



Univerzitet
Singidunum

**Departman za poslediplomske studije i međunarodnu saradnju
SAVREMENE INFORMACIONE TEHNOLOGIJE**

MASTER STUDIJE

ZAŠTITA PODATAKA NA PRENOSNIM MEDIJIMA

-Master rad-

mentor
prof. dr Mladen Veinović

student
Dejan Ubović
410339/2011

Beograd, 2012. godine

IZVOD

U ovom master radu opisani su osnovni tipovi prenosnih medija, njihova funkcija i rad. Pošto je njihova osnovna namena čuvanje podataka, te podatke je potrebno učiniti sigurnim, a i poverljivim, i zato su objašnjeni i principi poverljivosti, zaštite i kriptografije, odnosno šifrovanja tih podataka.

ABSTRACT

This masters paper gives a description of the basic types of transmission media, their function and operation. Since their basic purpose is data storage, it is necessary to have that data secure and confidential and hence in addition this paper explains the principles of confidentiality, protection and cryptography as well as data encryption.

SADRŽAJ:

1.	UVOD.....	1
2.	METODOLOGIJA ISTRAŽIVAČKOG PROJEKTA.....	3
	2.1. UVODNE NAPOMENE I OBRAZLOŽENJE RADA.....	3
	2.2. PREDMET ISTRAŽIVANJA.....	3
	2.3. CILJEVI I ZADACI ISTRAŽIVANJA	4
	2.4. ISTRAŽIVAČKE HIPOTEZE.....	4
	2.5. METODI ISTRAŽIVANJA I TOK ISTRAŽIVAČKOG PROCESA	4
3.	TIPOVI PRENOSNIH MEDIJA	5
	3.1. FLOPI DISK	5
	3.2. PRENOSIVI HARD DISK	6
	3.3. CD	8
	3.4. DVD	9
	3.5. USB FLEŠ DISK.....	10
	3.6. SMART KARTICE	12
	3.6.1. <i>ELEMENTI SMART KARTICA.....</i>	<i>13</i>
	3.6.2. <i>TIPOVI SMART KARTICA.....</i>	<i>15</i>
4.	POVERLJIVOST / KRIPTOGRAFIJA.....	17
5.	ISTORIJAT ZAŠTITE PODATAKA.....	18
6.	SAVREMENE TEHNIKE ZAŠTITE PODATAKA.....	21
	6.1. SISTEMI ŠIFROVANJA PODATAKA.....	21
	6.2. AUTENTIFIKACIJA I DIGITALNI POTPIS	26
	6.2.1. <i>FORMAT DIGITALNOG CERTIFIKATA.....</i>	<i>29</i>
7.	RSA ALGORITAM.....	32
8.	SOFTVER ZA ŠIFROVANJE DISKA.....	35
	8.1. POREĐENJE SOFTVERA ZA ŠIFROVANJE DISKA	35
	8.2. KORIŠĆENJE TRUECRYPT-A ZA ŠIFROVANJE DISKA	38
	8.3. KORIŠĆENJE TRUECRYPT-A ZA ŠIFROVANJE USB-A	46
	8.4. KORIŠĆENJE BITLOCKER-A ZA ŠIFROVANJE DISKA	53
9.	ZAKLJUČAK.....	58
10.	LITERATURA	60

1. UVOD

Razvoj informacionih tehnologija, telekomunikacionih sistema u poslednje tri decenije doživeo je ekstremni rast. Uporedo sa tim razvojem raste i mogućnost zloupotreba podataka koji se tim putem prenose. Brzi razvoj hardvera i softvera, koji se koriste za prenos podataka, uslovljava česte promene i usavršavanja istih. U toj trci proizvođači često nemaju vremena za detaljno testiranje opreme, jer će u vremenu kada klijenti primete potencijalne probleme tržište nuditi novu paletu proizvoda koja prevazilazi pomenute probleme. Usled nedovoljnog testiranja, često se javljaju propusti koji čine osnovu za rad potencijalnih napadača. Napadači razvijaju sopstvene alate i tehnike pomoću kojih zaobilaze sigurnosne mere i na taj način dolaze do „važnih“ podataka. U cilju eliminisanja ovih nedostataka nameće se novi pravac istraživanja u sferi sigurnosti informacionih sistema, koji se odnosi na zaštitu podataka od neovlašćenog pristupa, modifikacija ili različitih zloupotreba. Na važnost zaštite podataka ukazuje činjenica da je ona postala jedan od najvažnijih komponenata nacionalnih bezbednosti zemalja, državnih administracija, banaka i sl. Isto tako, veliki broj kompanija sve više poklanja pažnju merama sigurnosti sopstvenih informacionih sistema i podataka.

Podaci smešteni na CD/DVD medijima i USB memorijama najviše su podložni gubitku, u smislu da je u tim slučajevima najlakše fizički izgubiti i oštetiti medije na kojima se podaci nalaze. Pomenuti mediji se moraju čuvati na propisanim uslovima (temperatura, vlaga, osvetljenje) kako bi podaci bili zaštićeni tokom perioda zagarantovanog perioda koji je u slučaju CD-a deset godina. Ukoliko se medij ne čuva na pravi način, događa se ubrzana degradacija pod dejstvom svetlosti (oštećenje srebrnog filma na disku), vazduha (oksidacija srebrnog filma kiseonikom) i fizičkih oštećenjima prilikom transporta. Iako su USB memorije manje podložne hemijskim oštećenjima, mehanička oštećenja nisu retka.

Savremena preduzeća se sve više susreću sa problemima kao što su pojačana konkurencija, finansijska nestabilnost i nesigurnost tržišta, pa se kao imperativ nameće stalno smanjenje troškova poslovanja, tj. povećanje efikasnosti i produktivnosti. Jedan od načina za postizanje veće konkurentnosti je uvođenje i primena savremenih informacionih i telekomunikacionih tehnologija.

Svako poslovanje podrazumeva učešće dve ili više strana koje razmenjuju dobra, usluge ili informacije. Tradicionalni način poslovanja obuhvata razmenu mnoštva podataka, pre svega u „papirnom“ obliku, pa se do informacija dolazi sporo, uz velike troškove. Realizacija posla je takođe usporena, kao i izveštavanje. Primenom savremenih tehnologija u procesu razmene podataka moguće je značajno unaprediti efikasnost poslovanja.

Uporedo sa razvojem informacionih tehnologija i telekomunikacionih sistema raste i mogućnost zloupotreba podataka koji se tim putem prenose. Brzi razvoj hardvera i softvera, koji se koriste za prenos podataka, uslovljava česte promene i usavršavanja istih. U toj trci proizvođači često nemaju vremena za detaljno testiranje opreme. Usled nedovoljnog testiranja, često se javljaju propusti koji čine osnovu zarad potencijalnih napadača. Napadači razvijaju sopstvene alate i tehnike pomoću kojih zaobilaze sigurnosne mere i na taj način dolaze do „važnih“ podataka. U cilju eliminisanja ovih nedostataka nameće se novi pravac istraživanja u sferi sigurnosti informacionih sistema, koji se odnosi na zaštitu podataka od neovlašćenog pristupa, modifikacija ili različitih zloupotreba. Na važnost zaštite podataka ukazuje činjenica da je ona postala jedan od najvažnijih komponenata nacionalnih bezbednosti zemalja, državnih administracija, banaka i sl.

Kao najzastupljeniji medijum za prenos podataka se koriste računarske mreže. Kao takve logično predstavljaju usko grlo po pitanju sigurnosti informacija koje se tim putem prenose. Iz tog razloga, posebna pažnja posvećena je zaštiti podataka koji se prenose putem računarske mreže. Verifikacija dokumenata u savremenim komunikacionim sistemima često ne predstavlja siguran vid razmene poruka. Daleko bolje rešenje predstavljaju sistemi koji podržavaju međusobnu autentifikaciju obe strane u komunikaciji.

2. METODOLOGIJA ISTRAŽIVAČKOG PROJEKTA

Metodologija istraživanja je okosnica informativnih nauka i predstavlja sistem pravila i uputstva na koji se na način tačno izvode istraživanja. Metodologija najčešće sadrži način prikupljanja činjenica, sistematizaciju i obradu istih, interpretaciju rezultata i zaključak.

U medijima je objavljeno da je Američka vlada izgubila na desetine hiljada dolara po svakom neovlašćeno objavljenom dokumentu. Ako se zna da je poslednjih godina broj takvih dokumenata prerastao u stotine hiljada, lako se dolazi do zaključka da je zaštita podataka jedan od glavnih prioriteta Američke, ali i svake druge vlade. Briga o zaštiti podataka je jednako bitna i kod malih i srednjih preduzeća, kao i kod multinacionalnih gigantskih korporacija. Na žalost, vlasnici podataka često toga postaju svesni kada se objave njihove lične informacije, podaci, fotografije, prepisi, skripte, poslovni i lični kontakti, pa čak i nadoknadiivi podaci kao što su opisi podešavanja i informacije o internet protoku unutar kompanije.

2.1. UVODNE NAPOMENE I OBRAZLOŽENJE RADA

Tokom pisanja ovog rada sprovedeno je svojevrsno istraživanje koje je za rezultat imalo zaključak da je zaštita podataka gotovo podjednako važna kao i sadržina istih, ukoliko se radi o „osetljivim“ podacima.

Iako je ovaj rad oformljen na zadatu temu, može se korigovati kao svojevrsni priručnik o zaštiti podataka pa samim tim i aplikativnog softvera, fotografija, spisa, skripti i drugog digitalnog materijala. On sadrži bitne informacije koje bi mogle biti korisne pri bilo kakvoj zaštiti informacija i podataka u bilo kojoj formi.

2.2. PREDMET ISTRAŽIVANJA

U ovom radu su opisane metode kojima se efikasno štite podaci od neovlašćenog korišćenja, kopiranja, premeštanja, prikrivanja i trajnog brisanja. U ovom radu su pojašnjeni šifrovanje, sigurnosno kopiranje, maskiranje i brisanje podataka u cilju njihove zaštite.

Svaki od pomenutih načina ima svoje prednosti i mane. Tako na primer šifrovanje podataka štiti podatke od neovlašćenog pristupa, ali i otežava pristup autorizovanim osobama i zahteva više njihovog vremena. Kod pravljenja backup-a mora postojati redovna navika pravljenja kopija, a USB flash memorije su prečesto male, a CD diskovi nedovoljno pouzdani u trajnom očuvanju informacija. USB memorije velikih kapaciteta su pak skupe, ali ipak drastično jeftinije od gubitka informacija. Maskiranje podataka je veoma dobar način zaštite fajlova, ali autorizovana osoba mora prepoznati koji je fajl kako maskiran kako bi ga na pravi način iskoristila. Brisanje fajlova u potpunosti štiti od neželjenog korišćenja podataka, ukoliko govorimo o trajnom brisanju, ali zato ni autorizovano lice više ne može pristupiti istim.

2.3. CILJEVI I ZADACI ISTRAŽIVANJA

Zadatak ovog rada je da pronađe valjane načine za zaštitu podataka i da se na njima bazira.

Cilj ovog rada je da kroz teorijske i empirijske aktivnosti koje se odvijaju utvrđenim redosledom dođe do zaključaka koji su presudni za zaštitu podataka na prenosnim medijima kao što su CD, flash i prenosni hard diskovi.

2.4. ISTRAŽIVAČKE HIPOTEZE

Generalna ili opšta hipoteza:

Počinjemo od hipoteze da su prenosni podaci na prenosnim medijima najčešće nezaštićeni, što je i najčešći slučaj. PC magazin je prošle godine naveo da je 60% upropaštenih podataka u svakom radnom okruženju rezultat lošeg rukovanja sa prenosnim medijima, oko 20% je bio problem istekao rok medija (npr. za CD je taj rok oko 10 godina), 10% je nestalo kao rezultat loše kategorizacije i samo 10% upropašteno upadom neovlašćenog lica (fizički ili putem interneta) i neautorizovanim rukovanjem istim. Naša polazna hipoteza je da se svaki podatak može zaštititi jednom metodom zaštite ili čak koristeći više metoda.

2.5. METODI ISTRAŽIVANJA I TOK ISTRAŽIVAČKOG PROCESA

Osnovne metode:

Za potrebe istraživanja izvršena je analiza pomoću nekoliko izvora stručne literature, pojedinih internet portala o zaštiti podataka velikih bankarskih sistema, ali i razgovora sa ljudima na terenu koji imaju korist od praktične primene zaštite podataka.

Statističke metode:

U radu se koriste statistički podaci koji su javno dostupni i objavljeni bar jednom u štampanim i/ili elektronskim medijima.

Tok istraživačkog procesa:

Najpre je sprovedena analiza zaštite podataka koja se danas koristi. Potom su pojašnjene njihove karakteristike i objašnjeno je na koje se podatke to najčešće odnosi. Na kraju je dat zaključak o važnosti zaštite podataka pri korišćenju prenosnih medija, jer to ima poseban akcenat na njih.

3. TIPOVI PRENOSNIH MEDIJA

3.1. FLOPI DISK

Flopi disk je medijum za skladištenje sastavljen od tankog diska i fleksibilnog magnetnog medijuma za skladištenje, zatvoren u pravougaoni plastični nosač, obložen tkaninom, koja uklanja čestice prašine¹.

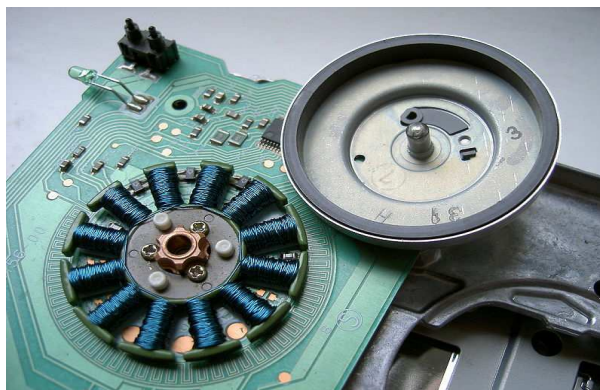
Flopi diskovi su počeli da se koriste 1980-ih i 1990-ih u personalnim računarima za distribuciju softvera, prenos podataka i kreiranje rezervnih kopija (backup). Pre nego što su hard diskovi postali dostupni, flopi diskovi su se često koristili za skladištenje operativnih sistema. Većina računara je imala primarni operativni sistem sačuvan kao ROM, sa mogućnosti učitavanja naprednijeg operativnog sistema sa flopi diska. Do ranih 1990-ih, povećanje veličine softvera zahtevalo je veće pakete kao što su Windows ili Adobe Photoshop, koji su zahtevali desetak i više disketa. Distribucija većih programa je postepeno zamenjena sa CD-ROM i online distribucijom (za manje programe).



Slika 3.1.1. Prikaz flopi diska u radu

Motor u flopi čitaču rotira magnetni medijum diskete određenom brzinom, dok stepper motor pomera magnetnu glavu za čitanje/pisanje preko površine diska. Obe operacije, čitanja i pisanja, zahtevaju da se medijum rotira i da magnetna glava dodiruje medijum, i to zahvaljujući 'disk load' solenoidu. Za upisivanje podataka, struja se šalje kroz kalem u magnetnu glavu, dok se medijum rotira. Magnetno polje glave poravnava magnetne čestice tačno ispod glave na medijumu. Kada struja promeni smer, čestice se poravnavaju u suprotnom smeru i kodiraju podatke digitalno. Za očitavanje podataka, magnetne čestice u medijumu izazivaju mali napon u kalemu, dok on prolazi ispod njega. Ovaj mali signal se pojačava i šalje u kontoler, koji konvertuje ovaj signal u podatke, proverava greške i prosleđuje ih dalje.

¹ http://en.wikipedia.org/wiki/Floppy_disk datum posete linka 22.6.2012. 13:15



Slika 3.1.2. Unutrašnjost flopi čitača

3.2. PRENOSIVI HARD DISK

Spoljni prenosivi hard diskovi se obično povezuju preko USB priključka. Uključi i koristi (Plug and play) opcija nudi kompatibilnost sistema, i funkcije velikog skladišta i prenosivog dizajna. Opcije eksternog hard diska su²:

- kloniranje diska
- skladištenje podataka
- backup fajlova i informacija
- skladištenje i pokretanje virtuelnih mašina
- pokretanje operativnihi sistema

Eksterni hard diskovi su dostupni kao 2.5 " i 3.5 ", a kapaciteti su u rasponu od 160GB do 2TB.

Hard disk je uređaj za skladištenje i preuzimanje digitalnih informacija, pre svega kompjuterskih podataka. Sastoji se od jednog ili više čvrstih brzo rotirajućih diskova, obloženih magnetnim materijalom, i od magnetnih glava uređenih da upisuju i očitavaju podatke sa površine diskova. Hard diskovi su klasifikovani kao digitalni magnetni uređaji za skladištenje podataka sa slučajnim pristupom³.

² http://en.wikipedia.org/wiki/External_hard_disk_drive#External_removable_drives datum posete linka 5.7.2012. 15:00

³ http://en.wikipedia.org/wiki/Hard_disk_drive datum posete linka 5.7.2012. 13:10

Magnetsko snimanje

Hard disk upisuje podatke, tako što magnetizuje tanak sloj feromagnetskog materijala na disku. Sekvencijalne promene u pravcu magnetizacije predstavljaju binarne bitove podataka. Podaci se očitavaju sa diska, tako što se detektuju prelazi u magnetizaciji.

Tipičan hard disk se sastoji od vretena, koji drži diskove. Diskovi su napravljeni od ne magnetnog materijala, obično legure aluminijuma, stakla ili keramike, i obloženi su tankim slojem magnetnog materijala, obično 10-20nm, sa spoljašnjim slojem od ugljenika za zaštitu. U današnjim hard diskovima, diskovi se okreću brzinom od 7200 obrtaja u minuti.

Informacije se očitavaju sa diska dok se okreće pomoću uređaja, koji se zove glava za čitanje i upisivanje, koja je na 10nm od magnetne površine. Za čitanje i upisivanje podataka glava se koristi za detekciju i izmenu magnetizacije materijala ispod nje. U današnjim hard diskovima postoji jedna glava za svaki disk na vretenu, montirana na zajedničku osovinu. Osovina pomera glave preko površine diskova, dok se okreću, omogućavajući glavama da pristupe celoj površini diska.

Magnetna površina svakog diska je konceptijski podeljena na više manjih mikrometarskih regiona, magnetnih domena, koji uglavnom imaju jedinstvenu magnetizaciju. Zbog polikristalne prirode magnetnog materijala, svaki ovaj magnetni region se sastoji od nekoliko stotina magnetnih zrna. Svaki magnetni region formira magnetni dipol, koji generiše magnetno polje. Glava za upisivanje magnetizuje region generisanjem jakog lokalnog magnetnog polja, a glava za očitavanje detektuje magnetizaciju regiona.

Tipičan hard disk ima dva električna motora: motor diska, koji vrti diskove i motor pokretača, koji pozicionira glavu za čitanje i upisivanje, slika 3.2. Motor diska ima spoljni rotor, koji je povezan na diskove, a namotaji statora su fiksirani na mestu. Naspram motora pokretača je glava za čitanje i upisivanje, a tanki štampani spoj kablova spaja glavu sa pojačavačem monitoranog na stožer pokretača.



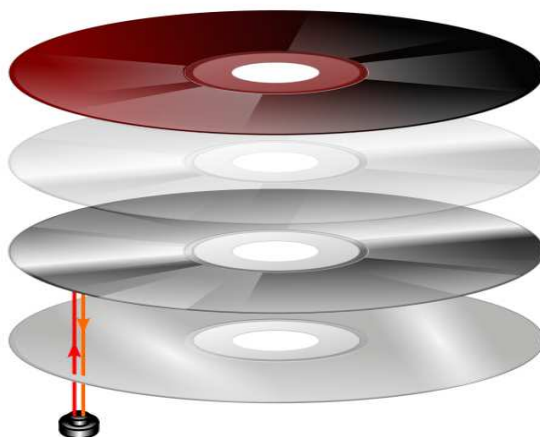
Slika 3.2. Unutrašnji izgled hard diska

3.3. CD

Kompakt disk ili CD je optički disk, koji služi za skladištenje digitalnih podataka. Prvobitno je razvijen za čuvanje i puštanje zvučnih zapisa, ali format je kasnije adaptiran za skladištenje podataka (CD-ROM), za upisivanje jednom audio zvuka i skladištenje podataka (CD-R), piši-briši medija (CD-RW), video kompakt diskova (VCD), super video (SVCD), PhotoCD, PictureCD.

Standardni CD ima prečnik od 120mm i može da uskladišti do 80 minuta nekompresovanog audio zvuka ili 700MB podataka. Mini CD ima različite prečnike u rasponu od 60 do 80mm, ponekad se koriste za CD singlove, i mogu da uskladište do 24 minuta audia ili za čuvanje dražvera za razne uređaje⁴.

CD je napravljen od 1,2mm debele polikarbonat plastike i težak je 15-20g. Od centra ka spolja, komponente su: centralna rupa (15mm), prvo prelazno područje (stezni prsten), područje spona (prsten spajanja), drugo prelazno područje, područje podataka i ivica. Područje podataka zahvata područje prečnika 25-58mm. Tanak sloj alumijuma, ili ređe zlata, se nanosi na plastičnu površinu čineći je reflektivnom. Metal je zaštićen slojem laka, a nalepnica se štampa na sloj laka, obično sitoštamptom ili ofset štamptom, slika 3.3.1.



Slika 3.3.1. Slojevi CD-a

Podaci na CD se čuvaju kao niz sitnih ureza, poznatih kao jame ('pits'), kodiranih u spiralnom putu presovanom u vrhu sloja polikarbonata. Oblasti između jama se zovu polja ('lands'). Svaka jama je oko 100nm duboka i 500nm široka, a dužina varira od 850 nm do 3.5 μ m. Dužina između pesama je 1.6 μ m.

Brzina skeniranja je 1.2-1.4m/s (približno 500 obrtaja u minuti na unutrašnjoj ivici diska, a oko 200 na spoljašnjoj ivici). Disk pušten ispočetka usporava tokom reprodukcije.

⁴ http://en.wikipedia.org/wiki/Compact_Disc datum posete linka 21.6.2012. 12:05

Očitavanje CD-a se vrši fokusiranjem lasera talasne dužine 750nm kroz dno polikarbonata. Promena u visini između jama i polja rezultuje razlike u načinu na koji se svetlost reflektuje. Meranjem intenziteta promena sa fotodiodom podaci mogu biti očitani sa diska.

Jame i polja ne predstavljaju direktno nule i jedinice u binarnim podacima, već promena sa jame na polje i polja na jamu predstavlja jedinicu, a ako nema promene očitava se kao nula. Mora postojati najmanje dve ili ne više od deset nula između jedinica, što je određeno dužinom jame.



Slika 3.3.2. Mehanički delovi CD čitača

3.4. DVD

DVD je format optičkog diska za skladištenje, i nudi veći kapacitet skladištenja od CD, a ima iste dimenzije.

Već snimljeni DVD su masovno proizvedeni korišćenjem mašina za oblikovanje, koje su fizički štampale podatke na DVD. Takvi diskovi su poznati kao DVD-ROM, zato što mogu samo da se očitavaju, ne mogu da se brišu niti ponovo upisuje na njih. Prazni DVD diskovi (DVD-R i DVD+R) mogu se narezati pomoću DVD rekordera, a potom koristiti kao DVD-R. Ponovno ispisivi (piši/briši) DVD (DVD-RW, DVD+RW i DVD-RAM) mogu biti narezani i obrisani više puta.

3.5. USB FLEŠ DISK

USB fleš disk je uređaj za skladištenje podataka, koji sadrži fleš memoriju integrisanu sa USB interfejsom. USB fleš diskovi su obično ponovo ispisivi i uklonjivi, i fizički manji od flopi disketa, i većina je teška oko 30g. Od septembra 2011. dostupni su u veličinama od 256GB, a planiraju se i veći od 2TB, koji će zahtevati poboljšanja u veličini i ceni po kapacitetu. Neki dozvoljavaju i do 100 000 upisivanja i brisanja, u zavisnosti od tipa memorijskog čipa.

USB fleš diskovi se koriste za iste namene, za koje su se koristile diskete i diskovi. Oni su manji, brži, imaju više hiljada puta veći kapacitet, i više su izdržljiviji i pouzdani, jer nemaju pokretnih delova. USB diskovi sa USB 2.0 podrškom mogu da uskladište mnogo podataka i da ih prenose mnogo brže od nekih većih optičkih diskova, CD-RW i DVD-RW, i mogu biti očitani u bilo kojim drugim sistema, kao npr. Xbox 360, Playstation 3.

U fleš disku se ništa ne pomera mehanički, a termin disk se koristi, jer kompjuter očitava i upisuje podatke u njega istim sistemskim komandama, kao i za mehaničke. Njegovo skladište se u kompjuterskom sistemu prikazuje kao još jedan uređaj.

Fleš disk se sastoji od malih štampanih ploča, koji nose elemente kola i USB konektor, i izolovan je i zaštićen unutar plastike, metala ili gumiranog kućišta, i može se nositi u džepu ili kao privezak na ključevima. USB konektor može biti zaštićen poklopcem ili da se uvlači u plastično telo, mada nije verovatno da se može oštetiti ako je nezaštićen. Većina fleš diskova koristi standardni tip A USB konekcije, omogućavajući priključivanje u portove na svim računarima, ali postoje i diskovi za druge interfejse. USB diskovi koriste napajanje iz računara, koristeći USB konektor. Neki uređaji kombinuju audio plejer sa USB flešom, ali oni zahtevaju bateriju samo kad se sluša muzika.

Na USB disku jedan kraj je opremljen sa jednim USB konektorom A standarda, a unutar plastičnog kućišta se nalazi mala štampana ploča, koja sadrži naponska kola i mali broj integrisanih kola na površini. Obično jedan od ovih integrisanih kola obezbeđuje vezu između USB konektora i ugrađene memorije, dok je ostalo fleš memorija.

Osnovne komponente:

Obično postoje 4 dela fleš diska:

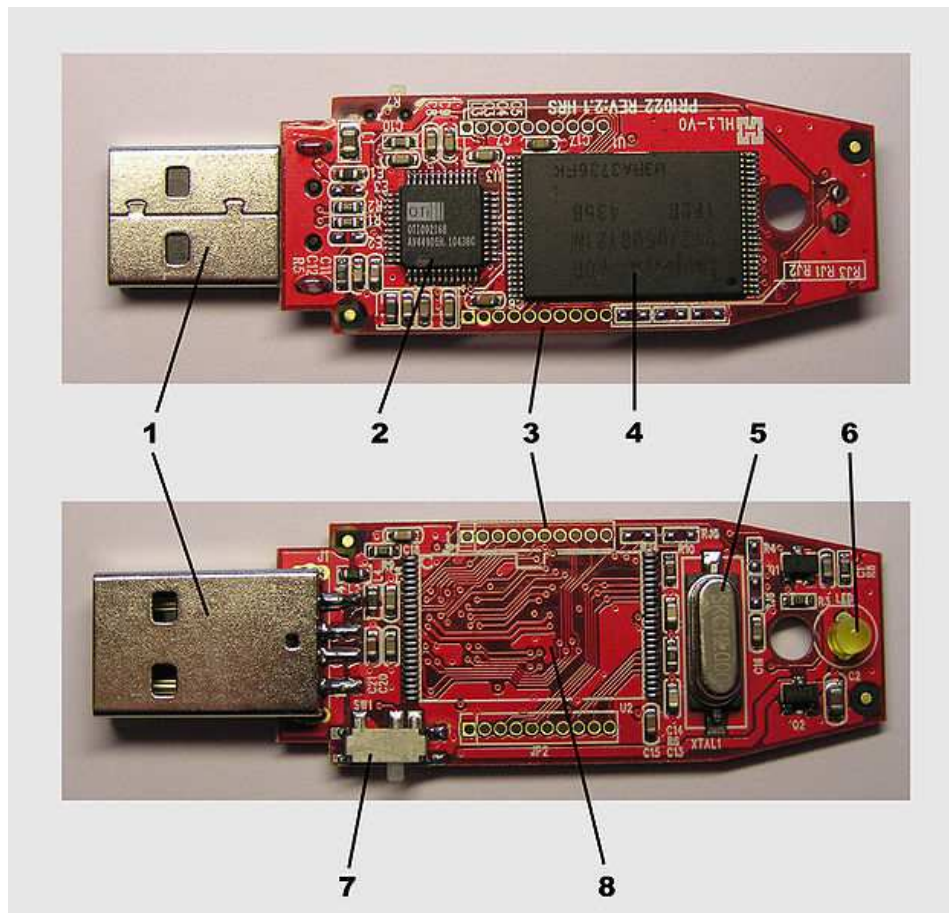
- USB priključak – omogućava fizičko povezivanje sa računarom,
- Kontroler USB skladišta – mali mikrokontroler, sa malim brojem ROM i RAM,
- NAND čip fleš memorije – čuva podatke,
- Kristalni oscilator – proizvodi klok signal na 12MHz, i kontroliše izlaz podataka pomoću zatvorene fazne petlje.

Dodatne komponente:

Tipičan uređaj može da sadrži i:

- LED – ukazuje na protok podataka, upisivanje ili očitavanje,
- Prekidač za zaštitu upisivanja – dozvoljava ili ne dozvoljava upis u memoriju,

- USB poklopac – smanjuje rizik od oštećenja, sprečava ulazak prašine, dok neki fleš diskovi mogu i da se uvlače,
- Transportni dodaci – poklopac ili telo mogu da imaju rupu, tako da se USB može okačiti npr. na privezak za ključeve.



Slika 3.5. Komponente fleš diska: 1. USB priključak 2. Kontroler 3. Test tačke 4. Čip memorije 5. Kristal oscilator 6. LED 7. Prekidač za zaštitu od upisivanja 8. Prostor za drugi čip memorije

Fajl sistem:

Većina fleš diskova je formatirana sa FAT12, FAT16 ili FAT32 fajl sistemima. Svepristupnost ovih sistema omogućava da se disk može priključiti na bilo koji uređaj sa USB podrškom. Standardne FAT funkcije održavanja mogu biti iskorišćenje za popravku ili povraćaj oštećenih podataka. Pošto se u računaru fleš diskovi pojavljuju kao hard diskovi priključeni preko USB, fleš disk može biti formatiran sa bilo kojim fajl sistemom, koji podržava računar.

Fleš diskovi mogu biti defragmentirani. Postoji mišljenje da defragmentacija donosi malu prednost i povećava performanse (jer ne postoji mehanička glava, koja ide od fragmenta do fragmenta,

i uglavnom zbog poboljšanog keširanja grupisanih podataka), a i da defragmentacija smanjuje/skraćuje životni vek, praveći nepotrebne upise.

Neki fajl sistemi su dizajnirani da raspodele korišćenje preko celog memorijskog uređaja, bez koncentracije upotrebe na samo jedan deo (npr. folder). Ovo „jednaka distribucija“ još više produžava život jednostavnih fleš memorija.

Sektori u fleš memoriji su dugi 512 bajtova, zbog kompatibilnosti sa hard diskovima, i prvi sektor može da sadrži master boot, i zbog toga USB diskovi mogu biti izdvojeni na particije, kao i hard diskovi.

3.6. SMART KARTICE

Smart Card ili tzv. 'Pametna kartica' je plastična kartica veličine obične kreditne kartice kakve su nam prisutne u svakodnevnom životu, s tim da u sebi ima ugrađen čip na kojem se nalaze procesor, memorija (RAM i ROM) i sklopovi koji omogućavaju komunikaciju odnosno razmenu podataka s okolinom. Čip je upravo ono što ove kartice čini pametnima. Ova veza između plastične kartice i mikroprocesora omogućava nam da se nezamisliva količina podataka može sačuvati, očitati i obraditi bilo online ili offline. Pametne kartice (Smart Card) mogu sačuvati nekoliko stotina puta više podataka nego dosadašnje obične kartice s magnetskom trakom. Informacija ili aplikacija sačuvana na čipu u kartici prenosi se pomoću ugrađenog sklopa do terminala ili čitača kartice. Bezkontaktna pametne kartice imaju u sebi ugrađenu antenu s kojom bežično komuniciraju s čitačem kartica, koji takođe ima sličan takav modul, čime se postiže veća komfornost i fleksibilnost. U zavisnosti od toga kakav je čip ugrađen u karticu razlikujemo dva tipa kartica: memorijske kartice i procesorske kartice.

Memorijske kartice su one kod kojih je u čip ugrađena samo memorija. Takve memorijske kartice mogu sačuvati i do hiljadu puta više podataka od običnih kartica sa magnetskom trakom. Zbog sigurnosnih razloga primena ovakvih kartica ograničena je na one aplikacije kod kojih sigurnost podataka ne igra veliku ulogu. Ovakve kartice obično se koriste u jednostavnim aplikacijama kao što su npr. telefonske čip kartice.

Procesorske kartice su kartice, koje osim memorije na čipu imaju ugrađen mikroprocesor, pa prema tome mogu obavljati različite funkcije kao što su npr. šifrovanje podataka, napredna sigurnost podataka (informacije), lokalna obrada podataka, kompleksne operacije nad podacima itd. Zbog svoje velike sigurnosti većina kartica koje sadrže poverljive podatke, su tipa procesorskih pametnih kartica.

Pametne kartice mogu biti identifikacione kartice koje koriste da bi se dokazao identitet vlasnika kartice. Mogu biti zdravstvene kartice na kojima se može čuvati istorija bolesti pacijenta. Pametna kartica može da služi kao kreditna ili debitna kartica, pa se mogu obavljati offline transakcije. Sve ove primene zahtevaju sigurno čuvanje podataka kao što su biometrijski podaci, istorije bolesti pacijenta, tajni broj kreditne kartice i razni ključevi za šifrovanu autentičnost.

Zbog dodatne procesorske inteligencije, veličine i mogućnosti obrade podataka, kartica može pružiti veću sigurnost i stoga ima veliku primenu u različitim područjima. Trenutno se pametne kartice koriste za plaćanje telefonskih poziva, pri plaćanju parkiranja i putarina, čuvanje poverljivih podataka, za pristup satelitskim televizijskim programima i u mnogim drugim aplikacijama.

Fizička struktura pametne kartice određena je od strane International Standards Organization (ISO). Sastoji se od tri osnovna elementa. Plastična kartica je najosnovniji element i ima dimenzije 85,6 mm×53,98 mm×0,80 mm. Integrisani čip i kontakti ugrađeni su na karticu.

Sposobnost pameti kod Smart kartica leži upravo u integrisanom krugu. Tipično se integrisani krug sastoji od mikroprocesora, ROM memorije, radne memorije (RAM) i električno izbrisive programabilne ROM memorije (EEPROM), koja će pamti svoje stanje i kad napajanje nestane. Čip na kartici napravljen je na silicijumu, što povlači činjenicu da nije fleksibilan i lako se lomi. Kako se čip ne bi uništio prilikom savijanja kartice njegova veličina je smanjena na svega par milimetara. Veličina, debljina i fleksibilnost prilikom savijanja dizajnirani su tako da zaštite karticu od fizičkog oštećenja. S druge strane to ograničava veličinu memorije i procesorske resurse, koji su na kartici. Zbog ovih ograničenja moraju postojati sklopovi koji se nalaze izvan kartice (npr. u čitaču) npr. napajanje, podaci o vremenu i datumu itd. Ova ograničenja mogu smanjiti nivo sigurnosti, jer su obično ti sklopovi u nekim okolnostima nesigurni i podložni napadima od strane hakera.

3.6.1. ELEMENTI SMART KARTICA

Smart kartice imaju ista osnovna tri elementa kao i svi ostali računarski sastavi: procesorsku snagu, čuvanje podataka i sredstva koja se bave ulazom i izlazom podataka.

Procesorska snaga je obično mikroprocesorski chip (npr. Intel 8051 i Motorola 6805), a čuvanje podataka je izvedeno pomoću memorijskog čipa (EEPROM, FLASH, ROM, RAM). U većini Smart kartica su ovi resursi ukombinovani u jedan čip. Prenos podataka varira od kartice do kartice, zavisno od namene. Da bi kartica mogla raditi mora imati i izvor napajanja koji je obično čitač kartice ili se nalazi na kartici.

- Mikroprocesor

Mikroprocesor je inteligentni element Smart kartice koji manipuliše podacima i vrši njihovu interpretaciju. Softver koji je zadužen za interpretaciju i manipulaciju podacima može biti upisan u memoriju prilikom proizvodnje kartice ili naknadno upisan pod kontrolom mikroprocesora. Mikroprocesori u Smart karticama mogu biti 16-bitni i raditi na taktu od 10 MHz.

- Memorija

Memorija u pametnim karticama može biti ili retko promenjiva (non-volatile), zadržavajući podatke nakon nestanka napajanja, ili promenjiva (volatile) kod koje podaci nestaju nakon nestanka napajanja. U tom slučaju Smart kartica bi zahtevala bateriju za napajanje. Memorija isto tako može biti takva da dozvoljava čitanje iz nje i pisanje u nju (RAM) ili pak samo čitanje iz nje (ROM). U većini slučajeva Smart Card aplikacije zahtevaju ne promenjivu memoriju za čuvanje podataka tipa identiteta vlasnika kartice i aplikacijskog softvera i promenjivu memoriju za ažuriranje sačuvanih podataka kao što je npr. stanje bankovnog računa nakon transakcije.

Memorije u Smart karticama se mogu podeliti u tri grupe: ROM, RAM i programabilni ROM (PROM). ROM memorija je nepromenjiva i njen sadržaj je u nju upisan prilikom proizvodnje. Jednom upisan, sadržaj se više ne može menjati. U Smart karticama prisutne su memorije od otprilike 32kB. RAM memorije su promenjive i služe samo za privremeno čuvanje podataka jer se podaci nakon nestanka napajanja iz nje brišu. Podaci se u RAM mogu upisivati, biti

čitani, menjani, i brisani. U Smart karticama je raspoloživo 64 kB RAM memorije. Postoje dve vrste programabilnih ROM memorija (PROM): električno programabilne ROM (EPROM) i električno izbrisive programabilne ROM (EEPROM) memorije. Za razliku od EPROM-a, EEPROM se može reprogramirati, ali mu je zato struktura mnogo složenija, što ga čini mnogo skupljim. Raspoloživo je oko 8 kB EEPROM memorije. Memorija može biti struktuirana tako da omogućava različite nivoe zone sigurnosti. Otvorena zona sigurnosti sadrži podatke koji nisu poverljivi npr. identitet vlasnika. Tajna zona memorije sadrži poverljive podatke (npr. PIN) pa je nedostupna svima, osim procesoru koji proverava taj broj sa brojem koji unosi korisnik. Na taj način poverljivi podaci nikada ne izlaze iz kartice.

- Ulaz/izlaz

Postoji više načina da se podaci prenesu u karticu ili da se iz nje pročitaju. Kontaktne kartice obično sadrže metalne kontakte na površini kartice, koji, kad su ubačeni u čitač, povezuju unutrašnjost kartice sa spoljnim svetom. Bezkontaktne kartice koriste neku od bežičnih tehnologija prenosa podataka, što zahteva da se kartica mora nalaziti u blizini uređaja koji vrši upis podataka. Super Smart kartice imaju integrisanu tastaturu i mali displej i prema tome im nije potreban neki uređaj za prenos podataka, već se podaci mogu uneti od strane korisnika. Ovakve vrste kartica imaju ipak kontakte, koji im omogućuju da komuniciraju s drugim uređajima takvog tipa.

- Izvori napajanja

Postoje tri metode napajanja Smart kartica. To su:

• Iz spoljnog izvora napajanja preko kontakata

U ovoj metodi energija je poslata kartici preko dva kontakta koja se nalaze na površini, kada se kartica ubaci u uređaj, koji zatim vrši pisanje/čitanje podataka. Nakon ubacivanja u uređaj kartica će se sama resetovati i početi izvršavati program u memoriji, koji će početi komunicirati.

• Iz spoljnog izvora napajanja prenosom energije

U ovoj metodi, bežičnim putem, kao npr. induktivnom vezom, će se preneti energija koja će biti dovoljna da pobudi u kartici nekakav proces, koji će izvršiti neku kratku operaciju i zatim se ugasiti. Da bi ovo bilo moguće kartica se mora nalaziti u neposrednoj blizini tog uređaja kako bi prenos energije bio učinkovit.

• Iz baterije koja je ugrađena u karticu

U ovoj trećoj metodi, baterija je sastavni deo kartice i kartica se iz nje napaja. Ova metoda nije popularna zbog teškoća koje nastaju u zadovoljavanju ISO standarda, a odnose se na dimenzije, težine, i troškova koji rastu s ugrađivanjem baterije u karticu⁵.

⁵ Seminarski rad, Smart card, Fakultet elektrotehnike i računarstva ZESOI, 2004.

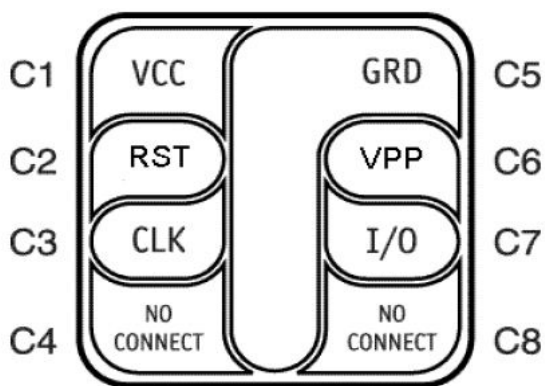
3.6.2. TIPOVI SMART KARTICA

Zavisno od toga kako se kartici pristupa, Smart kartice se mogu podeliti u 4 glavne grupe:

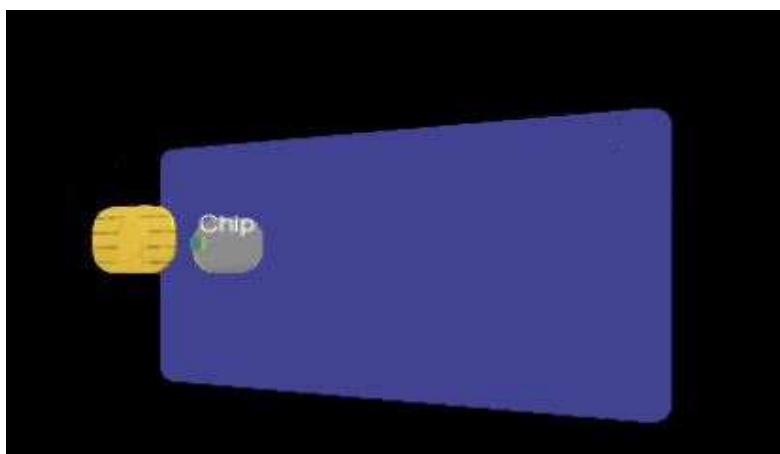
Kontaktne Smart kartice

Ove kartice imaju svu mikroelektroniku ugrađenu u unutrašnjost kartice u obliku jednog čipa, veličine oko 10 mm, kojem su zlatni kontakti izvedeni na površinu kartice. Kontakti omogućuju povezanost spoljne jedinice (Smart Card Reader) što omogućuje da neki uređaj uspostavi komunikaciju i prenese energiju do mikroelektronike u čipu.

Ima ukupno 8 kontakata: Dva su rezervisana za napajanje (VCC, GND), jedan za signal takta (CLK), jedan za reset (RST), dva se koriste za komunikaciju (I/O, CS), a dva su unapred rezervisana i ne koriste se, slika 3.6.1. Mnoge kartice imaju još i magnetsku traku na poledini radi kompatibilnosti s postojećom opremom. Znači integrisani krug treba da ima napajanje, signal takta koji upravlja procesorom i vezu s koje će primiti odnosno na koju će slati podatke. Kod ove vrste kartica ovo se postiže preko kontakata.



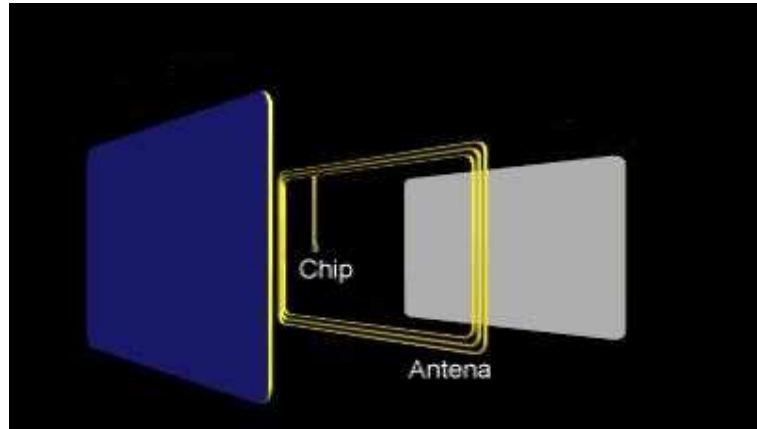
Slika 3.6.1. Položaj kontakata na kontaktnoj kartici



Slika 3.6.2. Kontaktne kartice

Bezkontaktne Smart kartice

Bezkontaktne Smart kartice imaju ugrađenu neku vrstu antene i umesto kontaktne veze koriste nekakvu vrstu elektromagnetskog povezivanja, slika 3.6.3. Kako prenos energije opada s udaljenošću, kartica se mora nalaziti u blizini čitača, na otprilike 3 cm. Induktivna ili kapacitivna veza se koristi kao način prenosa energije i podataka na karticu. Signal takta može biti interno izveden, a ulazno/izlazna komunikacija se može ostvariti pomoću jedne od vrsta modulacija.



Slika 3.6.3. Bezkontaktna kartica

CombiCard

Combi Card je kombinacija kontaktnih i bezkontaktnih kartica spojenih u jednu karticu, pa se time ostvaruje primena Smart kartica na bilo koji sistem. Ova kartica ima još kao dodatak magnetsku traku sa strane, dvodimenzionalni ili jednodimenzionalni bar kod, pa je kartica multiaplikacijska i primenljiva na postojeće sisteme.

Super Smart Card

Tipovi Smart kartica koji su opisani do sada bili su pasivni tipovi kartica koji su zahtevali spoljni izvor napajanja i terminal koji je vršio upis i ispis podataka. Ovo ograničenje utiče na primenu u određenim aplikacijama. Npr. svaki pasivni sistem Smart kartica mora da osigura raspoloživost terminala u planiranom području primene. Ovo je dovelo do razvoja treće generacije aktivnih Smart kartica poznatih pod nazivom Super Smart kartice. Super Smart kartice sadrže tastaturu i LCD display direktno na površini kartice. Ovakva kartica može biti potpuno samostalna (stand-alone) jedinica ili se može priključiti na računar, iz čega možemo zaključiti da ima i površinske kontakte koji joj to omogućavaju. Mane ovakvih tipova kartica je visoka cena proizvodnje u poređenju sa drugim Smart karticama, problemi koji se javljaju u zadovoljavanju ISO standarda i relativno mala veličina ugrađene tastature.

Glavna karakteristika Super Smart kartica je mogućnost offline rada i samoproveravanja. Za razliku od terminalno zavisnih pasivnih kartica Super Smart kartica se može koristiti na bilo kojem mestu i bilo koje vreme.

4. POVERLJIVOST / KRIPTOGRAFIJA

Poverljivost je mehanizam koji koristi postupak kriptografije kako bi se zaštitila informacija od neovlašćenog pristupa. Npr. običan tekst je pretvoren u šifrovani oblik pomoću nekog algoritma, a zatim dešifrovan u običan tekst istim postupkom. Kriptografija je metoda pretvaranja podataka iz oblika, koji je čitljiv ljudima u neki drugi oblik, a zatim nazad u njegov originalni čitljiv oblik, kako bi se otežao pristup neovlašćenim osobama.

Kriptografija se koristi u sledećim slučajevima:

- U osiguravanju privatnosti podataka, šifrovanjem podataka,
- U osiguravanju integriteta podataka, prepoznavanjem da li su podaci bili podvrgnuti neovlašćenom postupku,
- U osiguravanju jedinstvenosti podataka, proveravanjem da li je poruka originalna ili je kopija originala.

Pošiljalac u originalnu poruku dodaje neki jedinstveni identitet, koji primalac zatim proverava. Originalni podaci mogu biti obliku koji je čitljiv ljudima, kao npr. tekst datoteka, ili u obliku koji prepoznaju računari, kao npr. baza podataka, tablica ili slika. Originalni podaci se nazivaju nešifrovani podaci ili običan tekst. Podaci koji su podvrgnuti postupku kriptografije nazivaju se šifrovani podaci ili šifrovan tekst. Proces koji pretvara podatke u šifrovane naziva se šifrovanje, a obrnuti postupak, dakle pretvaranje šifrovanih podataka u originalni oblik naziva se dešifrovanje. Da bi se podaci mogli pretvoriti iz jednog oblika u drugi, potrebno je imati šifrovani algoritam i ključ. Ako je isti ključ korišćen za šifrovanje i dešifrovanje, on se naziva simetrični ključ, a algoritam je prema tome simetrični. Najpoznatiji simetrični algoritam je DES (Data Encryption Standard). DES simetrični algoritam je izmišljen u IBM-u 1970. god. Ovaj algoritam je bio proučavan od strane kriptografa više od 20 godina, i za to vreme nije bilo nikakvih metoda koje bi omogućile probijanje ove kriptografije. DES algoritam ima 56-bitni ključ. Kod simetričnog šifrovanja podataka problem predstavlja razmena ključeva, koji se koriste za šifrovanje i dešifrovanje podataka. Kako se za oba postupka koristi isti ključ, pošiljalac poruke mora primaocu poslati ključ s kojim je poruka šifrovana. Ako je taj ključ poslat preko mreže to ugrožava sigurnost komunikacije. Trostruki DES (Triple-DES) metoda šifrovanja koristi postojeći DES algoritam na poseban način kako bi se poboljšala sigurnost. Trostruki DES algoritam može biti izveden s dva ili tri ključa, zavisno od primene. Pošto algoritam obavlja šifrovanje-dešifrovanje-šifrovanje, često se naziva EDE algoritam. Ako su različiti ključevi korišćeni za šifrovanje i dešifrovanje, algoritam se naziva asimetrični algoritam. Asimetrično šifrovanje ima par ključeva, pri čemu se jedan ključ koristi za šifrovanje, a komplementaran ključ iz para se koristi za dešifrovanje. Na taj način svaki korisnik može objaviti jedan ključ (naziva se javni ključ), a drugi ključ ostaje poznat samo njemu (tajni ključ). Kada pošiljalac želi poslati poruku može je šifrovati javnim ključem primaoca poruke. Tada poruku može pročitati samo primaoc kome je namenjena, a sigurnost ključa nije dovedena u pitanje, jer se tajni ključ ne šalje mrežom. Uprkos ovoj očiglednoj sigurnosnoj prednosti, asimetrično šifrovanje se retko koristi, jer je algoritam puno sporiji od simetričnog šifrovanja. Najpoznatiji asimetrični algoritam je RSA, nazvan po svoja tri autora (Rivest, Shamir i Adleman). Kako bi imali prednosti oba tipa šifrovanja (simetričnog i asimetričnog), moderni sigurnosni mehanizmi koriste simetrično šifrovanje za šifrovanje dokumenata. Šifrovanje koristi slučajno generisan ključ koji se tada šifruje asimetričnim algoritmom i šalje zajedno s porukom. Na taj način je ključ zaštićen, a dokument se može dešifrovati bržim algoritmom.

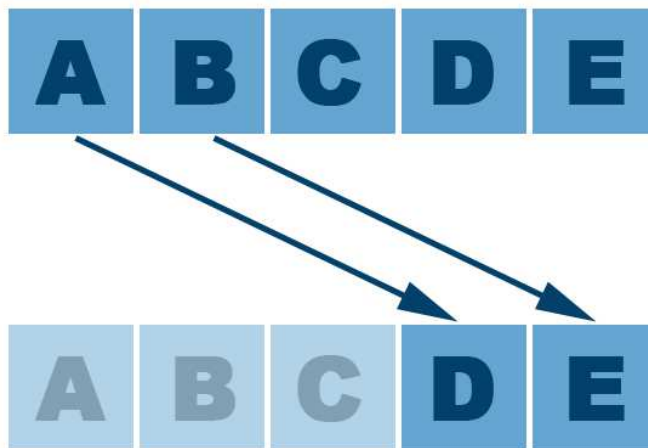
5. ISTORIJAT ZAŠTITE PODATAKA

Od najranijih početaka ljudskog postojanja postojala je potreba za razmenom informacija. Od početka čovekove komunikacije i postanka informacija koje su se verbalno prenosile, postojala je i razmena informacija koje nisu bile namenjene široj javnosti. Istorijat govora čak tvrdi da je šapat postao pre govora i da su čak i provobitne informacije štićene šapatom.

Istoričari veruju da su prve šifrovane poruke nastale u Neolitu kada su putem rasporeda kamenja praistorijski ljudi jedni drugima slali informacije o lokaciji potencijalnog plena, ali tako da je samo odabrani krug ljudi mogao to da razume. Ipak, neolitske šifrovane poruke nisu temeljno dokazane, pa se smatraju pretpostavkama.

Ipak, prvi zapis za koji se može sa sigurnošću reći da je zaštićen je nastao 1900. godine pre nove ere u Egiptu, a napisan je tako da su prva i poslednja slika u svakom segmentu zamenile mesta, a njihovim povratkom na pravo mesto zapis potpuno menja značenje. Način šifrovanja se vremenom menjao, pa su nekad sve slike u jednom segmentu izmenile mesta po određenom rasporedu. Iako su savremeni istoričari dešifrovali ove hijeroglife, nisu sa sigurnošću mogli da tvrde zašto su te informacije šifrovane.

Verovatno prvi širokoprimenljivi način šifrovanja pre nove ere je zasluga Julija Cezara, koji je šezdesete godine pre nove ere šifrovao poruke po sistemu „plus 3”.



Slika 5.1. Šifrovanje po sistemu „plus 3”

Za ljude koji nisu znali za „plus 3” pravilo poruke su delovale potpuno nečitljivo. Cezar je tako vršio prepiske sa vođama svoje vojske na bojnom polju, ali tako da niko od kurira, pa ni Cezarevo najuže okruženje nisu znali šta je u porukama pisalo. Jedina mana čitavog sistema je to što je neko slovo uvek menjano istim znakom, pa je tako bilo moguće uz dosta vremena i

kombinacije dešifrovati poruke koje je slao Cezar. Iako to šifrovanje nije bilo bez mana, zadržalo se u upotrebi vojne službe skoro čitav milenijum.

Prvu upamćenu raspravu o zaštiti podataka na čitavih dvadeset i pet stranica napisao je Leone Batista Alberti davne 1467. godine. On je takođe prvi izumitelj koji je doveo do svojevrzne automatizacije šifrovanja poruka kreiranjem njegovog čuvenog kriptografskog kruga. Svako slovo se po tom kriptografskom krugu menjalo sa nekim drugim slovom, pa je tako, na primer, slovo A uvek zamenjeno sa slovom S, itd.

Kriptografija je često korišćena u službi Katoličke crkve, a najplastičniji primer toga je nomenklator – kombinacija supstitucije abecede i malog koda koji je na zahtev pape Klementa VII načinio Garbijel Di Lavinde. Ova šifra je bila toliko uspešna u zaštiti podataka da je ostala u upotrebi narednih 450 godina u potpunosti nepromenjena.

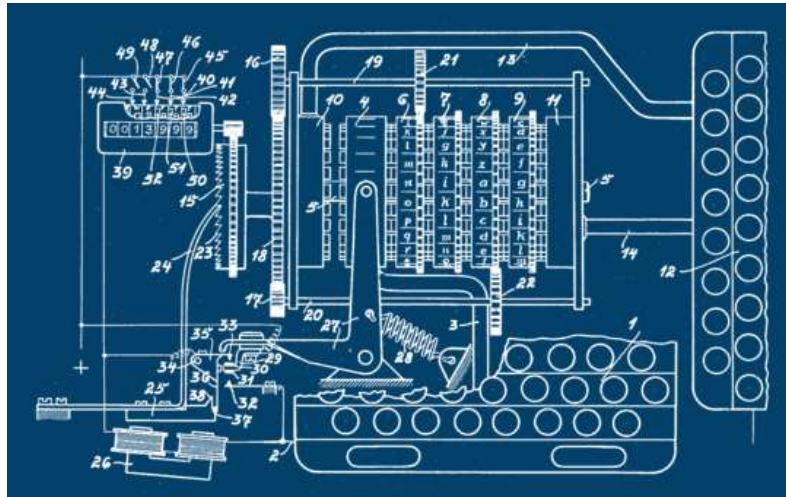
Kasnije su mnogi veliki ljudi nauke koristili šifrovane poruke kako bi svoje izume prezentovali samo osobama koje bi eventualno nastavile naučni rad bez zloupotreba prenetog znanja. Tako danas imamo prepiske Tesle sa Džordžom Vestinghausom koje su u određenim delovima pisama nerazumljive (šifrovane).

Prvi šifrarnik sa zupčanicima i valjcima je osmislio Tomas Džeferson (Thomas Jefferson) uz pomoć matematičara Dr. Roberta Petersona (Dr. Robert Patterson). On je kasnije često modifikovan i proizveden u više oblika, a najveću primenu je doživeo od strane ratne američke ratne mornarice u II Svetskom ratu.

Vilijam Fredman (William Friedman) je prvi osmislio pojam kritpoanaliza, i smatra se tvorcem tog dela kriptografije. On je uspešno dešifrovao japansku „ljubičastu” šifru i prosledio informacije o Japanu američkoj vojnoj komandi pre ulaska Amerike u II Svetski rat. Može se reći da je Vilijam Fredman svojim izumima zauvek izmenio istoriju sveta.⁶

Ipak, kada se govori o zaštiti podataka najčešće se pominje Enigma. Krajem 1928. godine je Artur Šerbius (Arthur Scherbius) patentirao svoju Enigma mašinu, a tek četiri godine kasnije grupa poljskih špijuna je uspela da dešifruje poruke koje je šifrovala Enigma. Njen značaj je u tome što jedan znak nije menjala drugim znakom na svim mestima, već je na osnovu algoritma dodeljivala svakom pojedinačnom slovu u nekoj poruci poseban znak, pa bi se tako AAAA šifrovano videlo kao EHJF.

⁶ D. Anucojić, Zaštita informacionih sistema i podataka, Prometej, Novi Sad 2008, str 99



Slika 5.2. Plan izrade Enigma mašine koji je predat prilikom pantentiranja

Takve šifre su bile izuzetno teške za dešifrovanje konvencionalnim metodama. Pronalazak Enigme i njena masovna primena dovela je do kreiranja Sigabe, američkog odgovora na prenosnu mašinu za šifrovanje. Sigaba je bila kompleksnija i gabaritno manja od Enigme, pa samim tim i prenosivija i primenljivija na bojištu.

Nakon II Svetskog rata razvoj računarske tehnike dao je novi zamah zaštiti podataka. Tako je 1970. IBM posle godina razvijanja prezentovao šifru Lucifer, koja je 1976. godine inspirisala DES (Data Encryption Standard). DES je odlično prihvaćen i često korišćen zbog dokazane otpornosti na napade.

Godinu dana po objavljivanju DES-a grupa početnika u zaštiti podataka (Rivest, Shamir i Adleman) stvorili su algoritam nazvan po početnim slovima svojih prezima – RSA. To je bila praktična šifra sa javnim ključevima koja se mogla koristiti za šifrovanje poruka ali i digitalni potpis, a bazirala se na faktorisanju veliki brojeva.

Šifrovanje poruka se umereno razvijalo do 1990. godine kada je u Švajcarskoj objavljen predlog za novi standard za šifrovanje podataka nazvan International Data Encryption Algorithm ili IDEA, koji je po planu trebao u potpunosti da zameni tada već prevaziđen DES. Kasnije se pod dejstvom IDEA-e pojavio PGP (Pretty Good Privacy) od autora Fila Cimermana (Phil Zimmermann) koji je svoj standard ponudio besplatno, što je dovelo do korišćenja ovog standarda u svetskim razmerama, iako se u to vreme koristio i RSA koji je smatran dosta sigurnim.

Brzina savremenih računara direktno utiče na razvoj kriptografije, pa tako danas računari naprednih performansi mogu da sakriju informacije tako da ih čovek vešt u kriptografiji za čitav svoj životni vek ne bi mogao rešiti. Budućnost kriptografije je direktno povezana sa budućnošću računara. Samim tim je za njih je direktno vezana i zaštita podataka.

Iako se tehnika zaštite podataka kroz vekove menjala, sama ideja skrivanja podataka je ostala ista – preneti neku poruku ili informaciju od jednog čoveka do drugog što je sigurnije moguće, korišćenjem algoritma koji bi omogućio skrivanje originalne poruke tako da bude potpuno ili pogrešno razumljiva osobama koje bi neovlašćeno došle u njen posed.

6. SAVREMENE TEHNIKE ZAŠTITE PODATAKA

Savremeno društvo egzistencionalno zavisi od zaštite podataka. Zbog bitnih podataka su se kroz istoriju vodili mnogi sukobi, od Krstaških ratova (i informacije o lokaciji Svetog Grala) do sukoba Alijanse sa Severnom Korejom (zbog informacija o nuklearnom programu).

S aspekta bezbednosti i zaštite podataka na prenosnim medijima, svaki od tih medija je u nekoj meri izložen rizicima gubitka podataka. Rizici koji prete zaštiti informacija na prenosnim medijima su kompjuterski kriminal, špijunaža svih oblika, nedovoljno kvalitetno održavanje medija, slučajno ili namerno nepravilno rukovanje medijima, prirodne katastrofe (poplave, zemljotresi, ...).

Kada govorimo o zaštiti podataka na tvrdim diskovima razlikujemo četiri načina za postizanje zaštite:⁷

1) Šifrovanje podatka

Šifrovanje podataka je tehnologija za zaštitu podataka koja šifrira podatke na prenosnom mediju. Šifrovanje u tom smilu može vršiti korišćenjem softvera i hardvera.

2) Sigurnosne kopije

Sigurnosne kopije (eng. backup) se rade kako bi se korisnici osigurali od gubitka podataka, koje kasnije ne bi mogli vratiti.

3) Maskiranje podataka

Maskiranje strukturiranih podataka je proces prikrivanja (maskiranja) određenih podataka u tablici baze podataka kako bi podaci bili osigurani i korisnikove informacije osetljivog sadržaja ne bi mogle "procureti" iz autorizovane okoline.

4) Brisanje podataka

Brisanje podataka je metoda kojom se u potpunosti uništavaju svi elektronski podaci na tvrdom disku ili nekom drugom digitalnom mediju kako bi se osigurali da podaci ili informacije ne procure nakon što se uređaj prestane koristiti.

6.1. SISTEMI ŠIFROVANJA PODATAKA

Šifrovanje podrazumeva korišćenje algoritamskih šema koje kodiraju originalni fajl koji je npr. tekstualni fajl u takvu formu da pomenuti fajl postaje nerazuman i nečitljiv, ali tako da proces bude reverzibilan i da je vraćanje u originalnu formu moguće. Tako se obezbeđuje neophodna zaštita kada se i ako za njom ukaže potreba.

Kako bi detaljno bio opisan proces šifrovanja, potrebno je da pre svega definišemo pojmove koji su bitni za taj proces i sve aktere u procesu šifrovanja.

⁷ M. Kostić, Zaštita podataka u sistemu zvanične statistke, Beograd 2006, str 102

Autentifikacija (*eng. Authentication*) je proces u kojoj se dokazuju identiteti krajnjih elemenata komunikacije korišćenjem digitalnih potpisa.

Integritet (*eng. Integrity*) podataka garantuje da nije došlo do izmene sadržaja poruke na njenom putu od izvora do odredišta, tako što se generiše heš informacija o proveru koja se zajedno sa njom smešta na prenosni medij. Najčešći oblik tih heš informacija za proveru je md5. Na prijemu se istim algoritmom korišćenim pri slanju poruke formira heš i poredi sa hešom koji je primljen u prenosnom mediju. Ako se te dve vrednosti ne poklapaju znači da je došlo do izmene originalnog sadržaja poruke. Danas se često uz programe koji sadrže samo jedan egzekutabilni fajl (npr. setup.exe) na prenosnom mediju kao što je disk stavlja i setup.md5 koji sadrži informaciju za proveru, pa tako klijent po dobijanju medija može da generiše md5, uporedi ga sa onim koji je poslao proizvođač i uveri se da je integritet fajla očuvan.

Neporicanje (*eng. Non-repudiation*) onemogućava da onaj ko je poslao poruku kasnije tvrdi da je nije poslao. Pošiljalac koristi svoj privatni ključ kako bi formirao digitalni potpis, a kako samo on ima pristup svom privatnom ključu znači da je samo on mogao da pošalje odgovarajuću digitalno potpisanu poruku. Neporicanje naravno postoji samo u slučaju da se koriste javni i privatni ključ. U slučaju korišćenja jednog ključa (šifre) moguće je poreći slanje podatka i kompromitovati zaštitu i verodostojnost podataka.

Asimetrični par ključeva – Privatni i javni ključ, kao matematički par koji se koristi za potrebe rada asimetričnog kriptografskog algoritma, kao što je na primer RSA algoritam.

Privatni ključ – Matematički podatak koji se koristi kao ključ za kreiranje elektronskog potpisa i za dešifrovanje simetričnog ključa kojim je šifrovan dokument za datog korisnika primenom asimetričnog kriptografskog algoritma.

Javni ključ – Matematički podatak koji može biti javno objavljen (najčešće se objavljuje u formi X.509v3 elektronskog sertifikata) i koji se koristi za verifikaciju elektronskog potpisa, kreiranog pomoću odgovarajućeg privatnog ključa koji je matematički par sa datim javnim ključem, kao i za šifrovanje podataka za korisnika koji poseduje odgovarajući privatni ključ.

Infrastruktura javnih ključeva - PKI (*eng. Public Key Infrastructure*) - Infrastrukturu javnih ključeva čine hardver, softver, polise i procedure koje su neophodne za upravljanje, generisanje, skladištenje i distribuciju kriptografskih ključeva i digitalnih sertifikata. Ona definiše model za sveobuhvatnu sigurnosnu infrastrukturu čije su usluge implementirane uz pomoć koncepta sistema za šifrovanje koji koriste asimetrične algoritme. Vredi napomenuti da sistem javnih ključeva funkcioniše identično kod mrežnog slanja podataka i slanja podataka na fizičkim medijima.

Sertifikaciono telo (*eng. CA – Certification Authority*) je pravno lice koje izdaje elektronske sertifikate. Sertifikaciono telo pre izdavanja sertifikata mora putem registracionog tela da proveri identitet osobe ili pravnog subjekta koji traži sertifikat, jer posedovanje potpisanog sertifikata zapravo znači da sertifikovano telo garantuje identitet pomenutog pravnog subjekta.

Registraciono telo (*eng. RA – Registration Authority*) je entitet koji je odgovoran za identifikaciju i autentifikaciju korisnika/vlasnika sertifikata, kao i kreiranje zahteva za izdavanje

sertifikata, ali koje ne izdaje i ne potpisuje sertifikat (RA vrši odgovarajuće poslove (identifikaciju korisnika) i u tom smislu je delegirano od CA).

CA sertifikat – Sertifikat za dato sertifikaciono telo izdat (digitalno potpisan) od strane drugog CA ili samopotpisan (ukoliko se radi o *Root CA*).

Politika Sertifikacije (eng. CP – *Certificate Policy*) – Imenovan skup pravila koji definiše primenljivost sertifikata na određeno okruženje i/ili na klasu podataka sa zajedničkim bezbednosnim zahtevima.

Praktična pravila rada Sertifikacionog tela (eng. CPS - *Certificate Practice Statement*) – Javna praktična pravila i procedure koje sertifikaciono telo primenjuje u proceduri izdavanja sertifikata.

Lanac sertifikata (eng. *Certificate chain*) – Uređena sekvenca sertifikata koja se, zajedno sa javnim ključem inicijalnog objekta u lancu, procesira u cilju provere istog u poslednjem objektu u lancu.

Treća strana – Primalac sertifikata koji proverava dati sertifikat i/ili proverava digitalni potpis dobijenog elektronskog dokumenta primenom javnog ključa potpisnika iz sertifikata. Takođe, treća strana proverava ispravnost sertifikata u istom procesu. Treća strana može biti i korisnik sertifikata izdatog od strane istog sertifikacionog tela ali i ne mora. Najčešće je treća strana krajnji korisnik.

Potpisnik – lice koje poseduje sredstva za elektronsko potpisivanje i vrši elektronsko potpisivanje u svoje ime.

Korisnik – fizičko lice kojem se izdaje elektronski sertifikat.

Zahtev za dobijanje sertifikata (eng. CSR – *Certificate Service Request*) – Standardna forma (po PKCS#10 preporuci) koja se koristi za slanje zahteva za dobijanje sertifikata. Zahtev za dobijanje sertifikata mora sadržati informacije o pravnom licu koje je sertifikat tražilo. Te informacije su: jedinstveno ime, ime kompanije ili organizacije, ime odseka, grad, region, zemlja i email adresa pravnog lica koji zahteva izdavanje sertifikata.

Sertifikacija – proces izdavanja elektronskog sertifikata. Postoje različiti nivoi sertifikacije koji su srazmerno nude veću ili manju sigurnost.

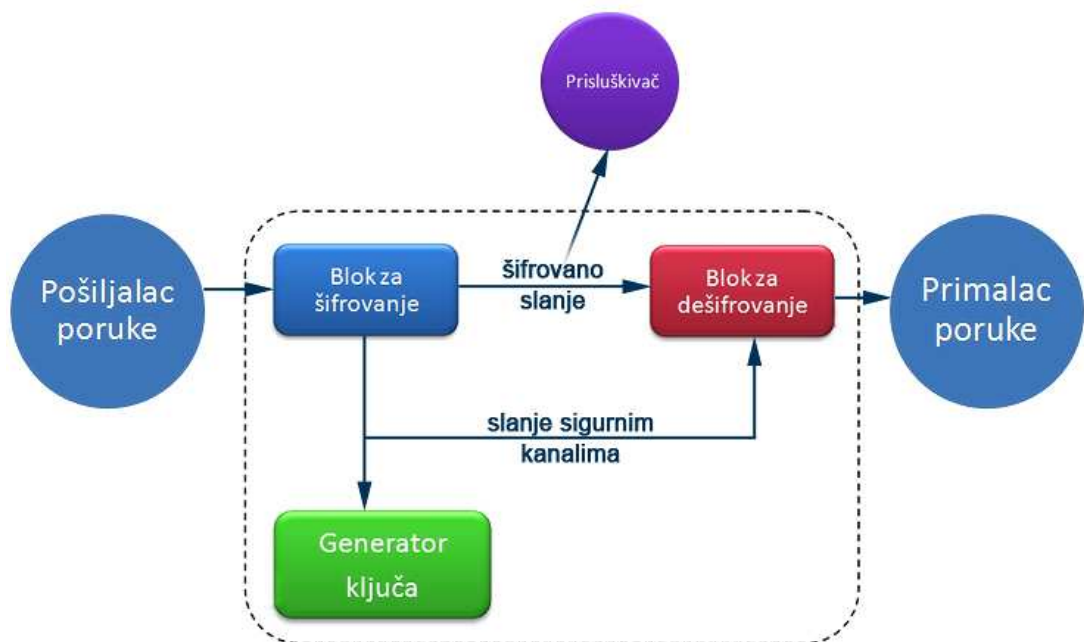
Serijski broj sertifikata – Pridruženi broj sertifikatu koji jedinstveno identifikuje sertifikat u domenu datog CA.

Lista opozvanih sertifikata (eng. CRL – *Certificate Revocation List*) – Lista izdata i elektronski potpisana od strane CA koja uključuje serijske brojeve opozvanih sertifikata i vreme kada je opoziv izvršen. Takva lista se zahteva od strane trećih strana uvek kada treba proveriti validnost sertifikata i/ili verifikaciju elektronskog potpisa.

Opoziv sertifikata – Trajno ukidanje validnosti datog sertifikata i njegovo smeštanje na CRL listu.

Repozitorijum – Baza podataka i/ili direktorijum na kome su objavljeni osnovni dokumenti rada CA, kao i eventualne druge informacije koje se odnose na pružanje sertifikacionih usluga od strane datog CA (kao na primer objavljivanje svih izdatih sertifikata...).

Na *Slici 6.1.1.* prikazana je opšta šema sistema za šifrovanje. Sistem za šifrovanje se sastoji od bloka za šifrovanje, bloka za dešifrovanje, generatora ključa i skupa poruka koje oni emituju. U bloku za šifrovanje se primenjuje neka matematička funkcija koja transformiše skup poruka koje se prenose u neprepoznatljiv oblik. Na ulaznu poruku, se pored same funkcije, primenjuje i ključ, koji predstavlja niz simbola čiji je zadatak da dodatno doprinesu promeni izvorne poruke. Ključ je nezavisan od izvorne poruke i od same funkcije i generiše se u generatoru ključa. Ovako izmenjena poruka se potom šalje preko nesigurnog telekomunikacionog kanala ka odredištu. Poruku u kanalu može presresti prislušivač u cilju dobijanja koristi bilo kroz samu informaciju koju poruka sadrži ili kroz izmenu poslatih podataka.



Slika 6.1.1. Šema sistema za šifrovanje⁸

Sistemi za šifrovanje sa simetričnim ključevima (algoritmi simetrične kriptografije) predstavljaju sisteme kod kojih se ključ za šifrovanje može lako odrediti iz ključa za dešifrovanje, i obrnuto. Najčešće su ova dva ključa ista pa je neophodno da se pošiljalac i primalac unapred dogovore o vrednosti ključeva koji će se koristiti za šifrovanje/dešifrovanje podataka.

⁸ Izvor: Đ. Petrović, Računari - Priručnik, Valjevo 2010

Rešavanje problema skalabilnosti i distribucije ključeva između učesnika u komunikaciji dovelo je do pojave sistema sa asimetričnim ključevima (algoritmi asimetrične kriptografije). U ovim sistemima svaka strana poseduje par ključeva, privatni i javni ključ, od kojih se jedan koristi za šifrovanje a drugi za dešifrovanje podataka. Privatni ključ je tajni i poseduje ga samo njegov vlasnik, dok je javni ključ dostupan svima. Korišćenjem sistema sa asimetričnim ključevima obezbeđuje se poverljivost podataka ali i autentifikacija pošiljaoca. Kako bi se obezbedila autentifikacija, pošiljalac vrši šifrovanje podataka koje šalje svojim privatnim ključem. Kada primalac primi poruku na prenosnom mediju, vrši njeno dešifrovanje javnim ključem pošiljaoca. Na taj način primalac je siguran da je poruku poslao samo onaj ko ima odgovarajući privatni ključ. Poverljivost podataka se dobija šifrovanjem tako što pošiljalac vrši šifrovanje koristeći javni ključ primaoca. Na taj način samo onaj kome je poruka namenjena može da je dešifruje jer samo on poseduje odgovarajući privatni ključ.

Jedan od prvih sistema koji se bazira na ovoj ideji je sistem Diffie i Hellmana koji omogućava korisnicima koji nisu imali prethodni kontakt generisanje simetričnog ključa preko nesigurnog kanala. Kod ovog sistema, svi korisnici poseduju jedan ključ koji je javno poznat i dostupan svim korisnicima (javni ključ), i drugi koji je dobro skriven (tajni ili privatni ključ). Ovi ključevi se generišu tako da iako su matematički povezani, računarski je neisplativo (u razumnom vremenskom periodu) pronalaženje privatnog ključa iz poznatog javnog. Sam proces generisanja simetričnog ključa počinje razmenom javnih ključeva zainteresovanih strana. Nakon toga, svaka strana primenjuje odgovarajuću matematičku funkciju na dobijeni javni i svoj privatni ključ. Zahvaljujući osobinama primenjene funkcije, rezultat je isti na obe strane i predstavlja deljeni simetrični ključ koji može da se koristi u daljoj komunikaciji za šifrovanje/dešifrovanje podataka koji se razmenjuju. Na ovaj način se ni privatni ni generisani simetrični ključ nikada ne transportuju nesigurnim kanalom, a primenjena funkcija je takva da bez poznavanja ovih ključeva sistem vrlo teško može da se analizira.

Na bazi rada Diffie i Helmana pojavili su se i drugi sistemi kao što su RSA, ElGamal, Cramer-Shoup. Ovi sistemi takođe koriste par asimetričnih ključeva koji se vrlo teško određuju jedan iz drugoga, ali za razliku od sistema Diffie i Helmana koristi se javni ključ korisnika kome se šalje poruka za šifrovanje same poruke. Na prijemu se uz pomoć privatnog ključa i algoritma za dešifrovanje primenjuje inverzan postupak i dobija originalna poruka. Kako je vlasnik privatnog ključa i jedina osoba koja ga poseduje, niko drugi ne može da dešifruje poruku te je sigurnost komunikacije zagarantovana. Sa matematičke strane, kod ovih sistema funkciju šifrovanja je vrlo lako izračunati, dok je pronalaženje inverzne funkcije veoma složeno.

Kombinovanjem sistema za šifrovanje sa simetričnim i asimetričnim ključevima na odgovarajući način, dobijaju se kombinovani sistemi za šifrovanje koji objedinjuje njihove najbolje osobine. Algoritmi simetrične kriptografije su jednostavniji pa omogućavaju veće brzine rada koristeći ključeve manjih veličina dok se skalabilnost i distribucija ključeva realizuju korišćenjem algoritama asimetrične kriptografije.

6.2. AUTENTIFIKACIJA I DIGITALNI POTPIS

Primenom kriptografske heš funkcije na proizvoljan blok podataka dobija se niz bita fiksne dužine koji se naziva heš vrednost poruke (*hash value, message digest, digest*). Osnovna karakteristika heš funkcije je da i najmanja promena u originalnoj poruci dovodi do promene njene heš vrednosti.

Idealna kriptografska heš funkcija treba da poseduje sledeće karakteristike:

- izračunavanje heš vrednosti neke poruke je jednostavno,
- nemoguće je (u konačnom broju koraka) pronaći poruku koja ima datu heš vrednost,
- nemoguće je (u konačnom broju koraka) promeniti poruku a da ne dođe do promene i njene heš vrednosti,
- nemoguće je (u konačnom broju koraka) pronaći dve različite poruke koje imaju istu heš vrednost.

Kriptografske heš funkcije se koriste kako bi se potvrdio integritet podataka koji se prenose nesigurnim kanalom, kako i za generisanje novih ključeva za šifrovanje na osnovu vrednosti početnog ključa.

U Tabeli 6.2.1 je data lista različitih heš funkcija i dužine njihovih heš vrednosti.

Naziv algoritma	Dužina heša
GOST	256 bita
HAS-160	160 bita
HAVAL	128-256 bita
MD2	128 bita
MD4	128 bita
MD5	128 bita
RadioGatun	Do 1216 bita
RIPEMD-64	64 bita
RIPEMD-160	160 bita
RIPEMD-320	320 bita
SHA-1	160 bita
SHA-224	224 bita
SHA-256	256 bita
SHA-384	384 bita
SHA-512	512 bita
Skein	256, 512, 1024 bita
Snefru	128, 256 bita
Tiger	192 bita
Whirlpool	512 bita
FSB	160-512 bita
ECOH	224-512 bita
SWIFFT	512 bita

Tabela 6.2.1 Lista funkcija sa prikazanom dužinom heš funkcije

MAC (eng. Message Authentication Code) predstavlja niz bita koji se dodaju na originalnu poruku kako bi se obezbedila autentifikacija pošiljaoca i integritet poruke. MAC vrednost se dobija tako što se na poruku i tajni ključ, koji poseduju obe strane komunikacije, primeni MAC algoritam. Autentifikacija se postiže korišćenjem tajnog deljenog ključa, jer samo primalac i pošiljalac imaju taj ključ. Na prijemu se ponovo računa MAC vrednost primljene poruke i poredi se sa vrednošću koja je poslata uz poruku. Ako se te dve vrednosi ne poklapaju, došlo je do neovlašćene promene sadržaja originalne poruke.

Postoje dve kategorije MAC-a:

- **HMAC** (*Hash-based Message Authentication Code*) – koristi se neki od poznatih heš algoritama u realizaciji MAC algoritma (HMAC-MD5, HMAC-SHA1),
- **CMAC** (*Cipher-based Message Authentication Code*)⁹

Digitalni potpis elektronskih podataka može da se posmatra u analogiji sa potpisom ili pečatom štampanih dokumenta. On omogućava da primalac poruke bude siguran da nije došlo do izmene originalnog sadržaja poruke, kao i da bude siguran u identitet pošiljaoca poruke. Drugim rečima, garantuje integritet poruke i autentifikaciju pošiljaoca iste.

Pored toga, digitalni potpis ne može da se porekne, tako da onaj ko je poslao poruku kasnije ne može da tvrdi da je nije poslao ili da je neko drugi poslao umesto njega.

Digitalni potpis poruke se formira korišćenjem tehnike asimetričnih ključeva. Pošiljalac kreira heš (šifrovani sažetak poruke) tako što na originalnu poruku primenjuje heš algoritam. Heš poruke predstavlja „digitalni otisak prsta“ poruke. Ako bi došlo do najmanje promene u originalnoj poruci, promenio bi se i rezultujući heš poruke. Pošiljalac zatim vrši šifrovanje heša svojim privatnim ključem. Ovako šifrovan heš predstavlja digitalni potpis poruke.

Pošiljalac dodaje na kraj originalne poruke i njen digitalni potpis i tako digitalno potpisanu poruku šalje. Na prijemu, primalac pomoću javnog ključa pošiljaoca vrši dešifrovanje digitalnog potpisa poruke kako bi dobio heš poslate poruke i poredi ga sa vrednošću heša koji on dobija primenjujući isti heš algoritam na samu primljenu poruku. Ako se dobijene heš vrednosti ne razlikuju primalac može da bude siguran da poruka nije izmenjena. Ako se vrednosti razlikuju znači da je došlo do neovlašćenog menjanja sadržaja poruke i/ili da je neko drugi poslao poruku od onog za koga se izdaje.

Infrastrukturu javnih ključeva čine hardver, softver, polise i procedure koje su neophodne za upravljanje, generisanje, skladištenje i distribuciju kriptografskih ključeva i digitalnih sertifikata. Ona definiše model za sveobuhvatnu sigurnosnu infrastrukturu čije su usluge implementirane uz pomoć koncepata sistema za šifrovanje koji koriste asimetrične algoritme.

Upravljanje, generisanje, skladištenje i distribucija kriptografskih ključeva i digitalnih sertifikata se odvija kroz **Sertifikaciono telo (CA)** i **Registraciono telo (RA)**.

⁹ M. Kostić, Zaštita podataka u sistemu zvanične statistke, Beograd 2006, str 129

Osnovna uloga CA je da predstavlja telo od poverenja kome svi učesnici u komunikaciji veruju. CA funkcioniše na sledeći način. Krajnji korisnici, koji međusobno nemaju uspostavljen lanac poverenja, veruju Sertifikacionom telu. CA prvo vrši autentifikaciju krajnjih korisnika (direktno ili posredstvom RA). Posle uspešne autentifikacije, CA izdaje digitalni sertifikat krajnjem korisniku. Izdati sertifikat garantuje identitet korisnika i potpisan je digitalnim sertifikatom samog Sertifikacionog tela. Krajnji korisnici sada koriste svoje digitalne sertifikate, izdate od strane Sertifikacionog tela kome veruju, kako bi dokazali svoj identitet jedan drugom i uspostavili sigurnu komunikaciju.

Da bi koristili usluge infrastrukture javnih ključeva, krajnji korisnici prvo moraju da prođu proces prijavljivanja koji obuhvata proveru identiteta i razmenu informacija sa, za to zaduženom komponentom infrastrukture javnih ključeva, Registracionim telom.

Prvi korak u procesu prijavljivanja je registracija pri kojoj se proverava identitet krajnjeg korisnika koji podnosi zahtev za sertifikat. Nivo provere identiteta zavisi od tipa sertifikata za koji se podnosi zahtev (sertifikati koji se koriste pri elektronskoj kupovini zahtevaju stroži nivo provere od ostalih tipova sertifikata) i svaki tip sertifikata je definisan odgovarajućim dokumentom 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: 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.

Digitalni sertifikati omogućavaju potvrdu identiteta pri elektronskim transakcijama, slično kao što to čine lične karte u međuljudskim interakcijama. On povezuje podatke o identitetu korisnika sa parom asimetričnih ključeva koji se koriste za šifrovanje i potpisivanje digitalne informacije čime potvrđuje nečije pravo na korišćenje kriptografskih ključeva.

Digitalni sertifikat je izdat i digitalno potpisan od strane sertifikacionog tela kome veruju svi učesnici u komunikaciji.

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
- Digitalni potpis izdavača

Pri slanju poruke pošiljalac digitalno potpisuje poruku i uz nju šalje i svoj digitalni sertifikat kako bi primalac mogao da bude siguran u identitet pošiljaoca. Uz poruku može da bude poslato i više digitalnih sertifikata koji formiraju hijerarhijski lanac poverenja, gde jedan digitalni sertifikat potvrđuje autentičnost prethodnog digitalnog sertifikata. Na samom vrhu u hijerarhiji poverenja nalazi se *root* (top-level) sertifikaciono telo kome veruju sva ostala sertifikaciona tela. Javni ključ *root* sertifikacionog tela mora da bude javno poznat i dostupan.

Opoziv sertifikata. Iako je period važenja digitalnog sertifikata definisan datumima u odgovarajućim poljima samog sertifikata dešava se da dođe do kompromitovanja tajnog ključa ili promene nekog od osnovnih ličnih podataka koji se nalaze u sertifikatu što ima za posledicu opozivanje sertifikata, odnosno njegovo povlačenje iz upotrebe. Opozvani sertifikati se objavljuju preko lista opozvanih sertifikata (eng. *Certificate Revocation List* - **CRL**) koje objavljuje sertifikaciono telo koje je izdalo sertifikat. U nekim slučajevima, umesto lista opozvanih sertifikata, koriste se protokoli za proveru stanja sertifikata u realnom vremenu koji daju pozitivan ili negativan odgovor o statusu sertifikata. Primer takvog protokola je OCSP (eng. *Online Certificate Status Protocol*).

Provera validnosti sertifikata. Kao što je već gore pomenuto, nevažeći (opozvani sertifikati) se objavljuju preko lista opozvanih sertifikata ili se koriste protokoli za proveru stanja sertifikata. Treća strana je dužna da pre nego što prihvati sertifikat proveru njegovu validnost.

6.2.1. FORMAT DIGITALNOG CERTIFIKATA

Format digitalnog sertifikata je definisan ITU-T X.509 standardom, a danas se najčešće koristi verzija 3.

Po preporukama datim u RFC5280 polja koja treba da sadrži digitalni sertifikat su sledeća:

- ♦ **Version** - informacija o verziji sertifikata. Trenutna verzija (i ona koja se najčešće sreće) je 3.

- ♦ **Serial number** – serijski broj sertifikata predstavlja jedinstveni identifikator sertifikata izdatih od određenog sertifikacionog tela.

- ♦ **Signature** - identifikator algoritma (u formi identifikatora objekta (OID)) korišćenog od strane sertifikacionog tela za potpisivanje sertifikata.

- ♦ **Issuer** - jedinstveno ime sertifikacionog tela koje je izdalo sertifikat.

- ♦ **Validity** - označava period važenja sertifikata i sadrži dva datuma od kojih jedan označava trenutak od kada se sertifikat može smatrati važećim - polje *Not Valid Before*, a drugi, trenutak do kog se sertifikat može smatrati važećim – polje *Not Valid After*.

- ♦ **Subject** - identifikuje korisnika kome je izdat sertifikat. Kao i polje *Issuer*, daje se u formi jedinstvenog imena.

- ♦ **Subject public key info** - sadrži javni ključ korisnika, kao i identifikaciju algoritma koji je korišćen pri kreiranju istog (RSA, DSA ili Diffie-Hellman).

- ♦ **Unique identifiers** - je dodatni identifikator sertifikata čija se upotreba ne preporučuje u verzijama 2 i 3.

- ♦ **Extensions** - sadrži listu jednog ili više proširenja sertifikata koja se koriste za specificiranje dodatnih informacija o sertifikatu. Svaki član liste pored tipa proširenja kog predstavlja sadrži i oznaku kritičnosti proširenja. U slučaju da korisnički softver ne ume da prepozna kritično proširenje prilikom procesiranja, sertifikat mora da bude označen kao

nevažeći (u slučaju nekritičnog proširenja, moguće je ignorisati dato proširenje). Proširenja koja su u upotrebi pripadaju sledećim kategorijama:

Standardna proširenja:

- ◆ Authority key identifier - AKI - omogućava identifikovanje javnog ključa koji odgovara tajnom ključu sertifikacionog tela kojim je potpisan sertifikat. Obično se koristi ako sertifikaciono telo ima više od jednog ključa za potpisivanje.

- ◆ Subject key identifier - SKI - jedinstveni identifikator koji se koristi se za identifikovanje sertifikata koji sadrže odgovarajući javni ključ.

- ◆ Key usage - definiše namenu ključa sadržanog u konkretnom sertifikatu – da li on može da se koristi za potpisivanje, za šifrovanje, za verifikaciju lista opozvanih sertifikata i sl.

- ◆ Certificate policies - sadrži listu identifikatora politika sertifikacije (datih u formi identifikatora objekta) i dodatnih opcionih tekstualnih parametara koji svedoče da je konkretan sertifikat izdat pod odgovarajućim skupom pravila objedinjenih u naznačenim politikama sertifikacije. Opcioni parametri koji se koriste su Certification Practice Statement pointer koji definiše lokaciju na kojoj mogu da se pronađu Praktična pravila rada Sertifikacionog tela i parametar User notice koji sadrži tekst poruke za krajnjeg korisnika.

- ◆ Policy mappings - koristi se u sertifikatima sertifikacionih tela iz različitih administrativnih domena da označi skup parova politika sertifikacije koje se smatraju ekvivalentnim. Par politika sertifikacije koje se navode u ovom proširenju daju se u poljima Issuer domain policy i Subject domain policy.

- ◆ Subject alternative name - sadrži dodatne podatke o subjektu sertifikacije (npr. njegov email, URL, IP adresu i sl.).

- ◆ Issuer alternative name - sadrži dodatne podatke o sertifikacionom telu koje je izdalo sertifikat (npr. njegov email, URL, IP adresu i sl.).

- ◆ Subject directory attributes - daje dodatne informacije o predmetu sertifikovanja

(npr. nacionalnost) i nije od velikog značaja.

- ◆ Basic constraints - govori da li je predmet sertifikacije sertifikaciono telo ili krajnji korisnik. U slučaju da je sertifikaciono telo, proširenje može da sadrži i parametar koji pokazuje koliki je broj sertifikata sertifikacionih tela koje mogu da ga slede (Path length).

- ◆ Name constraints - koristi se samo u sertifikatima sertifikacionih tela i definiše prostor imena dat u formi stabla dozvoljenih/zabranjenih imena (Permitted subtrees and/or Excluded subtrees) kome svi tipovi imena datih u sertifikatima krajnjih korisnika koje su izdala ova sertifikaciona tela moraju/ne smeju da pripadaju.

- ◆ Policy constraints - koristi se u sertifikatima sertifikacionih tela da zabrani preslikavanje politika sertifikacije ili da označi neophodnost pojavljivanja određene politike sertifikacije u

sertifikatima nakon ovog. Prisustvo polja inhibit Policy Mapping sugerše da je nakon određenog broja sertifikata (definisanog vrednošću ovog polja) zabranjeno preslikavanje politika sertifikacije, dok prisustvo polja Require explicit policy sugerše upotrebu određene politike sertifikovanja u određenom broju narednih sertifikata (definisanom ovom vrednošću).

- ◆ Extended key usage - koristi se u sertifikatima krajnjih korisnika da označi dodatne mogućnosti upotrebe ključa (pored onih koje su definisane u proširenju Key usage).

- ◆ CRL distribution points - ukazuje na lokacije na kojoj se nalazi lista opozvanih sertifikata.

- ◆ Inhibit any-Policy - koristi se u sertifikatima sertifikacionih tela da ukaže na broj sertifikacionih tela posle ovog za koje se specijalna vrednost politike sertifikacije any-Policy (koja označava mogućnost upotrebe bilo koje politike sertifikacije) ne smatra važećim uparenjem sa nekom drugom konkretnom.

- ◆ Freshest CRL pointer - predstavlja pokazivač na „najsvežije“ informacije vezane za opozvane sertifikate (u praksi, ovo je najčešće pokazivač na Delta listu opozvanih sertifikata).

Privatna proširenja:

Privatna proširenja se definišu prilikom korišćenja sertifikata u specifičnim oblastima. Tako, na primer, RFC5280 specifikuje dva proširenja ove vrste za primenu na Internetu:¹⁰

- ◆ Authority information access - definiše način pristupa uslugama (i informacijama) koje pruža sertifikaciono telo koje izdaje sertifikat (npr. o usluzi za online proveru ispravnosti sertifikata, dodatnim informacijama o politici sertifikovanja...).

- ◆ Subject information access - definiše način pristupa uslugama (i informacijama) koje može da pruža predmet sertifikovanja (npr. mesto skladištenja sertifikata kad je reč o predmetu sertifikovanja koje je sertifikaciono telo).

¹⁰ Đ. Petrović, Računari - Priručnik, Valjevo 2010

7. RSA ALGORITAM

RSA predstavlja algoritam za asimetrično šifrovanje pre svega podataka (primarno je osmišljen za prenos podataka na prenosnim medijima), ali se danas koristi i u sistemima elektronskog potpisa. Njegova primena se proteže od sigurnosnih protokola, zaštite informacija, zaštite čitavih baza podataka i multinacionalnih sistema elektronskog i svakog drugog poslovanja. Iako je primarno kreiran 1977. godine a objavljen tek godinu dana kasnije, patentiran je tek 1983. godine u SAD pod šifrom US Patent 4.405.829. Patentna prava tog patenta su istekla 2000. godine.

Zanimljivo je navesti da je Kliford Koks (Clifford Cox), britanski matematičar osmislio gotovo identičan sistem RSA algoritmu 1973. godine. Posle diplome na Kembridž univerzitetu, Kliford je pozvan da se pridruži GCHQ (Government Communication Headquarters – Središte za komunikaciju britanske vlade) kako bi pomogao u rešavanju problema javnih ključeva. Pošto je ranije izučavao teoriju brojeva, lako je uvideo gde se problem nalazio, identifikovao faktore koji na njega utiču i rešio ga u rekordnom roku. Zbog poverljivosti informacija kojima se bavio GCHQ ovaj sistem je objavljen tek 1997. godine.

Pre dvadeset godina Difie i Helman su izjavili: “We stand today on the bank of revolution in cryptography”. Danas se nalazimo na sredini te revolucije. U poslednje dve decenije došlo je do prave eksplozije istraživanja u oblasti kriptologije. Mnogi kriptosistemi bili su predlagani, a mnogi od njih bili su razbijeni. Povezanost između kriptologije, teorije kompleksnosti i teorije brojeva postepeno je otkrila i obogatila sve tri grane istraživanja.

Rivest, Šamir i Adleman su 1978. godine objavili kriptosistem sa javnim ključem koji zadovoljava sva tri zahteva koja su postavili Difie i Helman.

Šifrovani RSA algoritam je deterministički šifrovani algoritam (nema slučajnih komponenata) i napadač uspešno može izvršiti *chosen plaintext* napad na kriptosistem, šifrujući mogući osnovni tekst, korišćenjem javnog ključa, i proveravajući da li je jednak šifrovanom tekstu koji želi da dešifruje. Kriptosistem se naziva „semantički siguran“ ako napadač ne može razlikovati dva šifrovana teksta, čak i ako mu je poznat odgovarajući osnovni tekst. RSA bez *padding* šeme nije semantički siguran.

Da bi se izbegao ovaj problem praktična RSA implementacija obično ubacuje neki dodatak (*padding*) u osnovnu poruku pre nego što se izvrši šifrovanje. Ovaj dodatak omogućava da osnovna poruka ne upadne u opseg nesigurnog osnovnog teksta i da se data poruka šifruje u jednu od brojnih, različitih šifrovanih poruka.

Belar (*Mihir Bellare*) i Rogevaj (*Phillip Rogaway*) 1993. godine formalizovali su koncept *random orakla*, što predstavlja veoma važan deo teorije kompleksnosti u kriptografiji. Taj novi alat im je omogućio da predstave nekoliko asimetričnih šifrovanih šema koje su efikasne i dokazano sigurne (u random orakl modelu). *The Optimal Asymmetric Encryption Padding (OAEP)* najznačajnija je šema tog modela.

Određeno vreme naučnici su pokušavali da dođu do dokaza o sigurnosti kriptografskih protokola u redukcionom smislu. Da bi to postigli, predstavljali su algoritme koji koriste efektivan napad kao potprogram da bi razotkrili početnu tešku pretpostavku (kao što je RSA pretpostavka ili

nemogućnost faktorizacije celih brojeva). Takvi algoritmi nazivaju se „redukциони“ i mogu biti uspešni, grubo govoreći, ako ne zahtevaju previše poziva potprograma.

Pre nekoliko godina započeo je novi pravac u istraživanjima koji je kombinovao dokazivanje sigurnosti i efikasnosti. Da bi postigli cilj Belar i Rogevaj su formalizovali heuristiku koju su predložili Fiat (*Amos Fiat*) i Šamir. Ona se sastojala u izradi idealne pretpostavke o nekom objektu, kao što je heš funkcija, prema kojoj je moguće simulirati ponašanje zaista slučajne funkcije. Ova pretpostavka, poznata kao „random orakl model“, može izgledati strogo i bez mogućnosti praktične primene. U random orakl modelu se pretpostavlja da napadač ne može da koristi bilo koji specifičan nedostatak heš funkcije koja se koristi u praksi. Potrebno je naglasiti da čak i formalna analiza u random orakl modelu nije jak dokaz sigurnosti, jer je zasnovana na idealnoj pretpostavci.

Random orakl u kriptografiji je orakl (crna kutija) koji na svaki upit odgovara slučajnim odgovorom, izabranim uniformno iz izlaznog domena. Sa druge strane, random orakl je matematička funkcija koja slika svaki mogući upit na slučajan odgovor iz izlaznog domena. Random orakl predstavlja matematičku apstrakciju koja se koristi u kriptografskim dokazima, a koristi se kada nije poznata matematička funkcija koja dovodi do osobina traženih u dokazu. Sistem za koji je dokazano da je siguran, korišćenjem ovog načina dokazivanja, smatra se sigurnim u random orakl modelu, za razliku od sigurnosti u standardnom modelu. U praksi se random orakl obično koristi za modeliranje kriptografske heš funkcije u šemama u kojima je potrebna pretpostavka o strogoj slučajnosti. Ovakvi dokazi obično pokazuju da je sistem siguran, ukazujući na činjenicu da napadač mora da zahteva nemoguće ponašanje orakla ili da reši neki matematički problem za koji se veruje da je težak u cilju razotkrivanja sistema.

Ne postoji realna funkcija koja predstavlja random orakl. U suštini, određene šifrovane šeme su dokazano sigurne u random orakl modelu, ali su trivijalno nesigurne kada bilo koja realna funkcija zameni random orakl.

Bez obzira na to, dokaz o sigurnosti u random orakl modelu obično daje veoma jak dokaz da napad koji ne razbije druge pretpostavke dokaza (kao što je faktorizacija celih brojeva) mora otkriti neke nepoznate osobine heš funkcije koja se koristi. Među šemama koje su dokazano sigurne u random orakl modelu jedna od najznačajnijih je OAEP šema.

Posle Blaihenbaherovog (*Daniel Bleichenbacher*) razarajućeg napada na RSA-PKCS #1 v1.5 1998. godine, RSA-OAEP (RSA-PKCS #1 v2.0) postao je naslednik standarda 2, a samim tim i internacionalni standard. Interesantno je da je Soup (*Victor Shoup*) nedavno pokazao da originalni dokaz sigurnosti OAEP-a nije korektan. Srećom, ubrzo posle toga otkrio je formalan i kompletan dokaz koji garantuje visok nivo sigurnosti RSA-OAEP šeme. Međutim, ovaj novi dokaz sigurnosti još uvek ne garantuje sigurnost za veličinu ključa koji se koristi u praksi. Alternative OAEP šeme, kao što su OAEP+ i SAEP+ omogućavaju efikasnije dokazivanje i zbog toga obezbeđuju adekvatan nivo sigurnosti za veličinu ključa koja se koristi u praksi.

U vreme kada je Blaihenbaher objavio svoj napad na RSA-PKCS #1 v1.5 jedina efikasna i „dokazano sigurna“ šifrovana šema, zasnovana na RSA problemu, bila je OAEP šema, koju su predložili Belar i Rogevaj. OAEP se može koristiti sa bilo kojom *trapdoor* permutacijom f . Belar i Rogevaj su dokazali da OAEP *padding* korišćen bilo kojom *trapdoor* - jednosmernom permutacijom f semantički obezbeđuje sigurnost šifrovanoj šemi. Dopunjavanjem osnovne poruke

oni su, pored sigurnosti, dokazali i da je OAEP *padding* slabo svestan osnovne poruke. Kriptosistem je slabo svestan osnovne poruke ako bilo koji algoritam teško može da dode do šifrovanog teksta kad mu nije poznat odgovarajući osnovni tekst. Nažalost, *adaptive chosen-ciphertext* napad dozvoljava napadaču da proizvoljno dugo pristupa dešifrovanom oraklu, čak i posle primanja spornog šifrovanog teksta o kojem napadač želi da dobije neke informacije. Zbog toga, semantička sigurnost, zajedno sa slabom svešću o osnovnom tekstu, samo implicira semantičku sigurnost na *non-adaptive chosen-ciphertext* napad (*lunchtime* napad ili indiferentan *chosen-ciphertext* napad), gde je pristup dešifrovanom oraklu ograničen, dok napadač ne primi testirani šifrovani tekst.

Činjenica je da je jedini formalan dokaz sigurnosti OAEP šeme dokaz da je ona semantički sigurna na *lunchtime attacks*, pod pretpostavkom da je osnovna permutacija jednosmerna. Međutim, veruje se da je OAEP takođe semantički sigurna šema na *chosen-ciphertext* napad. OAEP šema je vrsta Feistelove mreže koja koristi par random orakla G i H da bi obradila osnovni tekst asimetričnim šifrovanjem. Kada se kombinuje sa bilo kojom jednosmernom *trapdoor* permutacijom f ova obrada će dokazano, u smislu random orakl modela, rezultirati kombinovanom šemom koja je semantički sigurna na *chosen plaintext* napad (INDCPA). Kada je implementirana sa pouzdanom *trapdoor* permutacijom (na primer RSA), OAEP će biti dokazano siguran i na *chosen ciphertext* napad (IND-CCA).

OAEP šema zadovoljava sledeća dva uslova:

- dodaje elemente slučajnosti koji mogu biti korišćeni za konvertovanje determinističke šifrovane šeme (kakva je RSA šema) u verovatnosnu šemu,
- štiti delimično dešifrovanje šifrovanog teksta, onemogućavajući napadača da otkrije bilo koji deo osnovnog teksta ako nije u mogućnosti da invertuje *trapdoor* jednosmernu permutaciju f .

Među algoritmima sa javnim ključem postoji ogroman jaz izmađu praktičnih šema i šema za koje je dokazano da su sigurne: praktični metodi su efikasni, ali nemaju dovoljan nivo dokazane sigurnosti, dok su dokazano sigurne šeme sigurne, ali ni blizu toliko efikasne. Pri dokazivanju sigurnosti OAEP šeme zahteva se da G i H budu random funkcije, međutim, prilikom konkretne implementacije koriste se kriptografske heš funkcije. Paradigma tvrdi da rezultati koji se zasnivaju na idealnoj heš funkciji i koji dokazuju sigurnost imaju veći značaj od protokola koji su dizajnirani *ad. hoc*. Pri dokazivanju da je OAEP sistem siguran garantuje se da napadač, koji poseduje šifrovani tekst, mora otkriti *message* $G(r)$ ako želi da otkrije bilo šta smisljeno o osnovnoj poruci *message*. Dokazano je da postoji jednostavnija *padding* šema za konvertovanje RSA šifrovane šeme u verovatno onu, koja je, takođe, sigurna u random orakl modelu. To je takozvana SAEP+. Primećeno je da jednostavnija *padding* šema čini sistem lakšim za opisivanje i lakšim za implementaciju, a samim tim mnogo elegantnijim. Pojednostavljenje *padding* šeme ima malo uticaja na performanse, jer je vreme za njeno izvršavanje zanemarljivo u odnosu na samo šifrovanje. Mada je SAEP+ *padding* šema jednostavnija od OAEP šeme, ona je i restriktivnija. Korišćenjem OAEP i OAEP+ šeme može se šifrovati poruka koja je dugačka skoro kao i modul. Na primer, za 1024-ro bitni modul bezbedno je šifrovati poruku koja je dugačka 768 bitova. Nasuprot tome, korišćenjem modula iste veličine, SAEP+ šema može šifrovati poruku od najviše 384 bita. Ova razlika je nije toliko bitna u svakodnevnoj upotrebi (za transport ključa), ali je ipak vredna pomena.

8. SOFTVER ZA ŠIFROVANJE DISKA

Softver za šifrovanje diska je softver za zaštitu kompjutera, koji je projektovan da zaštiti poverljivost podataka sačuvanih na hard disku, koristeći tehniku šifrovanja diska. Ova tehnika dozvoljava da podaci budu sačuvani, čak i kada OS nije aktivan, na primer kada se podaci očitavaju direktno sa hardvera. Takvi softveri šifruju podatke i transparentno ih dešifruju, kada ovlašćeni korisnik to zatraži, upisujući šifru.

U kriptografiji, cipher (šifra) je algoritam za šifrovanje i dešifrovanje, serija dobro definisanih koraka, koji mogu biti praćeni kao procedura. Šifrovanje ili kodovanje je procedura koja konvertuje informacije iz običnog teksta u šifre ili kodove. U ne tehničkoj upotrebi šifra je isto što i kod, ali u kriptografiji koncepti se razlikuju. U klasičnoj kriptografiji, šifre se razlikuju od kodova. Kada se koristi šifra, originalna informacija se naziva 'običan tekst', a šifrovana forma 'šifra tekst'. 'Šifra tekst' poruka sadrži sve informacije 'običan tekst' poruke, ali format ne može da očita čovek ili kompjuter bez pogodnog programa za dešifrovanje.

Šifra operacija obično zavisi od delića sporedne informacije, nazvane ključ. Procedura šifrovanja varira u zavisnosti od ključa, koji menja detaljan rad algoritma. Ključ mora biti izabran pre korišćenja šifre na poruku. Bez poznavanja ključa, biće teško, ako ne i nemoguće dešifrovati 'šifra poruku' u čitljiv 'običan tekst'.

Većina modernih šifara se može svrstati na nekoliko načina:

- po tome da li rade na blokovima simbola obično fiksne veličine (blok šifre), ili na kontinualnom toku simbola,
- po tome da li se isti ključ koristi za šifrovanje ili dešifrovanje (algoritmi simetričnih ključeva), ili se drugačiji ključ koristi za obe operacije (algoritmi asimetričnih ključeva). Ako je algoritam simetričan, ključ mora biti poznat primaocu i pošiljaocu, i nikom više. Ako je algoritam nesimetričan, ključ za šifrovanje se razlikuje, ali je u tesnoj vezi sa ključem za dešifrovanje.

8.1. POREĐENJE SOFTVERA ZA ŠIFROVANJE DISKA

Ovo su tehnički podaci poređenja različitih softvera za šifrovanje diskova.¹¹

¹¹ http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software, datum posete linka 9.9.2012. 18:15

Operativni sistemi:

	Windows	Windows mobile/ Pocket PC	Linux	Mac
BestCrypt	Da	Ne	Da	Da
BitLocker	Da	Ne	Ne	Ne
CrossCrypt	Da	Da	Ne	Ne
DiskCryptor	Da	Ne	Ne	Ne
DriveCrypt	Da	Ne	Ne	Ne
R-Crypto	Da	Ne	Ne	Ne
TrueCrypt	Da	Ne	Da	Da

Tabela 8.1.1. Poredjenje softvera na osnovu OS

Karakteristike:

	Skriveni kontejneri	Autentikacija pre-boot	Autentikacija po narudžbini	Višestruki ključevi	Hardversko ubrzanje	Fajl sistem
BestCrypt	Da	Da	Ne	Da	Da	Bilo koji
BitLocker	Ne	Da	Da	Da	Da	NTFS
CrossCrypt	Ne	Ne	Ne	Ne	Ne	
DiskCryptor	Ne	Da	Da	Ne	Da	Bilo koji
DriveCrypt	Da	Da	Ne	Da	Ne	Bilo koji
TrueCrypt	Da	Samo na Windows	Ne	Da	Da	Bilo koji

Tabela 8.1.2. Poredjenje softvera na osnovu karakteristika

Slojevi:

	Ceo disk	Particija	Fajl
BestCrypt	Da	Da	Da
BitLocker	Da	Da	Ne
CrossCrypt	Ne	Ne	Da
DiskCryptor	Da	Da	Ne
DriveCrypt	Da	Da	Da
R-Crypto	Ne	Ne	Da
TrueCrypt	Da	Da	Da

Tabela 8.1.3. Poredjenje softvera na osnovu slojeva

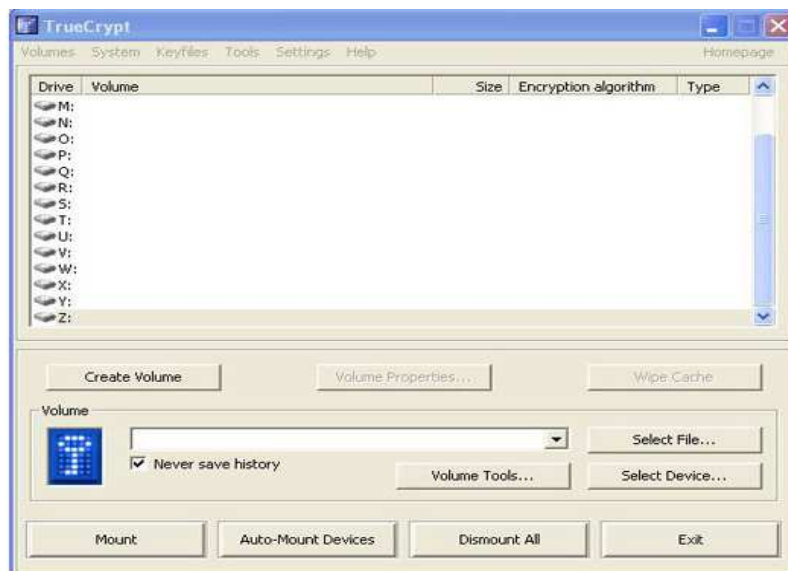
Modovi operacija:

	CBC - predvidljivi IVs	CBC - tajni IVs	CBC – nasumični ključ	LRW	XTS
BestCrypt	Ne	Da	Ne	Da	Da
BitLocker	Ne	Da	Ne	Ne	Ne
CrossCrypt	Da	Ne	Ne	Ne	Ne
DiskCryptor	Ne	Ne	Ne	Ne	Da
TrueCrypt	Da	Ne	Ne	Da	Da

Tabela 8.1.4. Poredjenje softvera na osnovu modova operacija

8.2. KORIŠĆENJE TRUECRYPT-A ZA ŠIFROVANJE DISKA

Prvo što radimo je da odemo na sajt TrueCrypt i skinemo i instaliramo program. Pokrenemo program, i prozor bi trebao da izgleda ovako, slika 8.2.1.¹²



Slika 8.2.1.

Postavljanje podešavanja za šifrovanje

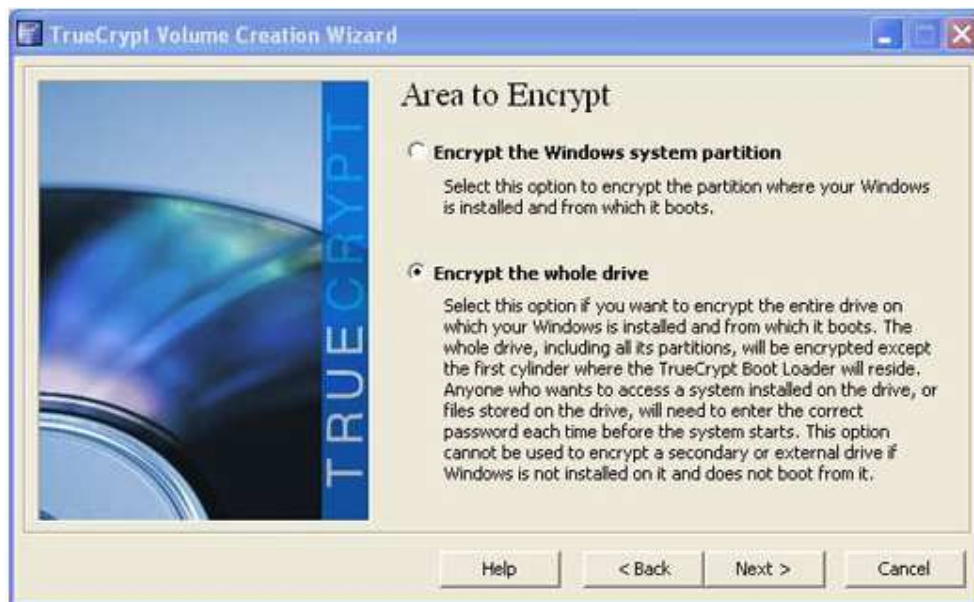
Kliknemo na 'Create volume' dugme. Na sledećem prozoru, obeležimo 'Encrypt the system partition or entire system drive', slika 8.2.2.



Slika 8.2.2.

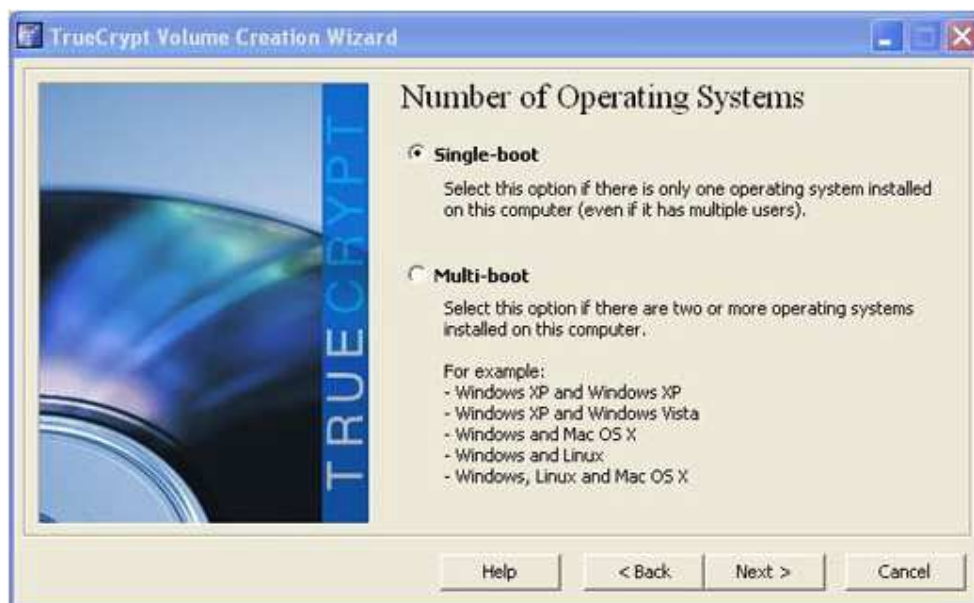
¹² <http://www.randyjensenonline.com/blog/using-truecrypt-to-encrypt-your-entire-hard-drive>, datum posete linka 9.7.2012. 17:00

Potom izaberemo opciju 'Encrypt the whole drive', slika 8.2.3.



Slika 8.2.3.

Za sledeći prozor imamo izbor 'Single boot' ili 'Multi boot'. S obzirom da imamo samo jedan OS na računaru, odabraćemo 'Single boot', slika 8.2.4.



Slika 8.2.4.

Sada odabiramo podešavanja za šifrovanje. Ukoliko stvarno ne znamo šta radimo, već podešeni parametri su u redu. AES je neverovatno jak algoritam za šifrovanje, slika 8.2.5.



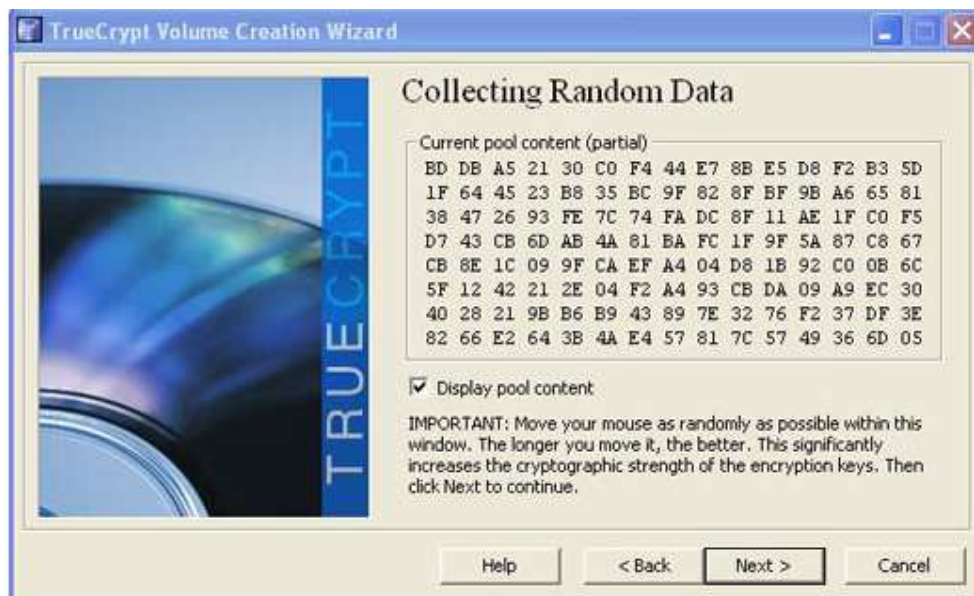
Slika 8.2.5.

Sledeći korak je postavljanje lozinke. U zavisnosti od toga koliko jaku i pouzdanu lozinku želimo da imamo, lozinka može biti duga i do 20 karaktera, slika 8.2.6.



Slika 8.2.6.

Sada moramo da pomeramo miša po prozoru TrueCrypta da napravimo slučajne podatke. Ovo je veoma važno, pa treba provesti minut dva da odradimo ovo, slika 8.2.7.



Slika 8.2.7.

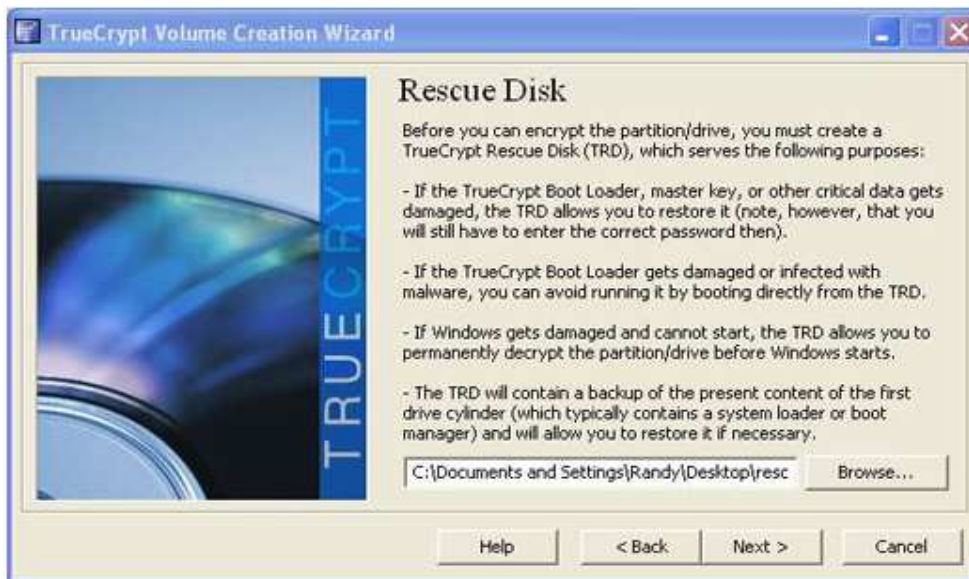
Sledeći prozor će pokazati šifru koju smo napravili, i kliknemo 'Next'.



Slika 8.2.8.

Pravljenje diska za spašavanje

Sledeći korak je da napravimo ono što TrueCrypt zove 'Rescue disk'. Disk će biti korišćen u slučaju 'boot'-ovanja, ili ako Windows bude zaražen, i uvek ćemo imati način da dešifrujemo sistem. Ovaj korak je veoma važan, i TrueCrypt neće dozvoliti da nastavimo ukoliko nije zadovoljan, mora biti urađeno sve tačno. Počinjemo klikom na 'Browse'. Pretražujemo gde ćemo sačuvati fajl, imenujemo ga sa ekstenzijom .iso, slika 8.2.9.



Slika 8.2.9.

Sledeći prozor nam govori da je fajl sačuvan. Sada ćemo ovaj .iso fajl narezati na CD.



Slika 8.2.10.

Posle narezivanja, ne vadimo disk i kliknemo 'Next', slika 8.2.11.



Slika 8.2.11.

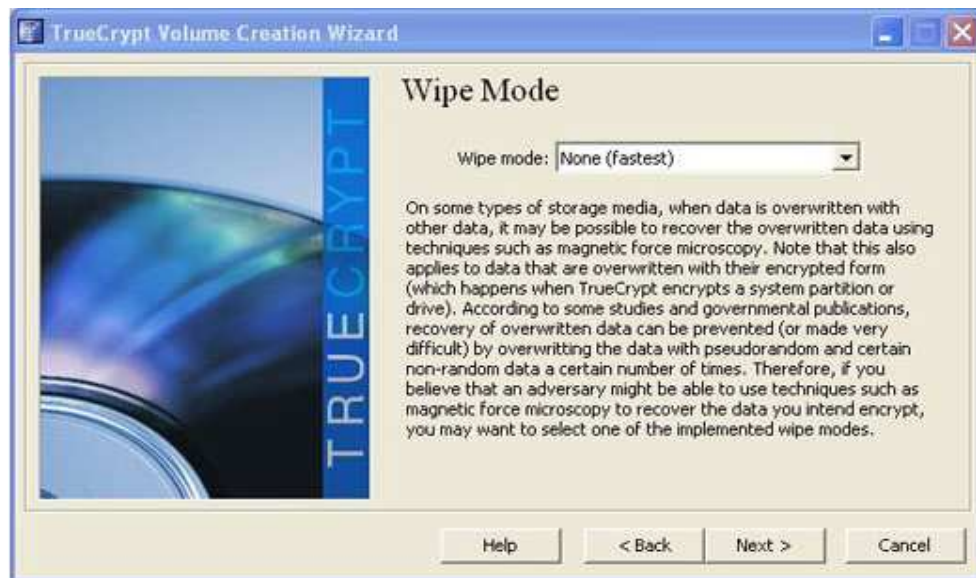
Ako je sve prošlo dobro, obavestiće nas da je Rescue Disk uspešno verifikovan, sl. 8.2.12.



Slika 8.2.12.

Testiranje i instaliranje Bootloader-a

Možemo izabrati da obrišemo dražv, i to će nam obezbediti veoma siguran hard disk, ili da ne brišemo, ako nećemo čuvati neke važne podatke, slika 8.2.13.



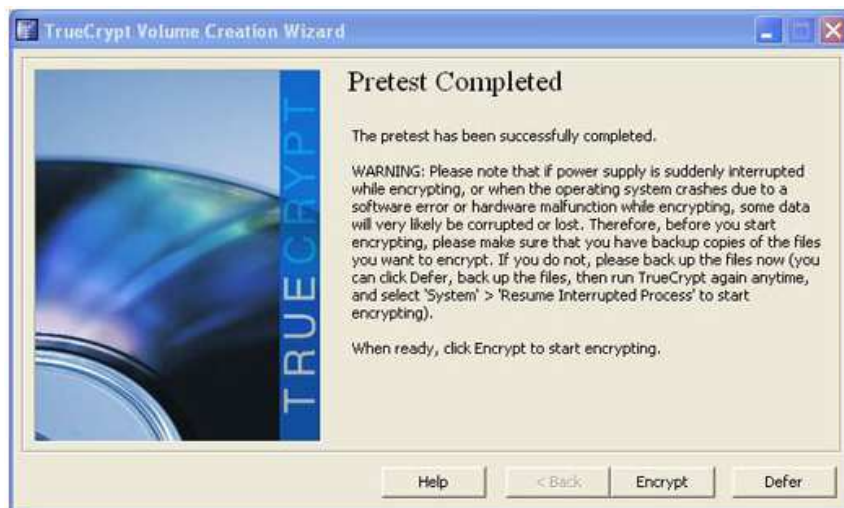
Slika 8.2.13.

Potom će TrueCrypt započeti test da vidi da li je sve u redu, pre nego što započne šifrovanje. Kliknemo na 'Test', slika 8.2.14.



Slika 8.2.14.

Otvora se prozor za restartovanje, naravno kliknemo na 'Yes'. Kad se kompjuter restartuje, videćemo crni prozor na kojem nam se traži sifra, i ukucavamo onu koju smo napravili. Ako je sve u redu, videćemo ovaj prozor, slika 8.2.15.



Slika 8.2.15.

Kliknemo na 'Encrypt' i proces započinje, slika 8.2.16.



Slika 8.2.16.

I na kraju dobijamo poruku, slika 8.2.17.

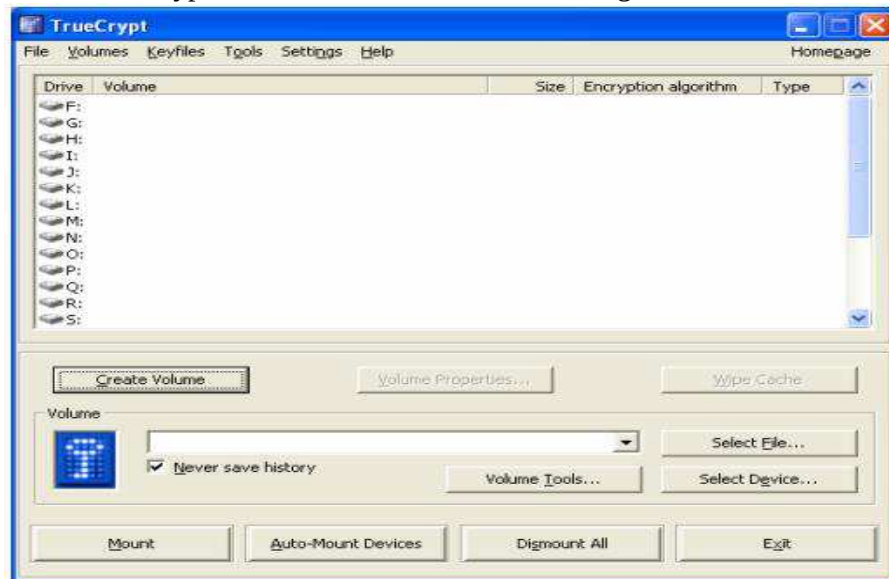


Slika 8.2.17.

8.3. KORIŠĆENJE TRUECRYPT-A ZA ŠIFROVANJE USB-a

Pretstavimo da je TrueCrypt već instaliran i da je USB prepoznat od strane Windowsa i da mu je dodeljeno slovo. I mora biti prazan.¹³

Pokrećemo TrueCrypt i kliknemo na 'Create volume' dugme, slika 8.3.1.



Slika 8.3.1.

Kliknemo 'Next' da bi napravili 'file container', slika 8.3.2.



Slika 8.3.2.

¹³ http://www.ucl.ac.uk/isd/common/cst/good_practice/encrypt/encrypt/EncryptingUSBTrueCrypt, datum posete linka 8.9.2012. 14:13

Izaberemo standardni TrueCrypt folder i kliknemo na 'Next', slika 8.3.3.



Slika 8.3.3.

Kliknemo na 'Select file', slika 8.3.4.



Slika 8.3.4.

Izaberemo naš USB i upišemo ime za kriptovan fajl. Ako postavimo ekstenziju .tc, automatski će biti prepoznata od strane Windowsa kao TrueCrypt fajl, što je preporučeno. Kliknemo 'Save', pa potom 'Next'.

Na sledećoj slici 8.3.5. možemo da biramo koje algoritamsko šifrovanje koristimo i koji 'hash' algoritam. Sve ove opcije nude dobro šifrovanje. Kliknemo 'Next' da potvrdimo izabrano.



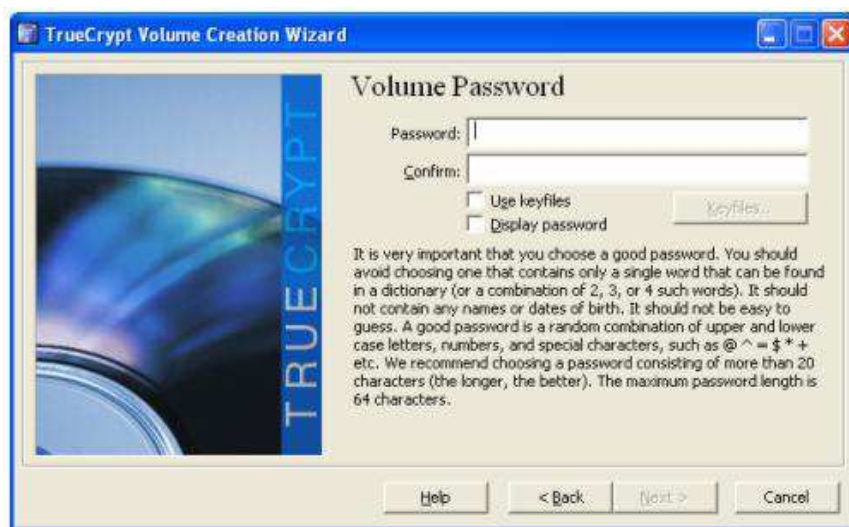
Slika 8.3.5.

Izaberemo veličinu TrueScript dela. Ne treba uzimati sav slobodan prostor, jer će neki deo biti potreban kasnije za TrueCrypt fajlove. Preporučeno je da se ostavi 8MB slobodno, slika 8.3.6.



Slika 8.3.6.

Izaberemo šifru, slika 8.3.7.



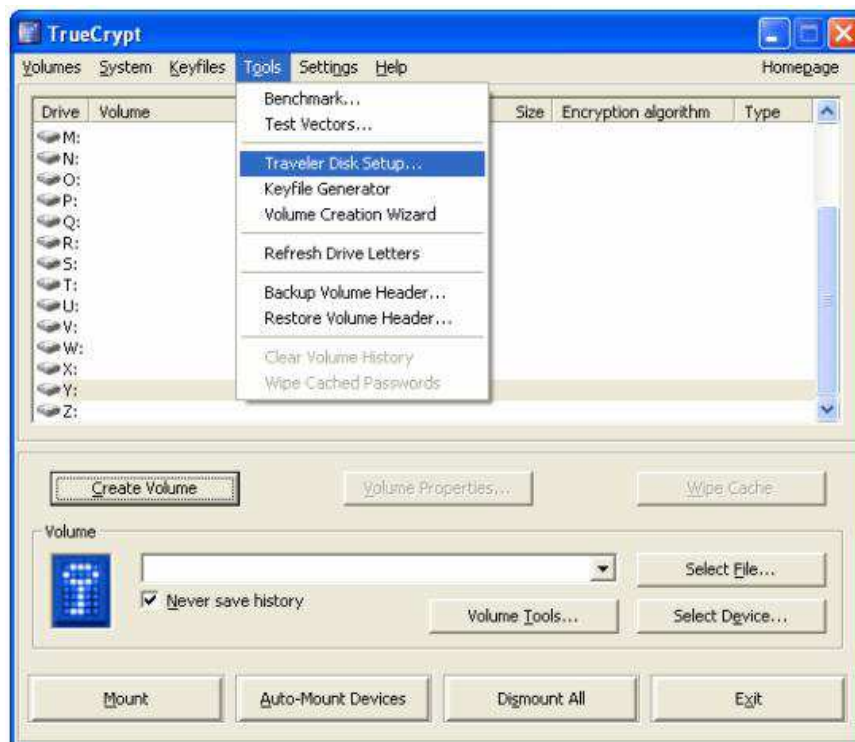
Slika 8.3.7.

Na sledećem prozoru pomeramo mišem preko ekrana, pre klika na 'Format'. Ovo omogućava nasumične informacije, koje pomažu za generisanje ključa za šifrovanje, slika 8.3.8.



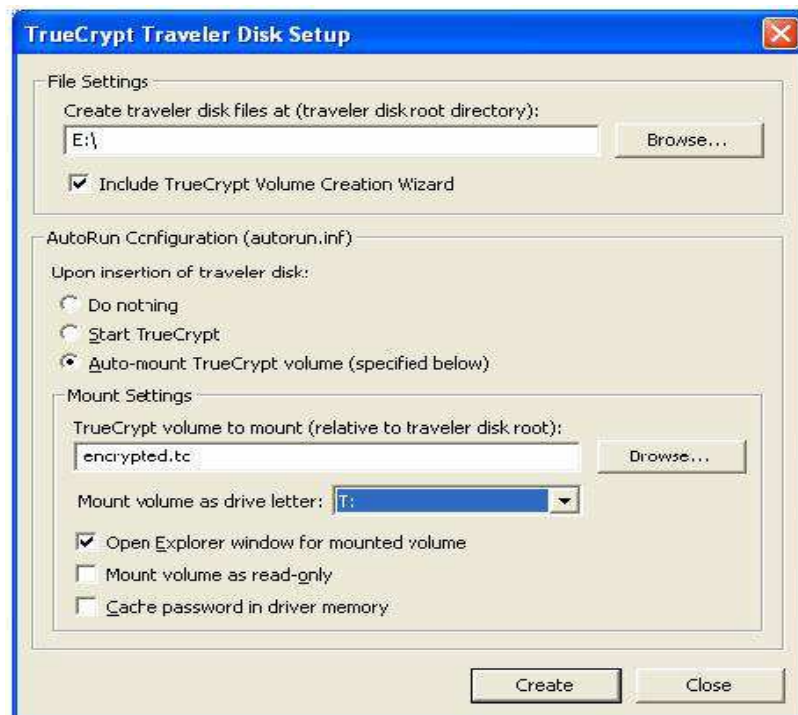
Slika 8.3.8.

Kliknemo na 'Next' i onda 'Cancel' da bi kompletirali proces. Na glavnom prozoru, kliknemo 'Tools' i onda 'Traveller Disk Setup', slika 8.3.9.



Slika 8.3.9.

Kliknemo 'Browse' i izaberemo naš USB, a u donjem delu izaberemo 'Auto-mount TrueCrypt volume', kliknemo 'Browse', i izaberemo .tc fajl, koji smo napravili, i izaberemo slovo za naš drajv (npr. T:). Kliknemo 'Create', slika 8.3.10.



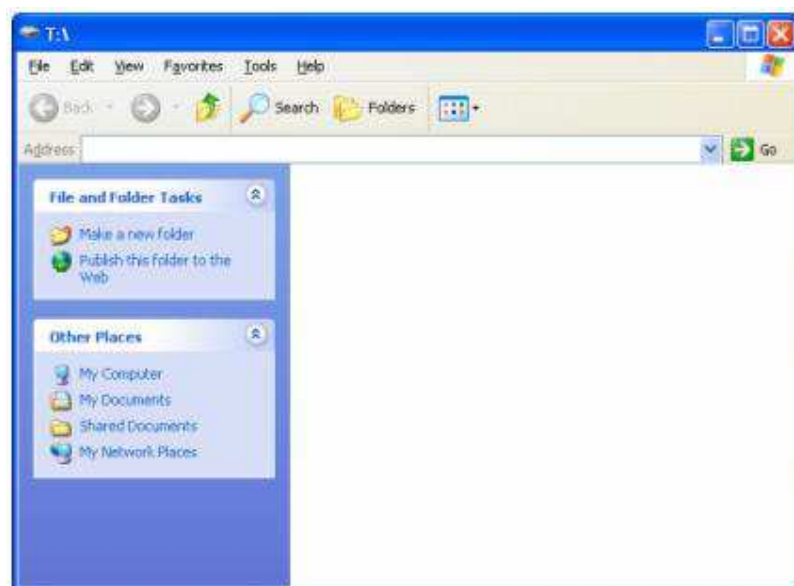
Slika 8.3.10.

Sledeći put kad ubacimo USB, Windows će nas pitati šta da radimo. Kliknemo OK na 'Mount TrueCrypt volume', i tražiće nam šifru, slika 8.3.11.



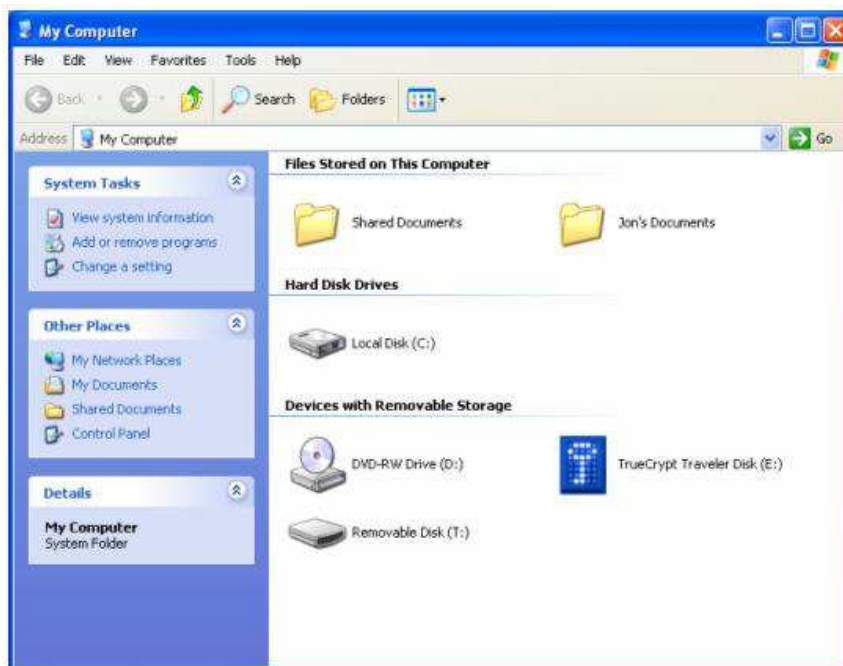
Slika 8.3.11.

Prozor koji se pojavi pokazuje sadržaj šifrovanog foldera. Biće mu dodeljeno slovo, koje smo izabrali u prethodnom koraku, slika 8.3.12.



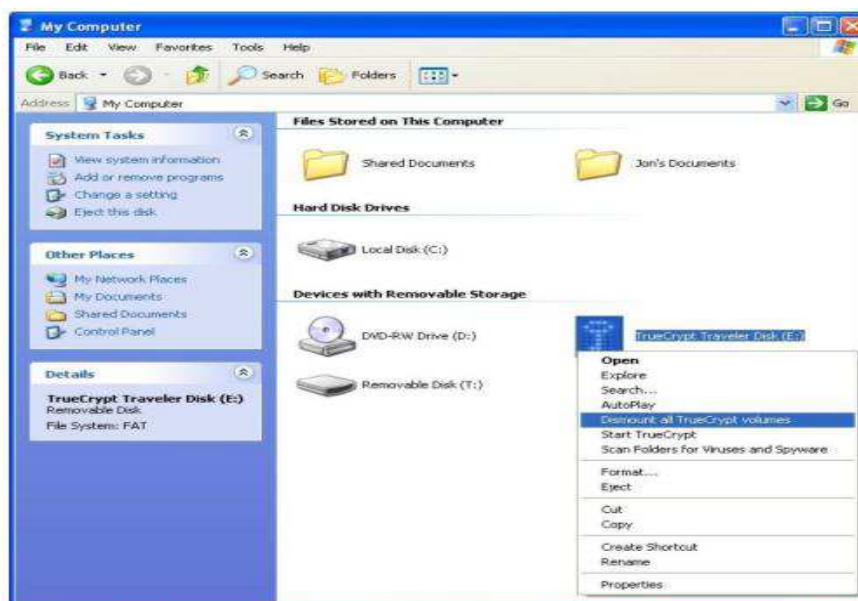
Slika 8.3.12.

USB sada ima 2 dodeljena slova, i to ne treba da nas buni. Na slici 8.3.13. vidimo USB drayv kao 'TrueCrypt Traveller Disk (E:)', koji sadrži TrueCrypt fajlove i šifrovan folder. Na njega ne treba čuvati fajlove. 'Removable disk (T:)' je šifrovani folder i tu treba da čuvamo fajlove.



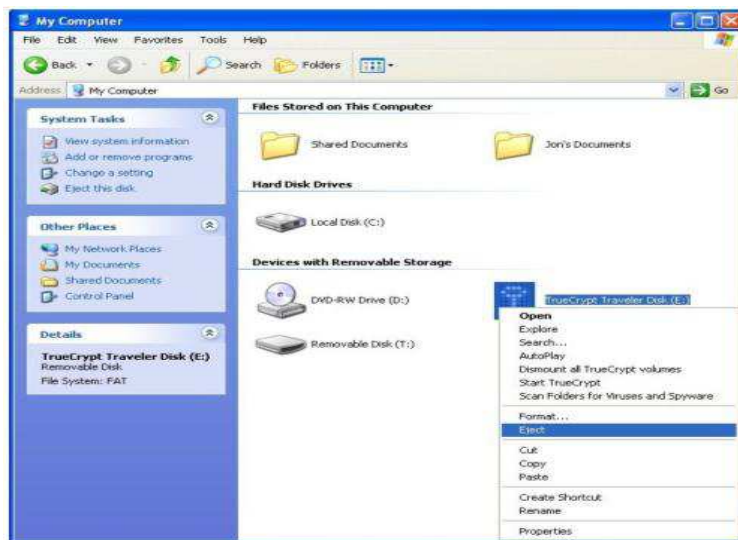
Slika 8.3.13.

Pre fizičkog isključivanja USB, prvo moramo otvoriti 'My computer' i desni klik na 'TrueCrypt Traveller Disk' i kliknuti na 'Dismount all TrueCrypt Volumes', slika 8.3.14.



Slika 8.3.14.

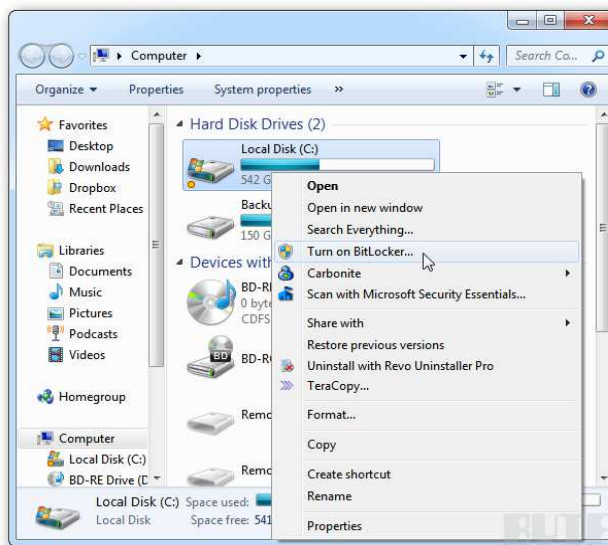
Potom opet desni klik i kliknemo na 'Eject'. I sada možemo izvaditi USB, slika 8.3.15.



Slika 8.3.15.

8.4. KORIŠĆENJE BITLOCKER-A ZA ŠIFROVANJE DISKA

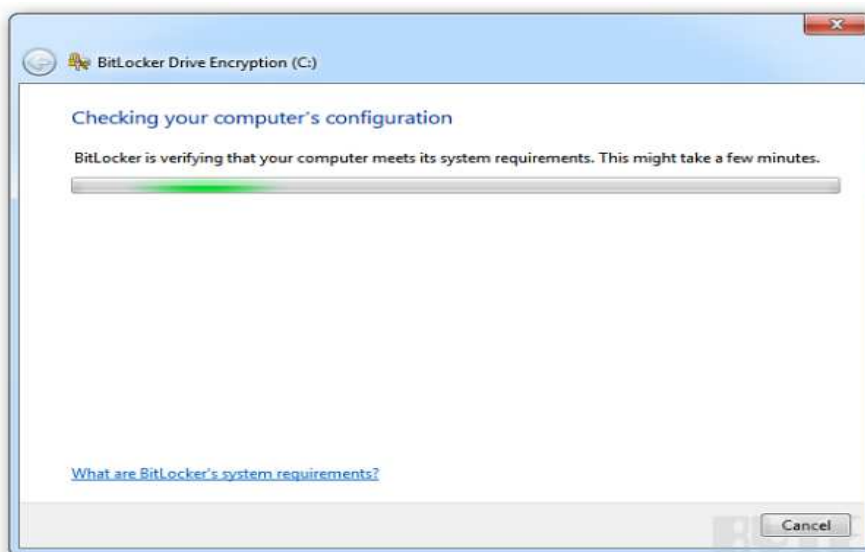
Pošto smo instalirali BitLocker, desnim klikom na dražv izaberemo 'Turn on BitLocker'¹⁴, slika 8.4.1.



Slika 8.4.1.

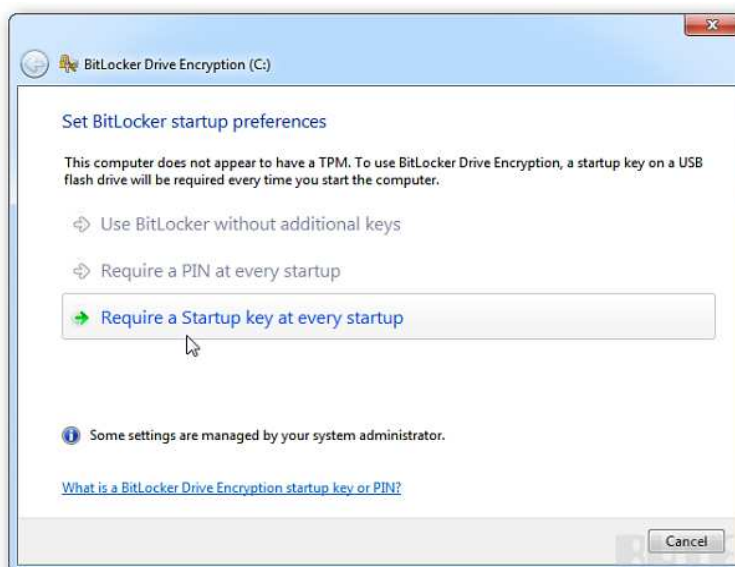
¹⁴ <http://www.informationweek.com/byte/howto/personal-tech/storage-memory/231000137>, datum posete linka 8.9.2012. 15:10

BitLocker će skenirati naš sistem da bi bio siguran da proces može da se nastavi, slika 8.4.2.. Može nas obavestiti da će biti napravljen novi sistemski drajv na praznom prostoru na drajvu C:. Ovde će BitLocker čuvati boot komponente. Posle ovoga, restartujemo kompjuter.

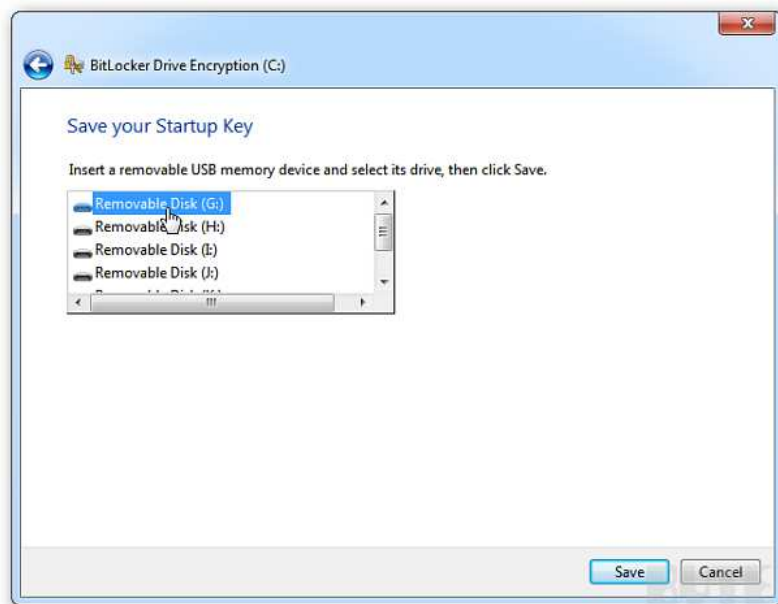


Slika 8.4.2.

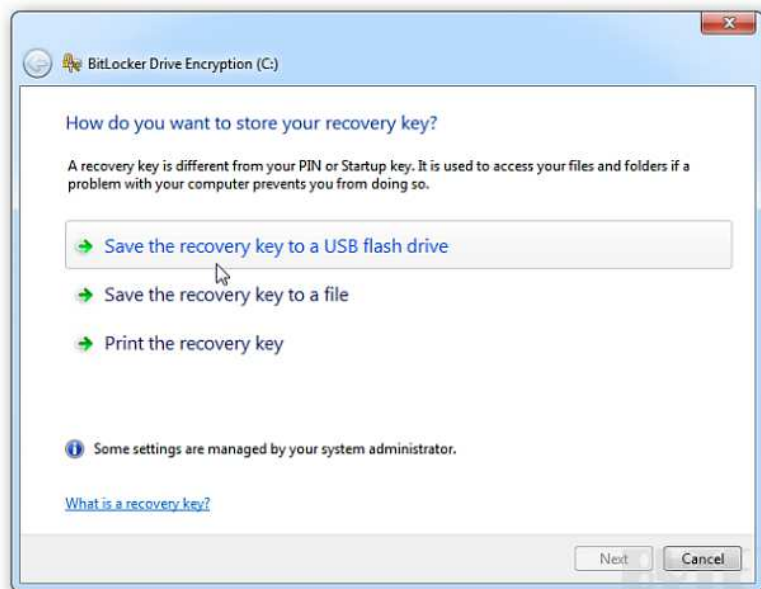
Potom konfigurišemo ključ za dešifrovanje. Samo ubacimo USB sa ključem pri startovanju računara ili ukucamo PIN. Kada izaberemo 'Require a Startup key', slika 8.4.3., sistem će zatražiti da ubacimo USB, i sačuvaće ključ za dešifrovanje, slika 8.4.4. Pitaće nas da sačuvamo kopiju rezervnog ključa, što bi trebali da uradimo, u slučaju da igubimo Startup ključ, slika 8.4.5.



Slika 8.4.3.

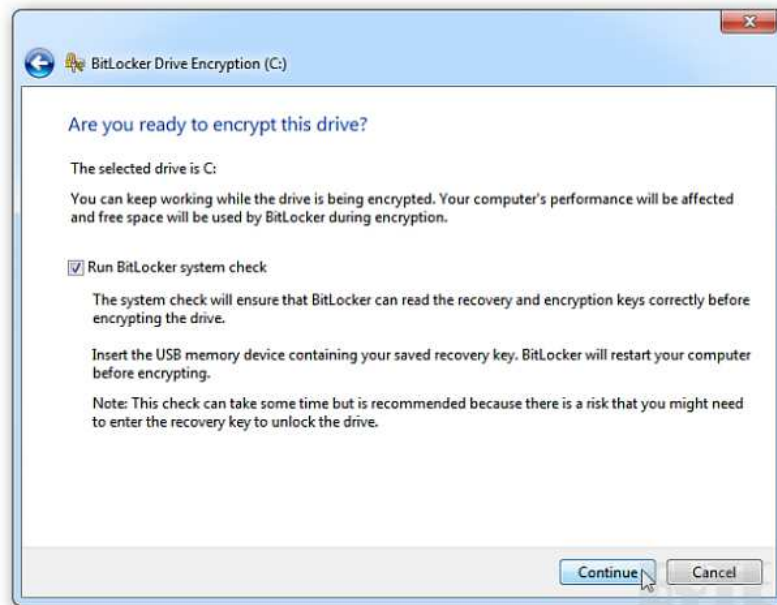


Slika 8.4.4.



Slika 8.4.5.

Pre početka šifrovanja, BitLocker će ponuditi sistemsku proveru. Ovo omogućava proveru Startup ključa, da li je čitljiv i da li dešifrovanje radi. Ceo proces traje par minuta, i preporučljivo je da se uradi, slika 8.4.6.



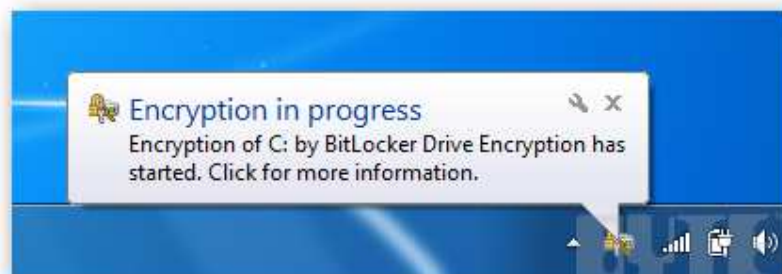
Slika 8.4.6.

Kad se proces završi potrebno je restartovati kompjuter, slika 8.4.7.



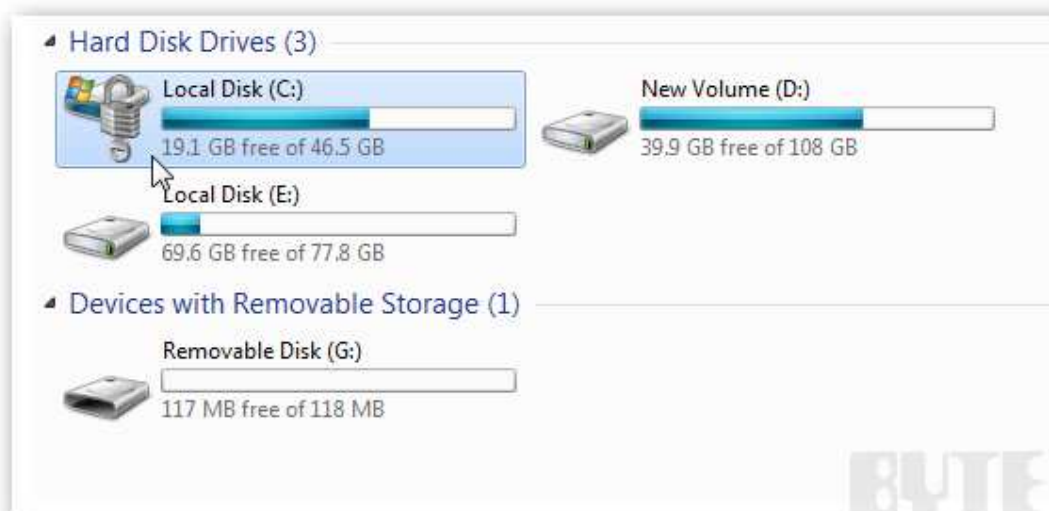
Slika 8.4.7.

Kada vidimo ovu poruku ne treba da uklanjamo ključ, inače se provera neće završiti i moraćemo sve ispočetka. Samo da potvrdimo ključ i nastavljamo proces. Posle ove provere, BitLocker će početi šifrovanje sistema u pozadini. Proces traje nekoliko sati. U toku operacije kompjuter se može koristiti, ali će sistem biti sporiji, slika 8.4.8.



Slika 8.4.8.

Šifrovani disk će imati zaključanu ikonicu, slika 8.4.9., i samo sistemski dražv je zaštićen, dok ostali koji je koriste kao pomoćni za čuvanje podataka, nisu. Njih možemo ručno da šifrujemo.



Slika 8.4.9.

9. ZAKLJUČAK

Sigurnost računarskih sistema postaje sve važnija, jer sve više korisnika na sve više načina koristi sve više informacija u računarskom svetu. U takvom sistemu postoji i sve veća opasnost od neovlašćene upotrebe informacija, podmetanja lažnih informacija ili uništavanja informacija. U računarskim sistemima informacije se prenose raznovrsnim otvorenim i nesigurnim komunikacijskim putevima. Pristup do tih puteva ne može se fizički zaštititi pa svaki neprijateljski nastrojen napadač može narušiti sigurnost sistema. Zbog toga zaštitni komunikacijski mehanizmi nad nesigurnim komunikacijskim kanalom postaju najvažniji oblik ostvarenja sigurnosti. Sa sigurnošću se danas može zaključiti da je najdelotvornija zaštita poruka njihovo šifrovanje.

Istorija nas je naučila da informacije mogu biti dobro prikrivene bez specijalno razvijenih tehnologija u tu svrhu, kao na primer sakrivanje religijskih informacija u delima srednjovekovnih umetnika, informacija koje na prvi pogled nisu primetne. Informacija može biti dobro skrivena na mnoge načine, a na još više načina otkrivena.

Transfer podataka na fizičkim medijima zahteva posebnu opreznost, jer se neovlašćenim korišćenjem istih mogu otkriti informacije koje mogu biti zloupotrebljene. Zato se mora obezbediti da u slučaju nestanka fizičkog medija informacije budu sigurne, a u slučaju dopremanja medija na željenu lokaciju ovlašćenoj osobi te informacije budu dostupne.

Veruje se da je zasluga razvijene međunarodne diplomatije za ne izbijanje sukoba po objavljivanju tajnih informacija od strane sajta Wikileaks. Pomenuti sajt je objavio na stotine hiljada tajnih dokumenata mnogih svetskih vlada i učinio ih javno dostupnim i time ugrozio mnoge živote i potencijalna partnerstva. U slučaju Wikileaksa nije bilo do probijanja šifara, krađe fizičkih medija, već su doušnici sajta koji su bili zaposleni u administracijama pomenutih vlada slali te medije.

Savremeno društvo egzistencionalno zavisi od zaštite podataka. Zbog bitnih podataka su se kroz istoriju vodile mnogi sukobi, od Krstaških ratova i informacije o lokaciji Svetog Grala do sukoba Alijanse sa Severnom Korejom zbog informacija o nuklearnom programu.

Nagli razvoj tehnologije računarskih sistema i mreža, doveo je do masovne razmene informacija i podataka. U toj razmeni pojavila se potreba za zaštitom poverljivih podataka od raznih krađa i zloupotreba, što je uslovalo pojavu novog pravca u oblasti bezbednosti podataka. Dalji razvoj tehnologije doprineo je poboljšanju karakteristika metoda koje doprinose bezbednosti podataka. Međutim, isti taj napredak doveo je do bržeg otkrivanja nedostataka i dodatno omogućio eventualne zloupotrebe. Tako su, tokom vremena, metode za zaštitu podataka postajale sve složenije i naprednije.

U osnovi priče o bezbednosti podataka u računarskim mrežama nalazi se kriptografija. Kriptografija je veoma dinamična nauka koju odlikuje uska povezanost između teorije i prakse. Na ovo ukazuje činjenica da se napredak u teoriji brzo implementira u praksi, gde se još brže testira. Otkrivanjem nedostataka odmah se unapređuje teorijski rad i stečena iskustva se upotrebljavaju za izradu nove i bolje metode. Kriptografija je veoma široka oblast, a u praksi se bazira na upotrebi kriptosistema koji se sastoje od algoritama za kriptovanje, jednog ili više ključeva, sistema za upravljanje ključevima, podataka u vidu standardnog i kriptovanog teksta. Na složenost dodatno ukazuju i činjenice da se kriptosistemi mogu realizovati hardverski, softverski ili hardversko-

softverski, kao i to da se prilikom realizacije moraju zadovoljiti osnovni sigurnosni servisi. Za realizaciju kriptografskih algoritma, koji su danas u upotrebi, koriste se složeni matematički izrazi kao i znanja iz elektronike i programiranja. Uprkos tome, napredak u postojećim kriptografskim algoritmima nastavlja se rastućim tempom, da bi zadovoljio potrebe širenja IT društva u kome živimo. Teško je zamisliti ozbiljnu PC aplikaciju koja u sebi nema implementiran neki sigurnosni algoritam, počev od bankarskih aplikacija, internet trgovine, pa sve do operativnih sistema. Takođe, kriptografski algoritmi za zaštitu su primenjivi u telekomunikacionim sistemima, televiziji, i drugim oblastima za koje često nismo ni svesni da ih čine ovi algoritami.

Sigurno je da će se kriptografija razvijati sve bržim i bržim koracima. Upotreba kvantnih računara, računarskih gridova kao i sve masovnije upotrebe računarskih mreža samo su jedan od nagoveštaja budućnosti. U skladu sa tim će se postavljati sve veći sigurnosni zahtevi u smislu ranog otkrivanja i sprečavanja zloupotreba. Odgovor na ove zahteve je upravo upotreba savremenijih i sigurnijih kriptografskih algoritama, koji će prevazilaziti granice jednostavne bezbednosti.

Zaključak koji se iz ovoga može izvesti je da ne postoji apsolutna zaštita informacija i da čovek kao faktor može iz savršeno kompleksnih sistema izvući najtajnije informacije ukoliko je u toj poziciji. Jasno je da apsolutna zaštita podataka ne postoji.

10. LITERATURA

1. Anucojić D. - Zaštita informacionih sistema i podataka, (2008), Prometej, Novi Sad;
2. Baigneres T, Junod P, Lu Y, Monnerat J, Vaudenay S. - A Classical Introduction to Cryptography Exercise Book, (2006), Springer, New York
3. Drakulić M. - Osnovi Kompjuterskog prava, (1996), DOPIS, Beograd;
4. Kostić M. - Zaštita podataka u sistemu zvanične statistke, (2006), Beograd;
5. Kurose J, Ross K. - Umrežavanje računara – od vrha ka dnu, (2005), Računarski fakultet Beograd, CET Beograd
6. Lilić S, Prlja D. - Pravna informatika-veština, (2008), Dosije, Beograd;
7. Petrović Đ. - Računari - Priručnik, (2010), Valjevo;
8. Pleskonjić D, Đorđević B, Ćurić M. - Sigurnost računarskih mreža, (2007), Mikroknjiga, Beograd;
9. Rankl W. - Smart Card Handbook, (1997) - John Wiley & Sons
10. Tomašević V. - Osnovi računarske tehnike, (2009), Beograd;
11. Velašević D. - Osnovni pojmovi i struktura zaštite podataka u računarskim sistemima, (1994), JISA - Časopis za informatiku, Beograd.
12. Zoreda J. L, Oton J. M. - Smart Cards, (1994), Artech House
13. www.wikipedia.org
14. www.randyjensenonline.com
15. www.scribd.com
16. www.ucl.ac.uk
17. www.informationweek.com