1. UVOD

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 pogrešnih 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. Pokazuje se da je najdelotvornija zaštita poruka njihovo kriptovanje.

2. POJAM KRIPTOGRAFIJE I OSNOVNI TERMINI

Izraz kriptografija potiče iz grčkog jezika i znači "tajno pisanje". Izvedenica je grčkog prideva κρσπτός (skriven) i glagola γράφω gráfo (pisati). Kriptografija ima dugu i zanimljivu istoriju koja seže hiljadama godina unazad. Istorijski posmatrano, kriptografiji su svoj doprinos dale četiri grupe ljudi: vojnici, diplomate, letopisci i ljubavnici. Najveći doprinos tokom vekova davali su vojnici, jer im je bio najznačajniji. Danas je to moderna nauka bazirana na primenjenoj matematici.

Kriptografija je nauka koja koristi matematiku i matematičke metode za kriptovanje i dekriptovanje podataka. Kriptografija nam omogućava transport "osetljivih informacija" preko nesigurnih komunikacijskih kanala bilo to korišćenjem staromodnih pisama ili u današnje vreme interneta, na način da niko ne može pročitati sadržaj tajne informacije osim osobe kojoj je stvarno namijenjena. Sama enkripcija se sastoji od toga da se čist tekst (ili bilo kakva druga informacija) sakrije tj. prikaže na nerazumljiv način svima osim osobama koje ne poznaju dekripcijski ključ. Pored gore navedenog, valja spomenuti jednu bitnu razliku izmeĐu termina kriptografija i termina kriptologija.

- Kriptografija je nauka koja se bavi svim aspektima sigurnosnog transporta podataka kao što su na primer autentifikacija (web, lokalne mreže i sl.), digitalni potpisi, razmena elektronskog novca.
- Kriptologija, je za razliku grana matematike koja se bavi matematičkim načelima, te matematičkom implementacijom kriptografskih metoda.

Profesionalci prave razliku između šifre i koda.
-Šifra omogućava zamenu znak za znak (bit za bit), bez obzira na jezičku strukturu poruke.
-Kodom se jedna reč zamenjuje drugom rečju ili simbolom. Kodovi se više ne koriste, mada su imali burnu istoriju.
Kriptografija je nauka koja se bavi metodima očuvanja tajnosti informacija. Kada se lične, finansijske, vojne ili informacije državne bezbednosti prenose sa mesta na mesto, one postaju ranjive na prisluškivačke taktike. Ovakvi problemi se mogu izbeći kriptovanjem (šifrovanjem) informacija koje ih čini nedostupnim neželjenoj strani. Šifra i digitalni potpis su kriptografske tehnike koje se koriste da bi se implementirali bezbednosni servisi. Osnovni element koji se koristi naziva se šifarski sistem ili algoritam šifrovanja. Svaki šifarski sistem obuhvata par transformacija podataka, koje se nazivaju šifrovanje i dešifrovanje.

Šifrovanje je procedura koja transformiše originalnu informaciju (otvoreni tekst) u šifrovane podatke (šifrat). Obrnut proces, dešifrovanje, rekonstruiše otvoreni tekst na osnovu šifrata. Prilikom šifrovanja, pored otvorenog teksta, koristi se jedna nezavisna vrednost koja se naziva ključ šifrovanja. Slično, transformacija za dešifrovanje koristi ključ dešifrovanja. Broj

simbola koji predstavljaju ključ (dužina ključa) zavisi od šifarskog sistema i predstavlja jedan od parametara sigurnosti tog sistema.

Kriptoanaliza je nauka koja se bavi razbijanjem šifri, odnosno otkrivanjem sadržaja otvorenog teksta na osnovu šifrata, a bez poznavanja ključa. U širem smislu, kriptoanaliza obuhvata i proučavanje slabosti kriptografskih elemenata, kao što su, na primer, heš funkcije ili protokoli autentifikacije. Različite tehnike kriptoanalize nazivaju se napadi.

Originalna poruka koju će pošiljaoc slati u daljnjem razmatranju će se zvati čisti tekst ili original. Zatim, kodiranje poruke tj. postupak pretvaranja originala (čistog teksta) u nečitljiv oblik ćemo nazvati enkripcija. Tako enkriptujen tekst ima engleski termin ciphertext, a mi ćemo je jednostavno nazvati kodiranom porukom. Nadalje, postupak dekodiranja poruke, tj. vraćanja poruke iz njenog enkriptujenog oblika u originalni (čisti tekst) oblik naziva se dekripcija. Vrlo važan termin u kriptografiji je ključ. Ključ ima veliku ulogu u enkripciji i dekripciji poruke.

3. ISTORIJAT KRIPTOGRAFIJE

Kada je pismo postalo sredstvo komunikacije, pojavila se potreba da se neka pisma sačuvaju od tuđih pogleda. Tada je i kriptografija ugledala svetlost dana. Od samog početka, enkripcija podataka koristila se prvenstveno u vojne svrhe. Kriptografija ima dugu i fascinantnu istoriju. Postoje čak podaci da su Egipćani pre više od 4000 godina koristili kriptografiju za zaštitu informacija. Jedan od prvih velikih vojskovođa koji je koristio šifrovane poruke bio je Julije Cezar. Naime, kada je Cezar slao poruke svojim vojskovođama, on je te poruke šifrovao tako što su sav ili pojedina slova u tekstu bila pomerana za tri, četri ili više mesta u abecedi. Takvu poruku mogli su da dešifruju samo oni koji su poznavali "pomeri za" pravilo. Poznata Cezarova izjava prilikom prelaska Rubikona u šifrirovanom dopisivanju glasila bi: "fqkf ofhzf kyz". Pomeranjem svakog slova za šest mesta u abecedi lako se može pročitati pravi smisao poruke: Alea iacta est (kocka je bačena) .
Prvu poznatu raspravu o kriptografiji, napisao je na 25 stranica italijanski arhitekta Leone Batista Alberti 1467. godine. On je takođe tvorac takozvanog šifarskog kruga i nekih drugih rešenja dvostrukog prikrivanja teksta koja su u XIX veku prihvatili i usavršavali nemački, engleski i francuski šifrantski biroi. Pola veka nakon toga objavljeno je u pet svezaka delo Johanesa Trithemusa prva knjiga iz područja kriptografije. Kasnije značajan doprinos daju milanski doktor Girolamo Kardano, matematičar Batisto Porta i francuski diplomata Blaise de Vigener.

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 je ona u to vreme bila revoluciona 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.

Početkom 60-ih sa razvojem računara došlo je do sve većih zahtjeva za zaštitom informacija, a time i do razvoja kriptografije. U zadnjih 20-ak godina desila se prava eksplozija u razvoju kriptografije. Dok je klasična kriptografija bila u upotrebi kod običnih ljudi već duže vreme, kompijuterska kriptografija je bila u potpunosti u vojnom domenu još od 2. svjetskog rata. Američka NSA (National Security Agency) i njihovi ekvivalenti u bivšem Sovjetskom savezu, Engleskoj, Izraelu, Francuskoj i drugde potrošili su milijarde dolara na razno razne igre osiguranja svojih komunikacija i pritom želeći razbiti tuđe. Privatne osobe sa manje

znanja i novaca su bile bespomoćne u zaštiti svoje privatnosti od takvih vlada.

Danas je situacija bitno drugačija. Postoji puno materijala, što besplatnih koji omogućavaju vrlo visoki nivo kriptovanja svakome ko želi. Doduše u nekim državama i danas postoje zakoni o ograničenju korišćenja kriptografskih alata, ali sve je to uzaludno kada se na internetu mogu naći gotovo sve implementacije kriptografskih metoda.