Seminarski rad o Kriptografiji

Seminarski rad u okviru kursa
Tehničko i naučno pisanje
Matematički fakultet

Stefan Lazović
mi15290@alas.matf.bg.ac.rs

8.11.2015

Apstrakt

Kriptografija 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, kriptografija pomaže u očuvanju tih informacija i čini ih nedostupnim neželjenim strankama. Ova nauka je pokazala koliko je ustvari moćna, kada je Alan Tjuring svojom mašinom **Kolos** uspeo da presretne i dešifruje poruke nemacče Enigme, što je u velikom pomoglo saveznicima i uticalo na ishod Drugog svetskog rata. Ova nauka ima mnoštvo podgrana, jedna od njih je kriptoanaliza.

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 sifrovanja. Svaki šifarski sistem obuhvata par transformacija podataka koje se nazivaju sifrovanje ili dešifrovanje u zavisnosti od smera transformacije. Šifrovanje bi bila procedura koja transforšise neku originalnu informaciju u šifrovane podatke (šifrate). Dok bi obrnut proces tokom koga se rekonstruiše otvoreni tekst na osnovu šifrata bio dešifrovanje.

Prilikom šifrovanja pored otvorenog teksta se koristi jedna nezavisna vrednost koja se naziva ključ šifrovanja. Slicno, 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 na tabeli moći da vidimo neke primere dužine ključa.

Kriptoanaliza 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 sto su na primer heš funkcije ili protokoli autentifikacije. Različite tehnike kriptoanalize nazivaju se **napadi**.

1.1 Istorija kriptografije

Kriptografija je ugledala svetlost dana u vreme kada je pismo postalo sredstvo komunikacije i kad se stvorila potreba da se ona čuvaju od tudjih pogleda. Od početka enkripcija se koristila u vojne svrhe. Jedan od prvih vojskovodja, sam Julije Cezar je koristio šifrovane poruke. Kada bi slao poruke svojim podredjenim vojskovodjama on ih je šifrovao tako sto je sva ili pojedina slova pomerao za 3 ili više mesta u abecedi, i tu poruku su mogli da dešifruju samo oni koji su poznavali **pomeri za** pravilo.

Primer 1.1 *[1]*

Poznata Cezarova izjava prilikom prelaska Rubikona u šifrovanom dopisivanju glasila bi: fqkf ofkhz kyz, ali pomicanjem svakog slova za šest mesta u abecedi, lako se može pročitati Alea iacta est, odnosno kocka je bacena.

Kriptografija mora da obezbedi sledeće:

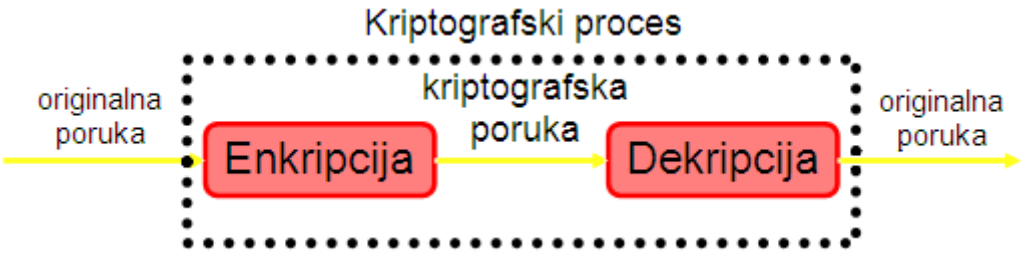
1. Integritet ili verodostojnost informacija koje se šifruju (engl. *Data integrity*) se brine o tome da ne dodje do neovlašćene promene informacija. Da bi se on osigurao mora postojati način provere da li je informacija promenjena od strane neovlašćene osobe.

2. Tajnost (engl. *Confidentiality*) informacija koja osigurava da je ona dostupna samo odredjenim ovlašćenim osobama, odnosno onim koje poseduju ključ. Postoje mnogi načini zaštite tajnosti, počev od fizičke zaštite do matematičkih algoritama koji skrivaju podatke.

3. Provera identiteta (engl. *Authentification*), korisnici koji počinju komunikaciju treba prvo da se predstave jedan drugom pa tek onda da počnu sa razmenom informacija.

4. Odgovornost, koja čini veliku ulogu u današnje vreme, najviše zbog toga sto se danas veliki deo novčanih transakcija obavlja putem interneta.

2 Simetrična i asimetrična kriptografija



Slika 1: Šifrovanje

Ključevi su minimalna potrebna informacija koju dve osobe moraju da dele ako žele da razmenjuju podatke na siguran način. Prema odnosu ključeva u kriptografskom sistemu delimo ih na:

- Simetrične
- Asimetrične.

Nivo zaštite zavisi od zaštite kljuca, a ne od zaštite algoritma. Zadatak algoritma je zaštiti podatke onoliko vremena koliko oni moraju da budu tajni. Takodje, potrebno je da bude zadovoljen uslov da broj podataka šifrovanih jednim ključem bude manji od broja potrebnih podataka da se dati algoritam razbije.

Tabela 1: Neki primeri asimetričnih ključeva [2]

Ime kljuca	Duzina kljuca
DES (Data encryption standard)	56 bita
Triple DES, DESX, GDES, RDES	168 bita
Rivest - RC2, RC4, RC5, RC6	promenljive duzine cak do 2048 bita
IDEA-osnovni algoritam za PGP	128 bita
Blowfish	448 bita
AES (Advanced encryption standard)	128,192 ili 256 bita

Kod simetrične enkripicije se koriste isti ključ za šifrovanje i dešifrovanje. Bas zato je raznovrsnost i sama sigurnost algoritma ovakve enkripcije velika. Bitan faktor je i brzina kojom se odlikuje ova vrsta enkripcije. Ali postoji jedan veliki nedostatak, kako preneti ključ? Problem je što ako se tajni presretne, poruka se moze pročitati. Zato se ovaj tip enkripcije najčešće koristi prilikom zaštite podataka koje ne delimo sa drugima.

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.

On je takodje odredio minimalnu veličinu ključa potrebnu da bi bili ispunjeni uslovi savršene tajnosti. Naime, dužina ključa K mora biti najmanje jednaka dužini otvorenog teksta M ($K \geq M$).

2.1 Asimetrična kriptografija

Za razliku od simetrične, asimetrična kriptografija koristi dva ključa - **javni i privatni**. Princip je sledeći: u isto vreme se prave privatni i odgovarajući javni ključ. Javni ključ se daje osobama koje šalju šifrovane podatke. Pomoću njega te osobe šifruju poruku koju žele da posalju. Kada primalac dobije šifrat, dešifruje ga pomocu svog privatnog ključa. Na taj nacin svaki primalac ima svoj privatni ključ a javni se može dati bilo kome, pošto se on koristi samo za šifrovanje a ne i za dešifrovanje.

Prednost ovog nacina šifrovanja je u tome što ne mora da se brine o slucaju da neko presretne javni ključ - jer pomoću njega moze samo da šifruje podatke. Takodje programi sa ovakvim načinom šifrovanja imaju opciju da potpisuju elektronske dokumente.

2.2 Funkcija za sažimanje - heš funkcija

Gore 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 i mogućnosti 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 (mogu se susresti i pod engleskim imenima: *one-way, has function, message digest, fingerprint)* algoritmi. Najpoznatiji, takodje i najkorišćeniji heš algoritmi su **SHA-1, MD5, MDC-2, RIPEMD-160...**. Heš algoritmi se svrstavaju u kriptografske algoritme bez ključa.

2.3 Digitalni potpisi

[3]

Svrha digitalnog potpisa je da potvrdi autentičnost sadržaja poruke odnosno da dokaže da poruka nije promenjena na putu od pošiljaoca do primaoca, kao i da obezbedi garantovanje identiteta pošiljaoca poruke. Pomoću svog potpisa korisnik ovlašćuje neku radnju i preuzima odgovornost za nju.

3 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 neodredjenosti. 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.

4 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:

- javni podaci - podaci u koje svi imaju uvid,
- autorizovani podaci - podaci u koje isto svi imaju uvid, ali su od korišćenja zaštićeni autorskim pravom
- poverljivi podaci - podaci koji su tajni ali njihovo postojanje nije.
- 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.

5 Zaključak

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 nadje 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] Klasična kriptografija. on-line na: https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html.

[2] Kriptografija u e-poslovanju. on-line na: http://www.link-elearning.com/lekcija-Kriptografija_6958.

[3] Wikipedia. Kriptografija. on-line na: https://sh.wikipedia.org/wiki/Kriptografija.