog modela za tajnu komunikaciju može da doprinese većoj društvenoj prihvatljivosti i da podstiče korisnike da koriste sredstva za zaštitu privatnosti koja su im lako dostupna. S podizanjem opšte svesti o jednostavnosti upotrebe predloženog modela i ukazivanjem na širok spektar mogućnosti koji se nude krajnjim korisnicima društveni cilj ovog istraživanja bi bio u potpunosti zadovoljen.

Naučni doprinos ovog rada odnosi se na primeni jedinstvenih parametara sa ličnih identifikacionih dokumenata za razvoj sopstvenog rešenja za zaštitu tajnih simetričnih ključeva. Poverenje u parametre koji se koriste za sopstveno rešenje počiva

na poverenju u rad kvalifikovanih sertifikacionih tela. U ovom radu korišćeni su kvalifikovani digitalni sertifikati koje izdaje MUP Republike Srbije. Kao dodatna mera koja je usmerena ka poboljšanju predloženog sistema za tajnu komunikaciju predlaže se primena steganografskih tehnika za sakrivanje šifrovanih ključeva simetrične kriptografije u odgovarajući stego nosač.

U disertaciji je izvršena detaljna analiza dostupnih protokola za elektronsku distribuciju tajnih simetričnih kriptografskih ključeva i ukazano je na potencijalne slabosti i prednosti predloženog rešenja. U radu je pokazana efikasnost predloženog postupka primenom na Veb galeriju slika koje su date u tzv. *JPEG* formatu. Predloženi postupak se efikasno može primeniti i kod drugih standardnih nosilaca u današnjim komunikacija (tekst, slika, govor, video i tome sl.), kao i kod standardnih komunikacionih servisa (imejl, *Viber*, *WhatsApp* i sl.). Dat je kritički osvrt na delove sistema za tajnu komunikaciju koji mogu da utiču na bezbednu upotrebu istog i date smernice za unapređenje nedostataka. Kada bi ovaj problem bio rešen, tj. kada bi se matematički mogla potvrditi apsolutna tajnost u elektronskoj distribuciji ključeva, to bi dovelo do revolucionarnih promena u profesionalnim i komercijalnim sistemima za zaštitu tajnosti u prenosu podataka.

U skladu sa do sada navedenim, doprinosi doktorske disertacije su:

- Razvijen je novi protokol za razmenu tajnih simetričnih kriptografskih ključeva na bazi ličnih identifikacionih dokumenata pošiljaoca i primaoca. Predloženo rešenje ima niz kriptoloških prednosti od kojih se izdvajaju:
 - Ne postoji potreba da se smešta i čuva veliki broj tajnih ključeva kod korisnika pošto se oni mogu kompromitovati,
 - Za svaku novu komunikacijsku sesiju generiše se novi tajni ključ. Eventualna kompromitacija jednog ovakvog ključa ne utiče na tajnost ostalih prenetih poruka, pošto su one šifrovane drugim ključem.
 - Ostvaruje se potpuna *end-to-end* zaštita za svaku komunikaciju i za svaki par učesnika u tajnoj komunikaciji.
- Razvijeno je sopstveno rešenje koje ne zahteva rad tzv. treće strane od poverenja. Koriste se samo parametri koji su izdati od strane tela koje izdaje kvalifikovane digitalne sertifikate.
- Razmatrana je primena steganografskih tehnika za sakrivanje šifrata u odgovarajući tzv. stego nosilac. Na primeru *JPEG* slika pokazano je da sakrivena informacija ne utiče na statističke karakteristike, niti na memorijske karakteristike stego nosioca.
- Novi protokol je otporan na veliki broj napada na mreži.

Rezultati rada se mogu koristiti za široki spektar komercijalnih rešenja za komunikaciju. Od korisnika takvih rešenja se ne zahteva profesionalno poznavanje kriptografije. Ostvarena komunikacija se teško može otkriti i obezbeđuje visok stepen tajnosti za aplikacije koje koriste tajne simetrične kriptografske ključeve. Za profesionalne sisteme zaštite, ostvareni rezultat se može posmatrati kao korak više u

zaštiti kada se posmatraju kombinovana rešenja sa nadšifrovanjem i sakrivanjem šifrovanog materijala.

Literatura

- [1] Meng, Keju, Fuyou Miao, and Yue Yu. *A secure and efficient on-line/off-line group key distribution protocol*. *Designs, Codes and Cryptography* 87.7: 1601-1620, 2019.
- [2] Vijayakumar, P., et al. *Key management and key distribution for secure group communication in mobile and cloud network*. *Future Generation Computer Systems* 84: 123-125, 2018.
- [3] Al-Qurishi, Muhammad, et al. *An efficient key agreement protocol for Sybil-precaution in online social networks*. *Future Generation Computer Systems* 84: 139-148, 2018.
- [4] Zhou, Yukun, et al. *A similarity-aware encrypted deduplication scheme with flexible access control in the cloud*. *Future Generation Computer Systems* 84: 177-189, 2018.
- [5] Guo, Cheng, et al. *Key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage*. *Future Generation Computer Systems* 84: 190-199, 2018.
- [6] Shen, Pei-Yuan, Vicky Liu, and William Caelli. *A viable and sustainable key management approach for a national e-health environment*. 2012 IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom), IEEE, 2012.
- [7] Kim, Sundeuk, Hyun-Taek Oh, and Young-Gab Kim. *Certificate sharing system for secure certificate distribution in mobile environment*. *Expert Systems with Applications* 44: 67-77, 2016.
- [8] von Maurich, Olga, and Alessandro Golkar. *Data authentication, integrity and confidentiality mechanisms for federated satellite systems*. *Acta Astronautica* 149 : 61-76. 2018.
- [9] John, Saju P., and Philip Samuel. *Self-organized key management with trusted certificate exchange in MANET*. *Ain Shams Engineering Journal* 6.1: 161-170, 2015.
- [10] Yüce, Emre, and Ali Aydın Selçuk. *Server notaries: a complementary approach to the web PKI trust model*. *IET Information Security* 12.5: 455-461, 2018.
- [11] Lozupone, Vincent. *Analyze encryption and public key infrastructure (PKI)*. *International Journal of Information Management* 38.1: 42-44, 2018.
- [12] Nagar, Sami A., and Saad Alshamma. *High speed implementation of RSA algorithm with modified keys exchange*. 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), IEEE, 2012.
- [13] Yao, Andrew Chi-Chih, and Yunlei Zhao. *Privacy-preserving authenticated key-exchange over internet*. *IEEE Transactions on Information Forensics and Security* 9.1: 125-140, 2013.

- [14] Zwattendorfer, Bernd, and Daniel Slamanig. *Design strategies for a privacy-friendly Austrian eID system in the public cloud*. Computers & Security 52: 178-193, 2015.
- [15] Zwattendorfer, Bernd, and Daniel Slamanig. *The Austrian eID ecosystem in the public cloud: How to obtain privacy while preserving practicality*. Journal of information security and applications 27: 35-53, 2016.
- [16] Rezaeighaleh, Hossein, Roy Laurens, and Cliff C. Zou. *Secure Smart Card Signing with Time-based Digital Signature*. International Conference on Computing, Networking and Communications (ICNC), IEEE, 2018.
- [17] Sánchez-García, Jesús, et al. *On-siteDriverID: A secure authentication scheme based on Spanish eID cards for vehicular ad hoc networks*. Future Generation Computer Systems 64: 50-60, 2016.
- [18] León-Coca, Jose Maria, et al. *Authentication systems using ID Cards over NFC links: the Spanish experience using DNle*. Procedia Computer Science 21: 91-98, 2013.
- [19] Carretero, Jesus, et al. *Federated identity architecture of the European eID system*. IEEE Access 6: 75302-75326, 2018.
- [20] Berbecaru, Diana, Antonio Lioy, and Cesare Cameroni. *Authorize-then-Authenticate: Supporting Authorization Decisions Prior to Authentication in an Electronic Identity Infrastructure*. International Symposium on Intelligent and Distributed Computing. Springer, Cham, 2019.
- [21] Lenz, Thomas, and Vesna Krnjic. *Towards Domain-Specific and Privacy-Preserving Qualified eID in a User-Centric Identity Model*. 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), IEEE, 2018.
- [22] Slamanig, Daniel, Klaus Stranacher, and Bernd Zwattendorfer. *User-centric identity as a service-architecture for eIDs with selective attribute disclosure*. Proceedings of the 19th ACM symposium on Access control models and technologies, ACM, 2014.
- [23] Poller, Andreas, et al. *Electronic identity cards for user authentication-promise and practice*. IEEE Security & Privacy 1: 46-54, 2012.
- [24] Lenz, Thomas, and Lukas Alber. *Towards cross-domain eid by using agile mobile authentication*. IEEE Trustcom/BigDataSE/ICSS, IEEE, 2017.
- [25] Lips, Silvia, et al. *Key Factors in Coping with Large-Scale Security Vulnerabilities in the eID Field*. International Conference on Electronic Government and the Information Systems Perspective, Springer, Cham, 2018.
- [26] Amin, Muhalim Mohamed, et al. *Information hiding using steganography*. 4th National Conference of Telecommunication Technology, NCTT 2003 Proceedings, IEEE, 2003.
- [27] El_Rahman, Sahar A. *A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information*. Computers & Electrical Engineering 70: 380-399. 2018.

- [28] Attaby, Abdelhamid Awad, Mona FM Mursi Ahmed, and Abdelwahab K. Alsammak. *Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3*. Ain Shams Engineering Journal, 2017.
- [29] Muhammad, Khan, et al. *Image steganography using uncorrelated color space and its application for security of visual contents in online social networks*." Future Generation Computer Systems 86: 951-960, 2018.
- [30] Jain, Mamta, Saroj Kumar Lenka, and Sunil Kumar Vasistha. *Adaptive circular queue image steganography with RSA cryptosystem*." Perspectives in Science 8: 417-420, 2016.
- [31] Achuthshankar, Aswathy, et al. *Encryption of Reversible Data Hiding for Better Visibility and High Security*. Procedia Technology 25: 216-223, 2016.
- [32] Xiaojian, Luo, and Long Xiang. *AS algorithm: An optimal on-line real-time scheduling algorithm for uniform multiprocessors*. 3rd International Conference on Computational Intelligence & Communication Technology (CICT), IEEE, 2017.
- [33] Bharti, Pria, and Roopali Soni. *A new approach of data hiding in images using cryptography and steganography*. International Journal of Computer Applications 58.18, 2012.
- [34] Uljarević, Dejan., A. Mišković et al. *An Overview of Steganographic Techniques and Methods Applied on Jpeg Images Using Different Transformational Techniques*. Sinteza 2016 - International Scientific Conference on ICT and E-Business Related Research, Singidunum University Belgrade, pp. 165-172, 2016.
- [35] Uljarević, Dejan, et al. *A new way of covert communication by steganography via JPEG images within a Microsoft Word document*. Multimedia Systems 23.3: 333-341. 2017.
- [36] Tanenbaum, Andrew S. *Computer networks, 5-th edition*. Prentice Hall, 2011.
- [37] Schneier, Bruce. *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, 1996.
- [38] Veinović, Mladen, and Saša Adamović. *Kriptologija 1 - 2018*. Univerzitet Singidunum, Beograd, 2018.
- [39] Milosavljević, Milan, and Saša Adamović. *Kriptologija 2 - 2017*. Univerzitet Singidunum, Beograd, 2017.
- [40] Van Tilborg, Henk CA, and Sushil Jajodia, eds. *Encyclopedia of cryptography and security*. Springer Science & Business Media, 2014.
- [41] Stamp, Mark. *Information security: principles and practice*. New York: Wiley, 2011.
- [42] Stamp, Mark, and Richard M. Low. *Applied cryptanalysis: breaking ciphers in the real world*. John Wiley & Sons, 2007.
- [43] Boneh, Dan, and Victor Shoup. *A graduate course in applied cryptography*. version 0.4, 2017. [Online], <https://crypto.stanford.edu/~dabo/cryptobook/> [Cited: 20.10.2019.]

- [44] Wagstaff Jr, Samuel S. *Cryptanalysis of number theoretic ciphers*. Chapman and Hall/CRC, 2003.
- [45] Gorbenko, Ivan, et al. *The research of modern stream ciphers*. 4th International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), IEEE, 2017.
- [46] Jindal, Poonam, and Brahmjit Singh. *A survey on RC4 stream cipher*. Journal of Computer Network and Information Security, 7: 37-45, 2015.
- [47] Ellis, Scott R. *A Cryptography Primer*. Computer and Information Security Handbook 2nd Edition: 25-46, Morgan Kaufmann, 2013.
- [48] Housley, Russell. *RFC 3686: Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)*. Tech. Rep., 2004.
- [49] Diffie, Whitfield, and Martin Hellman. *New directions in cryptography*. IEEE transactions on Information Theory: 644-654, 1976.
- [50] Kohnfelder, Loren M. *Towards a practical public-key cryptosystem*. PhD Thesis, Massachusetts Institute of Technology, 1978.
- [51] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. *A method for obtaining digital signatures and public-key cryptosystems*. Communications of the ACM, 1978.
- [52] Batten, Lynn Margaret. *Public key cryptography: applications and attacks*. John Wiley & Sons, 2013.
- [53] Azad, Saiful, and Al-Sakib Khan Pathan. *Practical cryptography: algorithms and implementations using C++*. Auerbach Publications, 2014.
- [54] Barker, Elaine, and Allen Roginsky. *Recommendation for cryptographic key generation*. NIST Special Publication (SP) 800-133 Rev. 1, National Institute of Standards and Technology, 2019.
- [55] Aryanti, Aryanti, and Ikhtison Mekongga. *Implementation of Rivest Shamir Adleman Algorithm (RSA) and Vigenere Cipher In Web Based Information System*. E3S Web of Conferences, Vol. 31. EDP Sciences, 2018.
- [56] Zhou, Xin, and Xiaofei Tang. *Research and implementation of RSA algorithm for encryption and decryption*. Proceedings of 2011 6th International Forum on Strategic Technology, Vol. 2. IEEE, 2011.
- [57] Schaefer, Edward. *An introduction to cryptography and cryptanalysis*. California's Silicon Valley: Santa Clara University: 4-5, 2009.
- [58] Barker, Elaine, et al. *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography*. NIST Special Publication (SP) 800-56B Rev. 2, National Institute of Standards and Technology, 2019.
- [59] Mišković, Aleksandar, and Mladen Veinović. *Comparative analysis of the Certification Authority in Serbia*. 19th Telecommunications Forum (TELFOR), Proceedings of Papers, IEEE, 2011. [18]

- [60] Kuhn, D. Richard, et al. *SP 800-32. Introduction to Public Key Technology and the Federal PKI Infrastructure*, 2001. [19]
- [61] Mrdović, Saša. *Izgradnja infrastrukture javnih ključeva (PKI)*. Magistarski rad, Elektrotehnički fakultet u Sarajevu, 2004. [20]
- [62] Chokhani, S., et al. *RFC 3647: Internet X. 509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, 2003. [21]
- [63] Housley, Russ, et al. *RFC 3280: Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile*, IETF, 2002. [22]
- [64] Kovinić, Milica et al. *Upotrebom digitalnih sertifikata do sigurnog pristupa servisima*. AMRES BPD 9 106, 2011. [23]
- [65] Prodanović, Radomir I., and Ivan B. Vulić. *Model for PKI interoperability in Serbia*. Vojnotehnički glasnik 65.2: 530-549, 2017. [24]
- [66] Milosavljević, Milan, and Vladislav Mišković. *Elektronska trgovina, 5. izdanje*. Univerzitet Singidunum, Beograd, 2019. [25]
- [67] Recommendation ITU-T X.509. *Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks*. 2019. [Online], <https://www.itu.int/rec/T-REC-X.509-201910-I/en> [Cited: 20.11.2019.] [26]
- [68] PGP Corporation. *An Introduction to Cryptography*. 2006. [Online], http://eval.symantec.com/mktginfo/downloads/PGP_Intro-to-Crypto_F.pdf [Cited: 15.11.2019.] [27]
- [69] Cooper, David, et al. *RFC 5280: Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile*. IETF, 2008.
- [70] Mišković, Aleksandar, and Srđan Atanasijević. *Analysis of the pull method for CRL list download by PKI simulation model*. Sinteza 2014 - Impact of the Internet on Business Activities in Serbia and Worldwide, Singidunum University Belgrade, 2014.
- [71] Veinović, Mladen, and Aleksandar Mišković. *Metode za proveru statusa i validnosti digitalnih sertifikata*. 10. naučni skup Sinergija, pp.53-58, Bijeljina, 2012. [28]
- [72] Santesson, Stefan, et al. *RFC 6960: X. 509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP*. 2013.
- [73] Chandramouli, Rajarathnam, Mehdi Kharrazi, and Nasir Memon. *Image steganography and steganalysis: Concepts and practice*. International Workshop on Digital Watermarking, Springer, Berlin, Heidelberg, 2003.
- [74] Simmons, Gustavus J. *The prisoners' problem and the subliminal channel*. Advances in Cryptology, Springer, Boston, MA, 1984.
- [75] Cox, Ingemar, et al. *Digital watermarking and steganography, second edition*. Morgan Kaufmann, 2007.

- [76] Walia, Ekta, Payal Jain, and Navdeep Navdeep. *An analysis of LSB & DCT based steganography*. Global Journal of Computer Science and Technology, 2010.
- [77] McAteer, Ian, et al. *Integration of biometrics and steganography: A comprehensive review*. Technologies 7.2: 34, 2019.
- [78] Cheddad, Abbas, et al. *Digital image steganography: Survey and analysis of current methods*. Signal processing 90.3: 727-752, 2010.
- [79] Sethi, Adarshpal S., and Vasil Y. Hnatyshin. *The practical OPNET user guide for computer network simulation*. Chapman and Hall/CRC, 2012.
- [80] Lu, Zheng, and Hongji Yang. *Unlocking the power of OPNET modeler*. Cambridge University Press, 2012.

Prilog

```
package org.acme.smartcard;

import org.acme.smartcard.domain.KeyStoreInfo;
import org.acme.smartcard.impl.ConfigServiceImpl;
import org.acme.smartcard.impl.CryptoServiceImpl;
import org.acme.smartcard.utils.FileIOUtils;

import java.nio.charset.StandardCharsets;
import java.security.KeyStore;
import java.security.PrivateKey;
import java.security.cert.X509Certificate;
import java.util.ArrayList;
import java.util.List;

public class Main {

    public static void main(String[] args) throws Exception {
        final String cfgLocation = "src/main/resources/config/pkcs11.cfg";
        final String keyType = "PKCS11";
        final char[] pin = {'3', '5', '1', '4'};

        // initializing personal ID as java KeyStore
        final ConfigService configService = ConfigServiceImpl.INSTANCE;
        configService.loadPkcsProvider(cfgLocation);
        KeyStore keyStore = configService.createKeyStore(pin, keyType);

        // getting right alias from java KeyStore
        final List<String> aliasList = new ArrayList<>();
        final List<KeyStoreInfo> infos = configService.readKeyStoreInfo(keyStore);
        for (final KeyStoreInfo info : infos) {
            final String alias = info.getAlias();
            aliasList.add(alias);
        }

        String alias = aliasList.get(1);

        // with cryptoService perform encryption and decryption
        CryptoService cryptoService = CryptoServiceImpl.INSTANCE;

        final String text = FileIOUtils.readFileIntoString( filePath: "src/main/resources/files/dummy.txt");

        // encrypting part of the code
        final X509Certificate cert = (X509Certificate) keyStore.getCertificate(alias);

        final byte[] encryptedData = cryptoService.encryptData(cert, transformation: "RSA", text.getBytes(StandardCharsets.UTF_8));

        // save encrypted file
        FileIOUtils.writeStringIntoFile(new String(encryptedData, StandardCharsets.UTF_8), filePath: "target/encryptedDummyFile.txt");

        // decrypting part of the code
        final String encryptedText = FileIOUtils.readFileIntoString( filePath: "target/encryptedDummyFile.txt");

        final PrivateKey privateKey = (PrivateKey) keyStore.getKey(alias, password: null);

        final byte[] decryptedData = cryptoService.decryptData(privateKey, transformation: "RSA/ECB/PKCS1Padding",
            encryptedText.getBytes());

        final String decryptedText = new String(decryptedData, StandardCharsets.UTF_8);

        // save decrypted data into the file
        FileIOUtils.writeStringIntoFile(decryptedText, filePath: "target/decryptedDummyFile.txt");

        // unload personal ID card
        configService.unLoadPkcsProvider();
        System.exit( status: 0);
    }
}
```

```

package org.acme.smartcard.impl;

import org.acme.smartcard.ConfigService;
import org.acme.smartcard.domain.KeyStoreInfo;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

import java.security.*;
import java.security.cert.X509Certificate;
import java.util.ArrayList;
import java.util.Enumeration;
import java.util.List;
import java.util.Objects;

/**
 * Singleton implementation of ConfigService
 *
 * @author Miskovic
 */
public class ConfigServiceImpl implements ConfigService {

    public static final ConfigServiceImpl INSTANCE = new ConfigServiceImpl();

    private static final Logger LOGGER = LoggerFactory.getLogger(ConfigServiceImpl.class);

    private String providerName;

    private ConfigServiceImpl() {

    }

    @Override
    public KeyStore createKeyStore(char[] pin, String keyType) throws Exception {
        LOGGER.info("Creating keystore of keyType {} ", keyType);
        final KeyStore keyStore = KeyStore.getInstance(keyType);
        keyStore.load(Stream.null(), pin);
        return keyStore;
    }

    @Override
    public void loadPkcsProvider(String config) {
        // final String config = "name = SmartCard\n" + "library = " + configPath;
        // LOGGER.info("Loading provider with config: {}", config);

        //final Provider provider = new SunPKCS11();
        final Provider provider = Security.getProvider("SunPKCS11");
        Provider configuredProvider = provider.configure(config);
        Security.addProvider(configuredProvider);

        this.providerName = provider.getName();
    }

    @Override
    public List<KeyStoreInfo> readKeyStoreInfo(KeyStore keyStore) throws Exception {
        final List<KeyStoreInfo> infos = new ArrayList<>();

        if (Objects.nonNull(keyStore)) {
            final Enumeration<String> aliasesEnum = keyStore.aliases();
            while (aliasesEnum.hasMoreElements()) {
                final KeyStoreInfo info = new KeyStoreInfo();

                final String alias = aliasesEnum.nextElement();
                info.setAlias(alias);
                LOGGER.info("Alias: {}", alias);

                final X509Certificate cert = (X509Certificate) keyStore.getCertificate(alias);
                info.setCert(cert);
                LOGGER.info("Certificate: {}", cert);

                final PrivateKey privateKey = (PrivateKey) keyStore.getKey(alias, password.null);
                info.setPrivateKey(privateKey);
                LOGGER.info("Private key: {}", privateKey);

                final PublicKey publicKey = cert.getPublicKey();
                info.setPublicKey(publicKey);
                LOGGER.info("Public key: {}", publicKey);

                infos.add(info);
            }
        }

        return infos;
    }

    @Override
    public void unloadPkcsProvider() {
        LOGGER.info("Unloading provider: {}", providerName);
        Security.removeProvider(providerName);
        this.providerName = null;
    }
}

```

```

package org.acme.smartcard.impl;

import org.acme.smartcard.CryptoService;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

import javax.crypto.Cipher;
import java.security.PrivateKey;
import java.security.PublicKey;
import java.security.cert.X509Certificate;
import java.util.Base64;
import java.util.Objects;

/**
 * Singleton implementation of CryptoService
 *
 * @author Miskovic
 */
public class CryptoServiceImpl implements CryptoService {

    public static final CryptoService INSTANCE = new CryptoServiceImpl();

    private static final Logger LOGGER = LoggerFactory.getLogger(CryptoServiceImpl.class);

    private CryptoServiceImpl() {

    }

    @Override
    public byte[] decryptData(PrivateKey privateKey, String transformation, byte[] base64Data) throws Exception {
        if (Objects.isNull(privateKey)) {
            throw new RuntimeException("Invalid input parameter. Parameter privateKey can not be null!");
        }

        if (Objects.isNull(base64Data)) {
            throw new RuntimeException("Invalid input parameter. Parameter base64Data can not be null!");
        }

        LOGGER.info("Start decrypting data...");
        final long startTime = System.currentTimeMillis();

        final byte[] decodedData = Base64.getDecoder().decode(base64Data);

        final Cipher cipher = Cipher.getInstance(transformation);
        cipher.init(Cipher.DECRYPT_MODE, privateKey);

        final byte[] decryptedData = cipher.doFinal(decodedData);

        final long totalTime = System.currentTimeMillis() - startTime;

        LOGGER.info("Decryption has finished. Time spent: {}", totalTime);

        return decryptedData;
    }

    @Override
    public byte[] encryptData(X509Certificate cert, String transformation, byte[] data) throws Exception {
        if (Objects.isNull(cert)) {
            throw new RuntimeException("Invalid input parameter. Parameter cert can not be null!");
        }

        if (Objects.isNull(data)) {
            throw new RuntimeException("Invalid input parameter. Parameter data can not be null!");
        }

        LOGGER.info("Start encrypting data...");
        final long startTime = System.currentTimeMillis();

        final PublicKey publicKey = cert.getPublicKey();

        final Cipher cipher = Cipher.getInstance(transformation);
        cipher.init(Cipher.ENCRYPT_MODE, publicKey);

        final byte[] encryptedData = cipher.doFinal(data);

        final byte[] encodedData = Base64.getEncoder().encode(encryptedData);

        final long totalTime = System.currentTimeMillis() - startTime;

        LOGGER.info("Encryption has finished. Time spent: {}", totalTime);

        return encodedData;
    }
}

```

```

package org.acme.smartcard.domain;

import java.security.PrivateKey;
import java.security.PublicKey;
import java.security.cert.X509Certificate;

public class KeyStoreInfo {

    private String alias;

    private X509Certificate cert;

    private PrivateKey privateKey;

    private PublicKey publicKey;

    public PublicKey getPublicKey() { return publicKey; }

    public void setPublicKey(PublicKey publicKey) { this.publicKey = publicKey; }

    public String getAlias() { return alias; }

    public void setAlias(String alias) { this.alias = alias; }

    public X509Certificate getCert() { return cert; }

    public void setCert(X509Certificate cert) { this.cert = cert; }

    public PrivateKey getPrivateKey() { return privateKey; }

    public void setPrivateKey(PrivateKey privateKey) { this.privateKey = privateKey; }
}

```

```
package org.acme.smartcard;

import org.acme.smartcard.domain.KeyStoreInfo;

import java.security.KeyStore;
import java.util.List;

public interface ConfigService {

    KeyStore createKeyStore(char[] pin, String keyType) throws Exception;

    void loadPkcsProvider(String configPath) throws Exception;

    List<KeyStoreInfo> readKeyStoreInfo(KeyStore keyStore) throws Exception;

    void unloadPkcsProvider();
}
```

```

package org.acme.smartcard;

import javax.crypto.Cipher;
import java.security.PrivateKey;
import java.security.cert.X509Certificate;

/**
 * Public API for encrypting and decrypting of various data formats.
 *
 * @author Miskovic
 */
public interface CryptoService {

    /**
     * @param privateKey - Private key that is used when decrypting data.
     * @param transformation - {@link Cipher} transformation (e.g. RSA/ECB/PKCS1Padding)
     * @param base64Data - The base64 encoded data that will be decrypted.
     * @return - Decrypted byte array
     * @throws Exception
     */
    byte[] decryptData(PrivateKey privateKey, String transformation, byte[] base64Data) throws Exception;

    /**
     * @param cert - Public certificate that is used for encrypting the data.
     * @param transformation - {@link Cipher} transformation (e.g. RSA)
     * @param data - Raw data that will be encrypted.
     * @return - Encrypted and base64 encoded byte array.
     * @throws Exception
     */
    byte[] encryptData(X509Certificate cert, String transformation, byte[] data) throws Exception;
}

```


UNAPREĐENJE PROTOKOLA ZA RAZMENU KLJUČEVA NA BAZI LIČNIH IDENTIFIKACIONIH DOKUMENATA POŠILJAOCA I PRIMAOCA

ORIGINALITY REPORT

4%

SIMILARITY INDEX

PRIMARY SOURCES

1	people.etf.unsa.ba Internet	246 words — 1%
2	www.singipedia.singidunum.ac.rs Internet	169 words — 1%
3	bpd.amres.ac.rs Internet	67 words — < 1%
4	www.singipedia.com Internet	59 words — < 1%
5	www.amres.ac.rs Internet	57 words — < 1%
6	www.bancaintesa.rs Internet	56 words — < 1%
7	Aleksandar Miskovic, Mladen Veinovic. "Comparative analysis of the Certification Authority in Serbia", 2011 19th Telecommunications Forum (TELFOR) Proceedings of Papers, 2011 Crossref	52 words — < 1%
8	viminacium.org.rs Internet	37 words — < 1%
9	217.24.23.93 Internet	33 words — < 1%

10	uprava.gov.hr Internet	33 words — < 1%
11	www.mingo.hr Internet	30 words — < 1%
12	naucniskup.sinergija.edu.ba Internet	19 words — < 1%
13	os2.zemris.fer.hr Internet	15 words — < 1%
14	www.pf.unsa.ba Internet	15 words — < 1%

EXCLUDE QUOTES ON
EXCLUDE BIBLIOGRAPHY ON

EXCLUDE MATCHES < 15 WORDS