TEHNIČKA ŠKOLA MLADENOVAC

Vuka Karadžića 75, 11400 Mladenovac, тел.011/8231-985, [tsm@gmail.com](mailto:tsm@gmail.com)

**Osnovne metode kriptološke zaštite**

**Profesor:** **Učenik:**

**Srđan Maričić Stefan Todorović IV6**

**Osnovne metode kriptološke zaštite**

**Uvod**

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.

**Sta obezbeđuje kriptografija?**

Kriptografija mora da obezbedi sledeće:

* Integritet ili verodostojnost informacija koje se šifruju se brine o tome da ne dođe do neovlašćene promene informacija, kao što su menjanje informacije, brisanje informacije i zamena informacije. Da bi se osigurala verodostojnost, mora postojati način provjere da li je informacija promenjena od strane neovlašćene osobe.
* Tajnost informacija osigurava da je sadržaj informacije dostupan samo ovlašćenim osobama odnosno samo onim koji poseduju ključ. Postoje brojni načini zaštite tajnosti, počev od fizičke zaštite do matematičkih algoritama koji skrivaju podatke.
* Provera identiteta korisnici koji počinju komunikaciju se trebaju prvo predstaviti jedan drugome pa tek onda počinju sa razmenom informacija.
* Nemogućnost izbjegavanja odgovornosti je vrlo važna stavka, pogotovo u novije vreme kada se veliki deo novčanih transakcija obavlja putem interneta.

**Osnovni pojmovi i termini**

Termini Plaintext ili Cleartext odnose se na izvornu poruku ili izvorni tekst koji je moguće pročitatii razumeti bez primene bilo kakvih posebnih metoda. Ukoliko se takav tekst treba preneti sa mesta A domesta B, on se naziva poruka. Poruka se može slati putem računarske mreže kao izvorni tekst ili kao nerazumljiv sadržaj koji se naziva šifrovan ili kriptovan tekst .

Postupak pomoću koga se izvorni tekst transformiše u šifrovan tekst se naziva kriptovanje (eng.encryption). Kriptovanje se koristi da bi se obezbedilo da nijedan korisnik, osim korisnika kome jeporuka namenjena, ne može da sazna sadržaj poruke . Ako neovlašćeni korisnici dođu u posed kriptovanog teksta i vide njegov sadržaj ne mogu pročitati izvorni tekst. Kriptovanje izvornog teksta se obavlja pomoću određenog pravila za kriptovanje odnosno kriptografskog algoritma. Svaki kriptografski algoritam kao ulazne podatke ima izvorni tekst i ključ a kao izlaz daje kriptovani tekst.

Postupak koji omogućava da se od kriptovanog teksta dobije originalni izvorni tekst naziva sedekriptovanje (eng. decryption). Dekriptovanje odnosno dešifrovanje predstavlja inverzni postupak odkriptovanja. Kriptovani tekst za koji nije poznat ključ zove se kriptogram.

Nauka koja proučava kriptovanja i dekriptovanja podataka se naziva Kriptografija. Kriptografija seoslanja na matematiku i omogućava čuvanje važnih podataka kao i njihov prenos preko računarske ili telekomunikacione mreže a da pri tome niko ne može da ih pročita osim korisnika kome su namenjeni.Dok se Kriptografija bavi zaštitom podataka, Kriptoanaliza je nauka o otkrivanju odnosno "razbijanju"kriptovanih poruka. Objedinjene Kriptografija i Kriptoanaliza se nazivaju Kriptologija.

Protokol predstavlja skup pravila i konvencija koji definiše komunikacioni okvir između dva ili višeučesnika u komunikaciji. Tu spadaju: uspostavljanje veze, održavanje veze, raskid veze i obnavljanjeveze u slučaju prekida. Kriptografski protokoli se upotrebljavaju za uspostavljanje sigurne komunikacije preko nepouzdanih globalnih mreža i distribuiranih sistema. Oslanjaju se na kriptografske metode zaštite kako bi korisnicima obezbedili osnovne sigurnosne usluge poverljivosti, integriteta i neporicljivosti.

Treba napomenuti razlike između termina kodiranje i šifrovanje. Pojam kodiranje se odnosi na transformaciju izvornog teksta koje se vrši na osnovu obimne „knjige“ kodova, u kojoj se reči i fraze zamenjuju slučajnim nizom znakova. Na primer, "UWRT" može biti kod za "Ja se zovem Petar".Nasuprot tome, šifra radi na nižem nivou: na nivou pojedinačnih slova, malih grupa slova, ili u modernim šemama nad pojedinačnim bitovima. Uz to se umesto “knjige” kodova koriste algoritmi koji su utemeljeni nekom matematičkom formulom.

Postoji dve vrste kriptosistema: simetrični i asimetrični. U simetričnim sistemima, isti ključ (tajni ključ) koristi se i za šifrovanje i za dešifrovanje. Manipulacija podacima u simetričnim sistemima brža je nego u asimetričnim sistemima jer generalno koriste kraću dužinu ključa. Asimetrični sistemi koriste javni ključ za šifrovanje poruke a privatni ključ za njeno dešifrovanje. Korišćenje asimetričnih sistema poboljšava bezbednost komunikacije. Primeri asimetričnih sistema su RSA (Rivest-Shamir-Adleman) i ECC (Elliptic Curve Cryptography). Simetrični modeli koriste AES (Advanced Encryption Standard) koji je zamenio stariji DES (Data Encryption Standard).

U kolokvijalnoj upotrebi, termin „kod“ često se koristi za bilo koju vrstu šifrovanja ili skrivanje značenja. Međutim, u kriptografiji, kod ima specifičnije značenje. On znači zamenu za jedinicu čistog teksta (reč ili frazu) sa šifrovanom rečju.

Kriptoanaliza je termin koji se koristi za proučavanje metoda za pribavljanje značenja šifrovane informacije bez pristupa ključu. To je proučavanje načina za proboj algoritama za šifrovanje ili njihovih implementacija. Proučavanje karakteristika jezika koji imaju neku primenu u kriptografiji ili kriptologiji naziva se kriptolingvistika.

**Kriptografija simetričnih ključeva**

Kriptografija simetričnih ključeva odnosi se na metode šifrovanja u kojima i pošiljaoc i primalac dele isti ključ. Ovo je bio jedini način šifrovanja koji je bio javno poznat sve do juna 1976. godine. Šifre simetričnih ključeva su implementirane ili kao blok šifre (engl. Block ciphers) ili kao šifre toka (engl. stream ciphers). Šifrovanje blok šifrom se izvodilo tako što se čisti tekst unosio u blokovima umesto u individualnim znacima, što je ulazna forma šifre toka.

DES standard i AES standard sudizajni blok šifre koji su dizajnirani po kriptografskim standardima vlade SAD-a. Uprkos negodovanju kao zvaničan standard, DES (pogotovo njegova i dalje odobrena i mnogo sigurnija trostruka DES varijanta) ostaju prilično popularni. Koriste se u velikom opsegu, od šifrovanja na bankomatima pa do privatnosti elektronske pošte i sigurnosti udaljenog pristupa. Mnoge druge blok šifre su dizajnirane i puštane, sa značajnim varijacijama u kvalitetu. Mnoge su temeljno provaljivane, kao što je to FEAL.

Šifre toka, suprotnost od blok šifri, stvaraju proizvoljno dugačak tok ključnog materijala, kombinovano sa čistim tekstom bit po bit ili karakter po karakter, nešto kao one-time pad. U šiframa toka, izlazni tok se pravi zasnovan na skrivenom unutrašnjem stanju koje se menja dok šifra radi. To unutrašnje stanje na početku se postavlja korišćenjem tajnog ključa. RC4 je široko korišćena šifra toka.

Kriptografske heš funkcije su treća vrsta kriptografskog algoritma. One koriste poruku bilo koje dužine kao ulaz, a kao izlaz daju kratki heš fiksirane dužine, koji se može koristiti za, na primer, digitalni potpis. Za dobre heš funkcije, napadač ne može pronaći dve poruke koje proizvode isti heš. MD4 je dugo korišćena heš funkcija koja je sada probijena. MD5, pojačana varijanta MD4, je takođe rasprostranjena ali je u praksi probijena. Nacionalna bezbedonosna agencija SAD-a razvila je seriju bezbednih heš algoritama sličnih MD5 heš funkciji. SHA-0 bio je nesavršen algoritam koji je agencija povukla. SHA-1 je široko raspoređen i sigurniji je od MD5, ali kriptoanalitičari su identifikovali napade protiv njega.

Kodovi za autentifikaciju poruke su slični kriptografskim heš funkcijama s tim da se tajni ključ može koristiti za autentifikaciju heš vrednosti pri potvrdi.

**Kriptografija javnih ključeva**

Kriptosistemi simetričnih ključeva koriste isti ključ za šifrovanje i dešifrovanje poruke, iako poruka ili grupa poruke mogu da imaju drugačiji ključ nego drugi. Značajni nedostatak simetričnih šifri je menadžment ključa koji je neophodan za njegovo bezbedno korišćenje. Svaki zasebni par komunikativnih „stranke“, idealno, moraju da dele različiti ključ, i možda razmene svaki šifrirani tekst takođe. Broj ključeva koji su neophodni raste kao kvadrat broja članova mreže, što veoma brzo zahteva kompleksne šeme za upravljanje ključem da bi sve ostalo tajno.

Revolucionarne 1976. godine, Vitfild Difi i Martin Helmen predložili su pojam kriptografije javnog ključa (obično nazivan asimetričnim ključem) gde su dva različita ali matematički povezana ključa korišćena, privatni i javni ključ. Sistem javnog ključa je tako napravljen da je računanje jednog ključa (privatnog ključa) računski neupotrebljivo od drugog (javnog ključa), iako su povezani. Umesto toga, oba ključa se tajno generišu, kao međusobno povezani par. Istoričar Dejvid Kan je opisao kriptografiju javnih ključeva kao „najrevolucionarniji novi koncept u polju još od polialfabetske zamene iz renesanse“.

U kriptosistemima javnih ključeva, javni ključ se može slobodno distribuirati, dok se njegov upareni privatni ključ čuva tajnim. Javni ključ se koristi za šifrovanje dok se privatni ili tajni ključ koristi za dešifrovanje. Iako Difi i Helmen nisu mogli da pronađu takav sistem, prikazali su da je kriptografija javnih ključeva itekako moguća ppreko Difi-Helmen protokola za razmenu ključeva, rešenja koje se sada široko koristi u bezbednim komunikacijama za dozvolu dvema strankama za tajno slaganje na deljenom šifarskom ključu.

**Kriptosistemi**

Kriptosistemi su dizajnirani radi pružanja posebne funkcionalnosti (npr. šifrovanje javnih ključeva) a u isto vreme garantovati određena bezbedonosna svojstva (npr. CPA (chosen-plaintext attack) bezbednost u nasumičnom oracle modelu). Kriptosistemi koriste svojstva osnovnih kriptografskih primitiva radi podrđke sistemskih bezbedonosnih svojstava. Naravno,razlika između primitiva i kriptosistema je proizvoljna, sofisticiran kriptosistem može izaći iz kombinacije nekoliko primitivnijih kriptosistema. U mnogim slučajevima, struktura kriptosistema uključuje napred-nazad komunikaciju između dve ili više stranki. Takvi kriptosistemi nekada se nazivaju i kriptografski protokoli.

Neki dobro poznati kriptosistemi su RSA šifrovanje, šnor potpis (Schnorr signature), El-Gamal šifrovanje, PGP itd. Složeniji kriptosistemi uključuju i elektronske keš sisteme itd. Neki „teoretski“ kriptosistemi uključuju i interaktivne dokazne sisteme, sisteme za tajno deljenje itd.

Sve do skoro, većina bezbedonosnih svojstava većine kriptosistema demonstrirana je korišćenjem empirijskih tehnika. U skorije vreme, uloženo je dosta truda u razvijanje formalnih tehnika za uspostavljanje bezbednosti kriptosistema. To se obično naziva dokazana sigurnost. Ideja dokazane sigurnosti jeste da pruži argumente o računskoj težini potrebnoj za nagodbu nekih delova kriptosistema.

Proučavanje kako najbolje implementirati i integrisati kriptografiju u softverskim aplikacijama je zasebno polje koje se naziva kriptografsko inženjerstvo.

**Istorijat kriptografije**

Kada je pismo postalo sredstvo komunikacije, pojavila se potreba da se neka pisma sačuvaju od tuđih pogleda. Tada se pojavila kriptografija. Od početka, enkripcija podataka koristila se prvenstveno u vojne svrhe. 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 šifriranom dopisivanju glasila bi: fqkf ofhzf kyz. Pomicanjem 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 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. U 16. 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.