Kriptografija

Seminarski rad u okviru kursa
Računarstvo i društvo
Matematički fakultet

Milica Kostadinović

April 2022

Sažetak

Kriptografija [1] ili šifrovanje se bavi metodama čuvanja tajnosti informacija. U slučaju prenosa nekih ličnih, finansijskih, vojnih ili informacija državne bezbednosti sa jednog mesta na drugo, one postaju ranjive na razne načine pa kriptografija pomaže u očuvanju tih informacija i čini ih nedostupnim neželjenim strankama. Ova nauka je pokazala koliko je u stvari moćna, kada je Alan Tjuring svojom mašinom Kolos uspeo da presretne i dešifruje poruke nemačke Enigme, što je puno pomoglo saveznicima i uticalo na ishod Drugog svetskog rata. Ova nauka ima mnoštvo podgrana, jedna od njih je kriptoanaliza.

Sadržaj

1 Uvod

Kriptografske tehnike koje se koriste da bi se implementirali bezbednosni servisi su šifra i digitalni potpis. Osnovni element koji se koristi naziva se šifarski sistem ili algoritam šifrovanja. Svaki šifarski sistem obuhvata par transformacija podataka koje se nazivaju šifrovanje ili dešifrovanje u zavisnosti od smera transformacije. Šifrovanje je procedura koja transformiše neku originalnu informaciju u šifrovane podatke (šifrate), a obrnut proces tokom koga se rekonstruiše otvoreni tekst na osnovu šifrata je dešifrovanje. Prilikom šifrovanja pored otvorenog teksta se koristi jedna nezavisna vrednost koja se naziva ključ šifrovanja. Slično, transformacija za dešifrovanje koristi ključ dešifrovanja. Broj simbola koji predstavljaju ključ odnosno dužina ključa zavisi od šifarskog sistema i predstavlja jedan od parametara sigurnosti tog sistema. Kasnije ćemo u tabeli moći da vidimo neke primere dužine ključa.

Kriptoanaliza [2] je nauka koja se bavi razbijanjem šifri, odnosno otkrivanjem sadržaja otvorenog teksta na osnovu malopre spomenutog šifrata, i to bez poznavanja ključa. Ova nauka konkretno obuhvata proučavanje slabosti kriptografskih elemenata, kao što su na primer heš funkcije ili protokoli autentifikacije. Različite tehnike kriptoanalize nazivaju se napadi. Kriptoanaliza obično ne razmatra metode napada čija primarna meta nisu slabosti posmatranog kriptografskog sistema, kao što su potplaćivanje, fizička sila, provaljivanje, logovanje tastature, ili socijalno inženjerstvo, mada ovi tipovi napada jesu važna stavka, i češće dovode do rezultata nego tradicionalna kriptoanaliza.

2 Istorijat kriptografije

Prvi primeri slanja skrivenih poruka sežu do Herodota, koji ih je zabeležio u konfliktima između Grčke i Persije. Po Herodotovom mišljenju, umetnost pisanja tajnih, skrivenih poruka spasla je Grke od napada persijskog vladara Kserksa. Naime, Kserks je započeo izgradnju Persepolisa, nove prestonice svog carstva i pokloni su stizali odasvud, osim iz Atine i Sparte. Kako bi kaznio ovakvo pokazivanje prkosa, sledećih pet godina Kserks je mobilisao najveću armiju u istoriji i bio spreman da krene u iznenadni napad. Međutim, ovim pripremama bio je svedok Demaratus, Grk proteran iz domovine, mada još uvek lojalan Grčkoj. Rešio je da obavesti svoje sunarodnike na opasnost, ali je teškoća ležala u pronalaženju načina da se takva poruka dostavi bez znanja Persijanaca. Demaratus je sastrugao vosak sa drvenih tablica korišćenih za pisanje, napisao poruku i ponovo je prekrio voskom, tako da su tablice delovale prazno. Poruka je nesmetano stigla do Grka, koji su uklonili vosak, pročitali upozorenje i počeli da se pripremaju za rat. Kserks je izgubio element iznenađenja i na kraju, izgubio i sam rat.

Bilo je još dosta ovakvih priča vezanih za slanje skrivenih poruka u tom periodu. Verovatno jedna od najpoznatijih je o glasniku kome je obrijana kosa, poruka mu je zapisana na koži glave, sačekano je da mu kosa ponovo izraste i tek je onda poslat na put.

Sve ovo su primeri samo skrivanja poruka kako bi ostale tajne, ali ne i njihove izmene. Ovaj princip, koji se naziva steganografija, ostao je u upotrebi i hiljadama godina kasnije, često u kombinaciji sa kriptografijom.

Paralelno sa steganografijom, razvijala se i kriptografija čiji je cilj bilo skrivanje ne same poruke, već njenog značenja. Prvi zabeleženi primer šifre jeste Spartanska šifra skitale (400 godina p.n.e.). Ovo je primer šifre

transpozicije. Slova poruke ispisuju se na dugačkoj papirnoj traci i naizgled sačinjavaju poruku koja ništa ne znači, ali kada se obmota oko skitale, drvenog štapa čiji je dijametar ključ za šifrovanje, i pročita s leva na desno, odozgo na dole, dobija se otvoreni tekst poruke.

Slika 1: Izgled šifrovane poruke namotane oko skitale

Prva zabeležena upotreba šifre supstitucije u vojne svrhe pojavljuje se u „Galskim ratovima“ Julija Cezara i stoga se naziva Cezarova šifra [3]. Ova šifra svako slovo zamenjuje trećim slovom udesno od njega (duž abecede). Ako je reč o engleskom alfabetu, onda su zamene A->D, B->E,..,Z->C, pa šifrat CGUYR odgovara poruci ZDRAVO. Uopšte gledano, moguća je zamena osnovnog alfabeta drugim alfabetom sa proizvoljnim rasporedom slova. Ovakva šifra je jednostavna za implementaciju i pruža relativno visok nivo sigurnosti, makar u prvom milenijumu nove ere, kada nije postojao način da se dešifruje. Cezarova šifra dominirala je sve dok Al-Kindi, arapski naučnik iz devetog veka nove ere, nije pronašao način da razbije ovu monoalfabetsku šifru supstitucije metodom poznatom kao analiza učestalosti.

Sve do 20. veka nije bilo značajnijeg napretka u kriptografiji – primenjivane su uglavnom razne varijacije monoalfabetske šifre supstitucije koje su otežavale njeno dešifrovanje – jedan od primera je Vižnerova šifra iz 16. veka. Ova šifra koristi Vižnerov kvadrat kako bi se izvršilo šifrovanje metodom supstiticije, ali pomoću 26 alfabeta od kojih je svaki pomeren za po jedno slovo u odnosu na prethodni.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Slika 2: Vižanerova tablica

Sve do Drugog svetskog rata šifrovane poruke mogle su se koliko-toliko i dešifrovati. Na nemačkoj strani pojavila se mašina koja je šifrovala poruke na do tada još neviđen način. Nemci su mašinu nazvali Enigma. Međutim ma koliko god da je ona u to vreme bila revolucionarna saveznici su uspeli da razbiju poruke šifrovane Enigmom.

Posle Drugog svetskog rata i pojavom prvih računara otvorila su se nova vrata kriptografiji. Računari su vremenom postajali sve brži i brži, radeći i po nekoliko stotina, a kasnije i miliona operacija u sekundi. Novom brzinom rada je omogućeno probijanje šifri za sve manje vremena. Uporedo s tim, radilo se i na izmišljanju novih, sigurnijih i komplikovanijih algoritama za šifrovanje.

3 Šta kriptografija mora da obezbedi?

Bezbedan sistem treba da obezbedi nekoliko garancija kao što su poverljivost, integritet i dostupnost podataka, kao i autentičnost i neporicanje [4]. Kriptografija može da obezbedi poverljivost i integritet kako podataka u tranzitu, tako i podataka u mirovanju. Takođe može da autentifikuje pošiljaoce i primaoce jedne drugima.

Softverski sistemi često imaju više krajnjih tačaka, obično više klijenata i jedan ili više pozadinskih servera. Ova komunikacija klijent/server se odvija preko mreža kojima se ne može verovati. Komunikacija se odvija preko otvorenih, javnih mreža kao što je Internet, ili privatnih mreža koje mogu biti kompromitovane od strane spoljnih napadača ili zlonamernih insajdera.

Postoje dve glavne vrste napada koje protivnik može pokušati da izvrši na mreži. Pasivni napadi podrazumevaju da napadač jednostavno osluškuje mrežni segment i pokušava da pročita osetljive informacije dok putuju. Pasivni napadi mogu biti onlajn (u kojima napadač čita saobraćaj u realnom vremenu) ili oflajn (u kome napadač jednostavno hvata saobraćaj u realnom vremenu i pregleda ga kasnije - možda nakon što je proveo neko vreme u njegovom dešifrovanju). Aktivni napadi uključuju napadača koji se lažno predstavlja kao klijent ili server, presreće komunikaciju u tranzitu i pregleda i/ili modifikuje sadržaj pre nego što ga prosledi na nameravano odredište (ili ga potpuno odbaci).

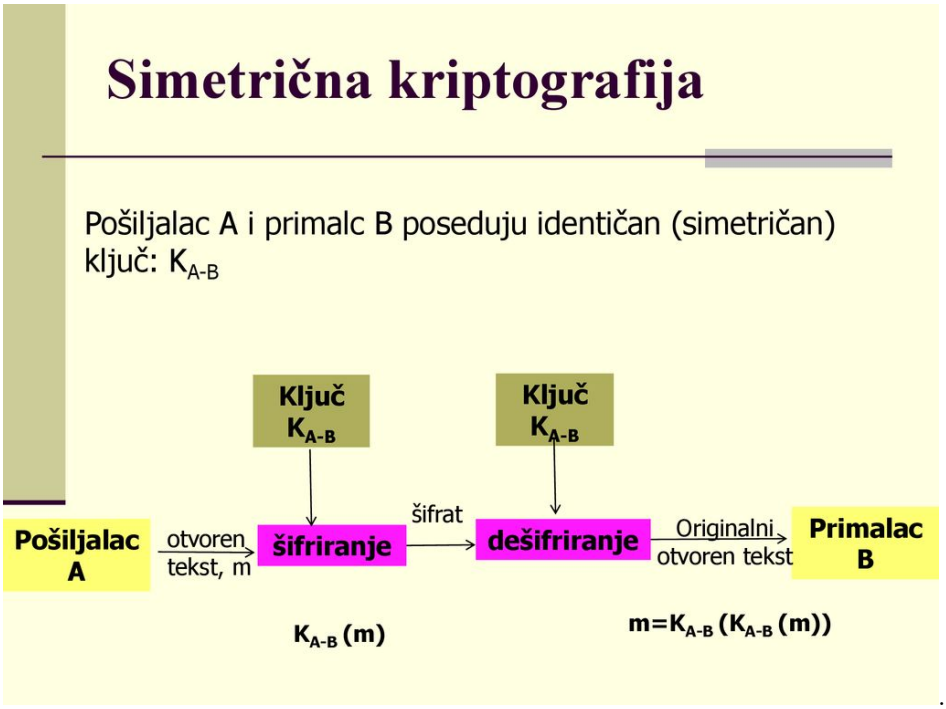
Zaštite poverljivosti i integriteta koje nude kriptografski protokoli kao što su SSL/TLS mogu zaštititi komunikaciju od zlonamernog prisluškivanja i manipulisanja. Zaštita autentičnosti obezbeđuje sigurnost da korisnici zaista komuniciraju sa sistemima kako je predviđeno. Na primer, šaljete li svoju lozinku za onlajn bankarstvo svojoj banci ili nekom drugom?

Takođe se može koristiti za zaštitu podataka u mirovanju. Podaci na prenosivom disku ili u bazi podataka mogu se šifrovati kako bi se sprečilo otkrivanje osetljivih podataka u slučaju gubitka ili krađe fizičkih medija. Pored toga, takođe može da obezbedi zaštitu integriteta podataka u mirovanju da bi se otkrilo zlonamerno neovlašćeno korišćenje.

4 Simetrična kriptografija

Kod simetrične enkripcije [5] koriste se isti ključ i za šifrovanje i za dešifrovanje. Baš zbog toga je raznovrsnost, a samim tim i sigurnost algoritama ovakve enkripcije velika. Bitan faktor je i brzina - simetrična enkripcija je veoma brza. Pored svih prednosti koje ima na polju sigurnosti i brzine algoritma, postoji i jedan veliki nedostatak. Kako preneti

tajni ključ? Problem je u tome, što ako se tajni ključ presretne, poruka se može pročitati. Zato se ovaj tip enkripcije najčešće koristi prilikom zaštite podataka koje ne delimo sa drugima.



Slika 3: Simetrična kriptografija

Klod Šenon je definisao uslove savršene tajnosti, polazeći od sledećih osnovnih pretpostavki:

1. Tajni ključ se koristi samo jednom
2. Kriptoanalitičar ima pristup samo kriptogramu

Šifarski sistem ispunjava uslove savršene tajnosti ako je otvoreni tekst X statistički nezavisan od kriptograma Y, što se može matematički izraziti na sledeći način: P(X=x|Y=y|=P(X=x). Drugim rečima, verovatnoća da slučajna promenljiva X ima vrednost x jednaka je sa poznavanjem vrednosti slučajne promenljive Y ili bez njega. Zbog toga kriptoanalitičar ne može bolje proceniti vrednost X poznavajući vrednost Y od procene bez njenog poznavanja. Koristeći pojam entropije iz teorije informacija, Šenon je odredio minimalnu veličinu ključa potrebnu da bi bili ispunjeni uslovi savršene tajnosti. Dužina ključa K mora biti najmanje jednaka dužini otvorenog teksta M: K >= M.

4.1 Sekvencijalni šifarski sistemi

Sekvencijalni šifarski sistemi se zasnivaju na svojstvu logičke operacije XOR: (X xor Y) xor Y = X, X, Y $\in (0, 1)$.

Naime, možemo zamisliti da nam je X jedan bit originalne poruke a Y bit ključa. Tada (X xor Y) = Z predstavlja jedan bit šifrata koji putuje javnim kanalima i koji neko može prisluškivati, dok je Z xor Y originalni bit X koji se dobija xor-ovanjem bita kodirane poruke sa bitom ključa. Definišimo još operaciju xor za proizvoljnu dužinu bita tj. bajtova i tada X, odnosno Y možemo smatrati bajtom, rečju odnosno porukom. U praksi se često koriste generatori pseudo slučajnih nizova (engl. PRNG – Pseudo Random Number Generator), koji predstavljaju determinističke algoritme za šifrovanje, ali nizovi simbola koje oni generišu imaju osobine slične slučajnim nizovima. Generatori pseudoslučajnih nizova koriste kratke ključeve radi započinjanja procesa generisanja. Ovi ključevi moraju biti prisutni na obe strane pre početka komuniciranja. Izlazni niz iz generatora se sabira po modulu 2 sa nizom otvorenog teksta i na taj način se dobija niz šifrata. Na prijemnoj strani se sabira primljeni niz šifrata sa pseudoslučajnim nizom generisanim pomoću istog ključa, počevši od istog početnog simbola kao i na predajnoj strani. Na taj način je prijemnik u stanju da rekonstruiše otvoreni tekst. Jasno je da dokle god se slučajni nizovi dobijaju pomoću bilo kog algoritma oni mogu biti samo pseudoslučajni i kao takvi postaju mamac za sve one koji se bave razbijanjem šifri. Pseudoslučajni nizovi su periodični u širem smislu (što znači da mogu imati aperiodični početak), ali ako su periodi takvih nizova mnogo veći od dužina nizova otvorenog teksta, sistem će se ponašati na sličan način kao i Vernamova šifra (sastoji se iz pomeranja svakog znaka poruke za nasumično odabrani broj mesta u abecedi). Osnovna ideja koja stoji iza sekvencijalnih šifara je da se generiše duga i nepredvidljiva sekvenca simbola iz nekog alfabeta (npr. binarnog) na osnovu kratkog ključa izabranog na slučajan način. Sekvencijalna šifra sa generatorom pseudoslučajnog niza je aproksimacija Vernamove šifre, i utoliko je bolja ukoliko je pseudoslučajni niz bliži po karakteristikama pravom slučajnom nizu.

5 Asimetrična kriptografija

Za razliku od simetrične kriptografije, koja podrazumeva postojanje jednog kjuča, asimetrična kriptografija uvodi postojanje još jednog ključa. Jedan ključ ostaje skriven od ostalih učesnika i naziva se privatni ključ, dok je drugi ključ poznat svim učesnicima i naziva se javni ključ. Ovakva postavka se može koristiti na dva načina:

- Privatni ključ se koristi za enkripciju, javni ključ za dekripciju
- Javni ključ se koristi za enkripciju, privatni ključ za dekripciju

U zavisnosti od cilja, bira se jedan od dva navedena pristupa. Tri osnovne primene asimetrične kriptografije su: enkripcija, razmena ključa i digitalni potpis. Upotreba asimetrične kriptografije široko je zastupljena, od HTTPS/SSL protokola koji se koriste na većini veb sajtova, do kriptovaluta gde javni ključevi predstavljaju identitete elektronskih novčanika. Isti algoritmi se mogu koristiti za više namena. Jednom privatnom ključu odgovara jedan javni ključ i obrnuto. Poznavanjem javnog ključa izuzetno je teško rekonstruisati privatni ključ.

Prednost ovog načina šifrovanja je u tome što ne mora da se brine o slučaju da neko presretne javni ključ, jer pomoću njega može samo da šifruje podatke. Takođe, programi sa ovakvim načinom šifrovanja imaju opciju da potpisuju elektronske dokumente (o tome će biti reči nešto kasnije). Pojam sistema sa javnim ključevima uveli su Difi i Helman 1976. godine. Prvi takav sistem koji su oni definisali bio je protokol, poznat pod imenom razmena ključeva Difi-Helman. 1977. godine objavljen je najčuveniji i najpopularniji algoritam za asimetričnu kriptografiju RSA, čije ime predstavlja skraćenicu sačinjenu od prvih slova prezimena autora Rona Rivesta, Adija Šamira i Leonarda Ejdlmana.

Ime ključa	Dužina ključa
DES(Data encryption standard)	56 bita
Triple DES, DESX, GDES, RDES	168 bita
Rivest - RC2, RC4, RC5, RC6	promenljive dužine čak do 2048 bita
IDEA-osnovni algoritam za PGP	128 bita
AES (Advanced encryption standard)	128, 192 ili 256 bita

Tabela 1: Primeri asimetričnih ključeva

5.1 Enkripcija

Kao što je bio slučaj i kod simetričnih šifara, enkripcija podataka podrazumeva skrivanje podataka od svih učesnika koji nemaju ključ kojim se podaci mogu otkriti. Asimetrična kriptografija koristi javni ključ primaoca za enkriptovanje podataka a privatni ključ primaoca za dekriptovanje podataka. Iako je moguće, asimetrična enkripcija nije pogodna za enkriptovanje velike količine podataka zbog svoje brzine, za razliku od simetričnih šifara koji su i do 1000 puta brži od asimetričnih. Iz tog razloga, simetrična kriptografija se koristi u specifičnim okolnostima gde je količina podataka mala i gde osobine asimetrične kriptografije daju najveći doprinos. Čest scenario je enkripcija podataka simetričnim ključem a zatim korišćenje algoritama asimetrične kriptografije za enkripciju simetričnog ključa koji se zajedno sa enkriptovanim podacima šalje primaocu

5.2 Razmena ključa

Razmena ključa može se smatrati posebnim oblikom enkripcije, gde je cilj skriveno (nerazumljivo za ostale učesnike) dogovoriti simetrični ključ koji će se nadalje koristiti za enkripciju podataka koji se prenose između učesnika koji učestvuju u razmeni. U zavisnosti od algoritma, ključ se može preneti enkripcijom privatnim ključem od strane oba učesnika, bez potrebe dekripcije (npr. Diffie-Hellman razmena) dok se kod drugih algoritama vrši enkripcija javnim ključem primaoca i dekripcija privatnim ključem primaoca, kao što je uobičajen slučaj kod enkripcije (npr. RSA).

5.3 Digitalni potpis

Digitalni potpis se koristi za potrebe identifikacije. Učesnik svojim privatnim ključem potpisuje (enkriptuje) podatke (ugovore, izjave, potvrde) dok je javni ključ učesnika registrovan kod autorizacionog tela i koristi se za proveru (dekripciju) podataka radi utvrđivanja da je podatke zaista enkriptovao vlasnik odgovarajućeg privatnog ključa. Kako je navedeno da se asimetrična kriptografija ne koristi za enkripciju velikih podataka, praksa je da se podaci prvobitno heširaju nekom od heš funkcija koja podatke preslikava u mali domen fiksne dužine a zatim se dobijeni rezultat heširanja enkriptuje privatnim ključem (npr. SHA256 + RSA), pri čemu rezultujući enkriptovani heš predstavlja digitalni potpis podataka.

6 Heš funkcija

Heš funkcija je svaki algoritam koji podacima proizvoljne dužine dodeljuje podatke fiksne dužine. Vrednost koju vraća heš funkcija zove se heš vrednost ili heš kod.

Navedeni algoritmi šifrovanja ne štite integritet odnosno verodostojnost poruke koja je šifrovana. Ovo je vrlo važno iz razloga jer je moguće da je ključ provaljen i da nam napadač šalje lažne poruke, ali postoji i mogućnost da je došlo do greške

prilikom šifrovanja, tako da primljena poruka nije identična originalnom dokumentu. Iz tog razloga kreirane su funkcije za sažimanje ili heš algoritmi (mogu se susresti i pod imenima engl. one-way, hash function, message digest, fingerprint). Najpoznatiji i najkorišćeniji heš algoritmi su SHA-1, MD5, MDC-2, RIPEMD-160 itd. Heš algoritmi se svrstavaju u kriptografske algoritme bez ključa.

7 Podela podataka

Potreba za primenom kriptografskih mera zaštite varira u zavisnosti od prirode podataka koje treba zaštiti i potencijalne vrednosti ovih podataka za one koji bi neovlašćeno došli u njihov posed.

Podaci mogu biti:

1. javni podaci - podaci u koje svi imaju uvid,

2. autorizovani podaci - podaci u koje isto svi imaju uvid, ali su od korišćcenja zaštićeni autorskim pravom

3. poverljivi podaci - podaci koji su tajni ali njihovo postojanje nije,

4. tajni podaci - podaci kod kojih i njihovo postojanje predstavlja tajnu.

Predmet zaštite moraju biti samo poverljivi i tajni podaci. Osobe koje neovlašćeno pristupaju podacima sa namerom da ih unište ili zloupotrebe su hakeri. Njihove akcije se smatraju kompjuterskim kriminalnom, a njihova motivacija su slava i novac.

8 IBM i kriptografija

1976. godine IBM Corporation je ušla u kriptografski posao kada je Lloid's Banking Group sklopila ugovor sa IBM-om da dizajnira bankarski sistem orijentisan na daljinski terminal. To je dovelo do sada sveprisutnih automatizovanih bankomata (ATM) na kojima su se mogli obavljati izdavanje gotovine i povezane bankarske transakcije.

Poslovne prednosti bankarstva orijentisanog na bankomat bile su očigledne bankarskoj zajednici. Mogao bi biti: dostupan 24/7, implementiran van banaka na prodajnim terminalima u hotelima ili supermarketima. Bankomatsko bankarstvo je bilo isplativo za banke i pojednostavjeno je upravljanje gotovinom na odmorima.

Banke su insistirale da klijent bude autentifikovan pre nego što se nastavi sa bankomatskom transakcijom. Da bi rešio zabrinutost banke, IBM je predložio ATM autentifikaciju koristeći dva kriptografski povezana identifikatora klijenata. Klijent bi počeo tako što bi ubacio bankovnu karticu u bankomat koji bi pročitao prvi identifikator klijenta, broj ličnog računa (PAN). Zatim, korisnik na tastaturi unosi drugi identifikator, lični identifikacioni broj (PIN). Kriptografija je obezbedila ispravan odnos između PAN-a i PIN-a koji je verifikovan da bi omogucio transakciju. Banke su upozorile klijente da čuvaju svoje PIN-ove u tajnosti i da ih ne pišu na bankovnoj kartici.

9 Budućnost kriptografije

Kvantna i DNK kriptografija će možda u nekoj skoroj budućnosti predstavljati osnov za zaštitu poverljivih dokumenata. Kvantna kriptografija nastala je kao posledica otkrića u oblasti kvantnog računarstva. Ona se zasniva na jednom od osnovnih principa kvantne fizike: Hajzenbergovom principu neodređenosti (što je preciznije jedno svojstvo izmereno, to se manje precizno drugo svojstvo može izmeriti). Leonard Ejdlman, jedan od tvoraca RSA algoritma, došao je na ideju korišćenja DNK kao računara. On je pretpostavio da se DNK može smatrati kao računar ogromne snage sposobne za paralelno izvršavanje operacija. Time se brzina izvršavanja eksponencijalno povećava u odnosu na obične računare.

10 Zanimljivosti

1. Šagborou – Šagborou Hol, velika vila u Engleskoj, postala je poznata po kipu pastira u uglu parka. Na kipu je pismo u šifri koju niko nije uspeo 'razbiti'.

2. Pamflet Bil – sastoji se od tri šifrovana teksta. Drugi od njih je dešifrovan i govori o zakopanom blagu. Ali, ostatak teksta govori o njegovoj tačnoj lokaciji, a on nije dešifrovan.

3. Ispred sedišta CIA-e u Virdžiniji nalazi se skulptura Džima Sanborna. Ironija je u tome što deo koda na njoj ne mogu razbiti briljantni kriptografi koji rade u CIA-i.

11 Zaključak

Kriptografija je postala i relevantna i važna u našim životima, ne samo kao rezultat bankomata pojednostavljenog bankarstva, već i zbog pojave e-trgovine, kupovine proizvoda i usluga preko elektronskih sistema poput Interneta. Otvoreno možemo reći da je kriptografija svetu donela odredjen nivo privatnosti, za kojim svi žudimo u nekim situacijama. Najvise je ima u vojnim i državnim sistemima jer su ipak te tajne najčuvanije i najvažnije za veliki broj ljudi ako ne i naroda. Jedno je sigurno, svakoj vrsti kriptografije se nađe neka mana i rupa s kojom bi se ona dešifrovala, ali svakim danom nastane novi algoritam, ključ, ili sama vrsta kriptografije pa se nivo bezbednosti uvek vrati na odgovarajući.

Literatura

[1] Alan Konheim: To Let Them Monitor or Not ... Is that the Real Question? in IEEE Technology and Society Magazine, June 2017, https://technologyandsociety.org/to-let-them-monitor-or-not-perhaps-that-is-not-the-real-question/

[2] Sandy Zabell: To Let Them Monitor or Not ... Is that the Real Question? in IEEE Technology and Society Magazine, June 2017, https://technologyandsociety.org/the-enigma-andred-hodges/

[3] Wikipedia: Kriptografija, https://sh.wikipedia.org/wiki/Kriptografija

[4] Synopsys: Cryptography, https://www.synopsys.com/glossary/what-is-cryptography.html

[5] Peter Smirnoff, Dawn M. Turner: Symmetric Key Encryption - why, where and how it's used in banking, https://www.cryptomathic.com/news-e...ow-its-used-in-banking