Vedrana Macanović
Fakultet za poslovno industrijski menadžment
Beograd
Nikola Abramović
Fakultet za ekonomiju Bar

UDK 004.056.55
Pregledni rad
Primljen: 14.VI 2016.

KRIPTOGRAFSKI ALGORITMI

Apstrakt

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 neovlaštene upotrebe informacija, podmetanja krivih 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 komunikacionim kanalom postaju najvažniji oblik ostvarenja sigurnosti. Pokazuje se da je najdelotvornija zaštita poruka njihovo kriptiranje.U ovom radu su objašnjeni osnovni pojmovi vezani za kriptovanje i algoritme koji su se koristili i koji se koriste kako bi se zaštitila privatnost unutar mreže računara.

Ključne reči: ključ, kriptovanje, algoritmi, sigurnost, enkripcija, kriptologija i kriptografija.

Uvod

Kriptografija je nauka "tajnog pisanja", tj. nauka čuvanja informacija u onoj formi koja će biti čitljiva samo onima kojima je informacija namenjena dok će za ostale biti neupotrebljiva. Usporedo sa razvojem kriptografije razvila se i nauka kojoj je cilj analizom kriptirane poruke odgonetnuti njen sadržaj. Ta nauka se naziva krip toanaliza.

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, razmjena elektroničkog novca.Kriptologija, je za razliku grana matematike koja se bavi matematičkim načelima, te matematičkom implementacijom kriptografskih metoda.
Originalna poruka koju je pošiljaoc će 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 enkriptiran tekst ima engleski termin ciphertext, a mi ćemo je jednostavno nazvati kodiranom porukom. Nadalje, postupak dekodiranja poruke, tj. vraćanja poruke iz njenog enkriptiranog 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.

1. Osnovni kriptografski algoritmi

Nekada, prije nego što su računari ušli u široku upotrebu, tj. prije nego su se dovoljno razvili, većina kriptografskih metoda šifriranja se bazirala na tajnosti šifre. No, tako bazirani algortimi su se pokazali dosta nepouzdani, te su se morale pronaći neke druge metode šifriranja. Današnje metode šifriranja zasnivaju se na upotrebi ključa. Ključ je najvažniji dio u pravilnom enkriptiranju i dekriptiranju poruka.

Upravo ovisno o načinu korištenja ključa, razvile su se dvje klase algoritama. Jedna je simetrična, a druga asimetrična klasa. Drugim rečima, postoje simetrični algoritmi kriptiranja i asimetrični algoritmi kriptiranja. Osnovna razlika je u tome da simetrični algoritmi koriste isti ključ za enkripciju i dekripciju neke poruke (ili se ključ za dekripciju može lako proizvesti iz originalnog ključa za enkripciju), dok asimetrični algoritmi koriste različite ključeve za enkripciju i dekripciju iste.

• Simetrični algoritmi:

Ove algoritme delimo u dvije grupe: stream šifriranje i blok šifriranje. Stream šifriranje radi tako da se enkripcija poruke (originala) vrši bit po bit, dok se kod blok4 šifriranja enkripcija vrši po blokovima podataka, tj. uzimaju se blokovi od više bitova (64, 128, 196, 256 ...), te se enkriptiraju kao celina. Dekripcija se najčešće vrši inverznim enkriptiranjem, tj. algoritam je isti, ali se podključevi enkripcije koriste obrnutim redosledom.

• Asimetrični algoritmi:

Ove algoritme nazivamo još i public-key algorithms, tj. algoritmi s javnim ključem. Razlog ovakvom nazivu je taj što je dozvoljeno da se jedan od ključeva potreban za enkripciju/dekripciju objavi javno (npr. Internet, novine). Ovdje treba obratiti pažnju na reči "jedan od ključeva". Ono što je specifično za ovaj tip algoritma je to da se koriste dva ključa za enkripciju/dekripciju poruke (originala).

Ideja je sljedeća: osoba A objavi svoj javni ključ preko nekog medija (npr. Internet). Osoba B, koja osobi A želi poslati tajnu poruku enkriptira tu svoju poruku s ključem koju je osoba A javno objavila te joj takvu poruku pošalje (recimo preko e-mail servisa). Jedino osoba A sa svojim privatnim (tajnim) ključem može dekriptirati poruku poslanu od osobe B i niko drugi.

Uglavnom, simetrični algoritmi su po svojoj prirodi brži, tj. implementacija na računaru se brže odvija od implementacije asimetričnih algoritama. No, zbog nekih prednosti asimetričnih algoritama u praksi se obe vrste algoritama isprepleću u cilju bolje zaštite poruka. Obično se asimetrični algoritmi koriste za enkripciju slučajno generisanog broja koji služi kao ključ za enkripciju originalne poruke metodama simetričnih algoritama. Ovo se naziva hibridna enkripcija.

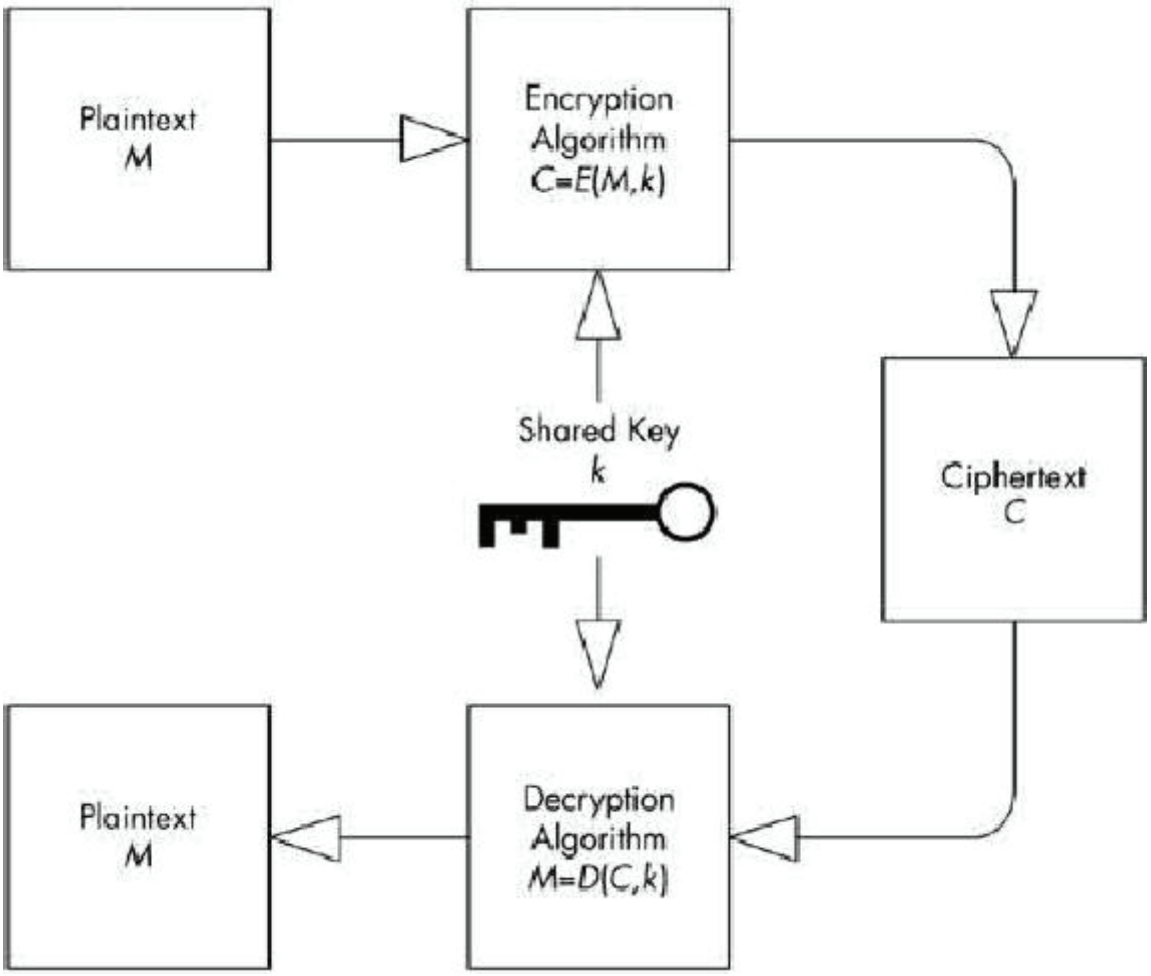
2. Simetrična kriptografija

Simetrična kriptografija je najstariji oblika kriptografije, stara gotovo koliko i ljudska komunikacija (naziva i kriptografijom tajnog ključa jer se podatak kriptira idekriptira istim ključem). Za proces kriptiranja u simetričnoj kriptografiji potrebno je znati algoritam kriptiranja i tajni ključ. Nekad su se algoritmi držali u tajnosti, ali se pokazalo da skrivanje algoritmane ne doprinosi sigurnosti.
Svi savremeni simetrični algoritmi javno su objavljeni. Zbog toga ih je u potpunosti moguće testirati i provjeriti njihovu otpornost na napade, odnosno moguće ih je analizirati (kriptoanaliza). Sigurnost simetričnih algoritama ovisi o sigurnosti samog algoritma i dužini ključa. Najpoznatiji simetrični algoritam je DES (Data Encryption Standard), koji je razvio IBM-a 1977. godine. Bio je standardni simetrični algoritam sve do 2000. godine kad ga je zamijenio AES (Advanced Encryption Standard), koji rukuje ključevima dužine 128, 192 i 256 bita. Glavni razlog zbog kojeg je DES zamijenjen AES-om je taj što DES ima dužinu ključa od 56 bita. Već smo rekli da je simetrična kriptografija tajnim ključem postupak kojim

se koristi jednak ključ za enkripciju i dekripciju podataka. Simetričnu kriptografiju možemo matematički prikazati izrazima

Dekripcija: $M = D_k (C)$

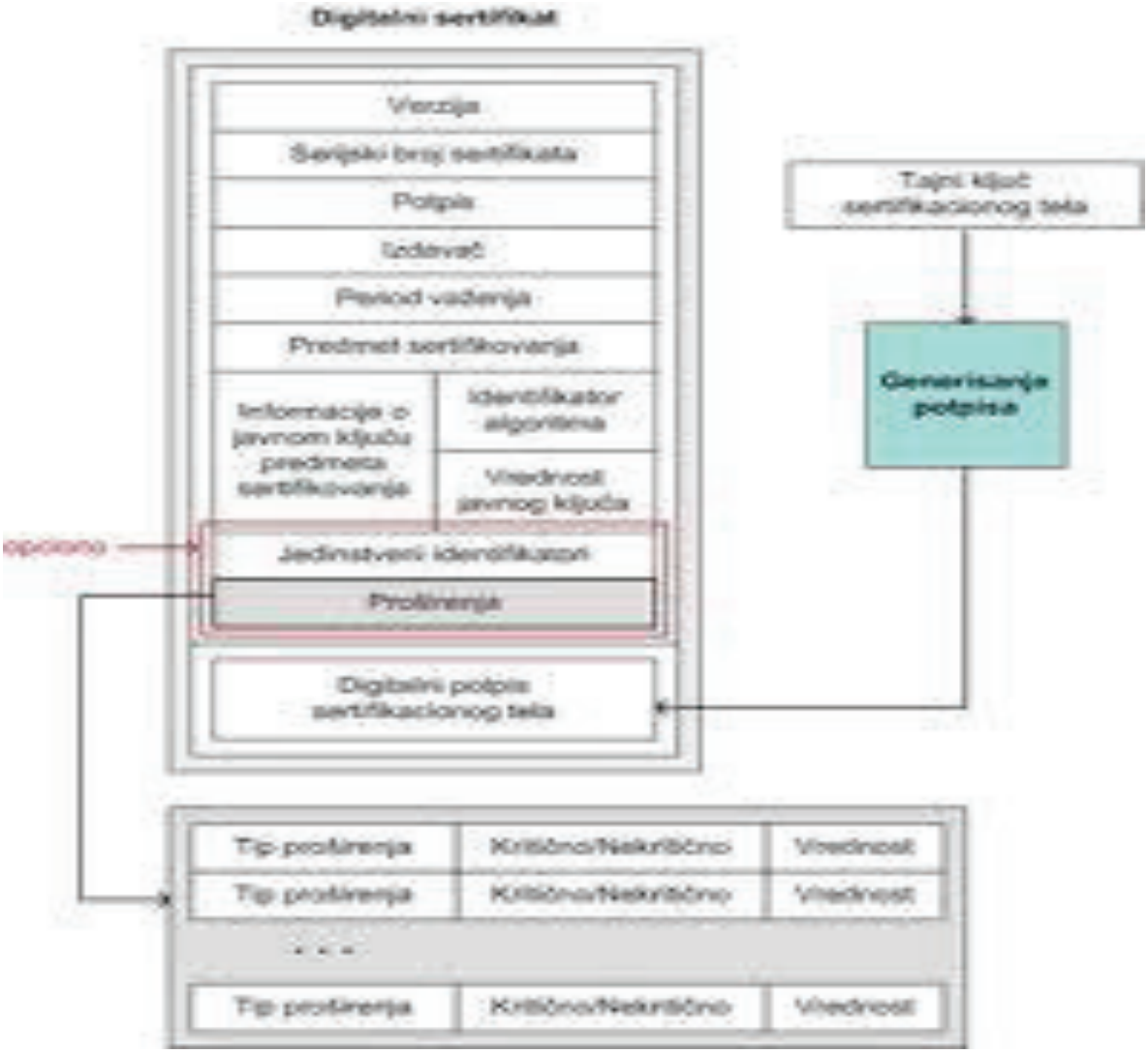
gdje E predstavlja enkripcijsku funkciju, D dekripcijsku funkciju, k je tajni ključ jedinstven za obe strane, M je originalna (plaintext) poruka, a C je pripadajuća enkriptirana poruka (ciphertext).



Slika1. Simetrična kriptografija

Način korištenja simetrične enkripcije najlakše je pokazati sledećim primerom. Pošiljaoc i primalac poseduju zajednički tajni ključ, koji samo oni znaju te su prethodno dogovorili zajednički kriptografski algoritam koji će koristiti. Kada Pošiljaoc želi poslati poruku primatelj - u, on enkriptira originalnu poruku (plaintext) korištenjem tajnog ključa i prethodno dogovorenog algoritma. Time dobija enkriptiranu poruku (ciphertext) koju dalje šalje primatelj – u .

njihove javne ključeve uključili u svoje browsere. Najčešće korišceni standard za digitalne certifikate je X.509.



Slika 4. Digitalni sertifikat

6. Asimetrični algoritmi

6.1. RSA algoritam

Pod pojomomalgoritma podrazumevamo precizno opisan postupak za resavanje nekog problema. Obicno je to spisak uputstava ili skup pravila kojima je, korak po korak, opisan postupak za resavanje zadatog problema. Svaki korak algoritma odnosno svako upustvo iz spiska mora da bude definisana operacija. Algoritmi moraju da budu nedvosmisleni i da se zavrsavaju u konacnom broju koraka.

RSA algoritam jedan od najkorišćenijih asimetričnih algoritama danas.
RSA je skračenica koja je nastala od prezimena njegovih tvoraca: RonaRivesta, Adi Shamira i Leonarda Adlemana. Svetlost dana ugledao je davne 1977. godine.

U RSA algoritmu ključnu ulogu imaju veliki prosti brojevi. To su, kao sto znamo, brojevi koji su deljivi samo samim sobom i jedinicom. Prosti brojevi (P i Q) u ovom algoritmu služe za generisanje javnog i tajnog ključa i to preko sledećih jednostavnih formula:

Kjavni = P * Q

Ktajni = (2 * (P - 1) * (Q - 1) + 1) / 3
Algoritam kodiranja i dekodiranja sastoji se iz dve formule.
Kodiranje:

Mkodirano = (Mizvorno ^ 3) mod Kjavni

Dekodiranje:
Mizvorno = (Mkodirano ^ Ktajni) mod Kjavni
Na primer, hocemo da kodiramo rec "MAJA".
Ona u ASCII formi glasi: 77 65 74 65 (M = 77; A = 65; J = 74; A = 65).
Kao dva prosta broja možemo uzeti, recimo P = 9839 i Q = 22391. U tom slucaju ključevi koji
ce se koristiti bice:
Kjavni = 220305049 i
Ktajni = 146848547.
Sada primenimo formule za kodiranje (koristeći samo javni ključ):

(77657465 ^ 3) mod 220305049 = 162621874

Primalac će primeniti formulu za dekodiranje (koristeći i javni i tajni ključ):
(162621874 ^ 146848547) mod 220305049 = 77657465
Ono što je pohvalno za ovaj algoritam je njegova jednostavnost, ali i sigurnost.

MIPS iz javnog ključa izračuna tajni ključ (na primer, Pentium I kompjuter ima oko 150 MIPS-a). Za enkripciju fajlova koriste se ključevi velicine 1024, 2048 ili 4096 bita.

Duzina ključa u bitovima i potrebno vreme:

50 - 3.9 h

100 - 74 god

150 - 10^6 god

200 - 3,8 * 10^9 god

6.2 PGP (Pretty Good Privacy)

PGP je hibridni sistem za enkripciju, jer kombinuje i simetricnu i asimetricnu enkripciju. Podaci se pre šifrovanja pakuju, ako je moguće. Ovo je korisno iz dva razloga. Prvi je manja količina podataka za prenos. Drugi je dodatna sigurnost, jer se pakovanjem eliminise pojavljivanje slicnih delova u izvornoj datoteci. Mnoge tehnike kriptoanalize iskoriscavaju bas te slicne delove da bi probile zastitu. Naravno, fajlovi koji su ili prekratki za pakovanje ili se ne mogu spakovati dovoljno, ostavljaju se u izvornom obliku. Posle pakovanja, PGP pravi privremeni ključ, odnosno slucajan broj koji se generise korisnikovim pokretima misa i pritiskanjem tastera, jer su i oni takodje slucajni. Ovaj ključ ima jednokratnu upotrebu, jer se koristi da bi se podaci sifrovali simetricnom enkripcijom. PGP zatim sifrujesamo privremeni ključ asimetričnom enkripcijom i pridruzuje šifrovanim podacima. Dešifrovanje se vrši suprotnim procesom. Prvo PGP pomoću tajnog ključa dešifruje privremeni ključ, a njim se onda dalje dešifruju podaci.

6.2.1 Zašto PGP koristi hibridnu enkripciju?

Razlog je jednostavan: simetricna enkripcija je oko hiljadu puta brza od asimetricne, ali kod simetricne enkripcije postoji problem prenosa ključa (ako se presretne ključ, podaci se mogu desifrovati). Kada se ukombinuju ova dva nacina enkripcije, dobija se zeljeni efekat: brza enkripcija sa sigurnim prenosom ključa. Ključ se, dakle, prenosi, ali šifrovan tako da ga samo osoba koja ima tajni ključ moze dešifrovati.

Posto PGP koristi asimetricnu enkripciju, to znaci da ima mogućnost digitalnog potpisivanja dokumenata, uz jednu razliku. Umesto da se ceo dokument šifruje tajnim ključem i od njega generise potpis, to se radi samo na kontrolnom kodu dokumenta (veoma slicno CRC-u). Bilo kakva promena na dokumentu rezultuje promenom u kontrolnom kodu, samim tim potpis vise nije vazeci, a vi znate da je u pitanju falsifikat.

Time se izbegava dupliranje dužine dokumenta, jer se potpis ne generiše od celog dokumenta.

7. Kriptoanaliza

Kriptoanaliza upravo je suprotno od kriptografije. To je nauka koja se bavi razbijanjem sifri, dekodiranjem, zaobilazenjem sistema autentifikacije, uopste provaljivanjem kriptografskih protokola.Znači kriptoanaliza je naučna disciplina koja proučava postupke otkrivanja otvorenog teksta bez poznavanja ključa, te postupke otkrivanja ključa uz poznavanje otvorenih i/ili kriptiranih tekstova, ili uz poznavanje nekih informacijao otvorenim i/ili kriptiranim tekstovima.. Razlicite tehnike kriptoanalize nazivaju se napadi.

Napadi na sigurnost se mogu razdvojiti u pasivne i aktivne napade. Pasivnim napadom se samo prisluškuje poslana poruka. Pasivni napad je puno težedetektirati nego aktivni napad. Aktivni napad uključuje mijenjanje poruke,maskiranje, ponovno slanje i DoS ('Denial of Service') napade.
Vrste napada:

- Napad poznatim šifriraniim tekstom: ovaj napad je najteži.
  Kriptoanalitičar poznaje samo algoritam kriptiranja i kriptirane tekstove.

- Napad poznatim otvorenim tekstom: za dani kriptirani tekst kriptoanalitičar poznaje odgovarajući otvoreni tekst ili njegov dio. Kriptoanalitičar zna algoritam i 1 do N otvorenih i kriptiranih tekstova, ali ne zna ključ.

- Napad odabranim otvorenim tekstom: kriptoanalitičar odabere otvorenitekst i kriptira ga. Ovaj napad omogućuje pronalaženje slabosti u algoritmu. Kriptoanalitičar zna algoritam, kriptirani tekst i 1 do N odabranih parova otvorenih i kriptiranih tekstova, ali ne zna ključ.
- Napad odabranim kriptiranim tekstom: kriptoanalitičar može odabratikriptirani, tekst i na neki način ga dekriptirati i dobiti otvoreni tekst. Također može odabrati neki otvoreni tekst po svojoj želji. Kriptoanalitičar zna algoritam, kriptirani tekst i 1 do N navodnih kriptiranih tekstova sa otvorenim tekstovima, ali ne zna ključ.

- Adaptivan napad odabranim otvorenim tekstom: kriptoanalitičar koristi napad odabranim otvorenim tekstom. Rezultati napada se koriste za biranje nekog drugog otvorenog teksta. Ovim načinom moguće je unaprijediti napad. Ovaj napad poznat je pod nazivom "diferencijalna kriptoanaliza". Kriptoanalitičaru je poznat algoritam, kriptirani tekst,dabrani otvoreni tekst sa kriptirani tekstom, te odabrani kriptirani tekst sa otvorenim tekstom.

- Birthday attack: ovaj napad je dobio ime po paradoksu rođendana

- Meet in the Middle: napad je sličan birthday napadu, osim štokriptoanalitičar može proveriti secište između tih skupova, a ne mora čekati pojavljivanje vrednosti dvaput u jednom skupu.

- Napad korištenjem srodnih ključeva: u ovom napadu pretpostavlja seznanje o odnosu između ključeva u dva različita kriptiranja. Napad može otkriti slabosti u postupku generiranja podključeva.

- Delomično znanje o ključu: napadač poseduje delomično znanje o tajnom kljluču (npr. zbog “rupe” u postupku generiranja podključeva). U dobrim kriptosustavima, djelomično znanje o ključu ne bi trebalo olakšati pronalaženje ostatka ključa. Ako nije tako, lakše je izvesti iscrpno pretraživanje

Prema količini i kvaliteti otkrivenih tajnih informacija može se klasificirati uspjeh kriptoanalize :
1.Potpuno probijanje ("Total break") - napadač otkriva ključ.
2. Globalna dedukcija ("Global deduction") - napadač otkriva funkcijski ekvivalent algoritma za kriptiranje i dekriptiranje, ali ne nalazi ključ.
3. Lokalna dedukcija ("Instance (local) deduction") - napadač otkriva dodatne otvorene tekstove (ili kriptirane tekstove), nepoznate od prije.

4. Informacijska dedukcija ("Information deduction") - napadač dobiva Shannon-ove informacije o otvorenim tekstovima (ili kriptiranetekstovima), nepoznatih od prije.

5. Algoritam koji omogućuje razlikovanje ("Distinguishing algorithm") -napadač može razlikovati kriptirane tekst od slučajne permutacije.

7.1 Osnovna pravila zaštite

Skoro svi programi za enkripciju umesto brojeva kao ključa, koriste niz slova i brojeva, tj. lozinku. Svi ovi algoritmi su u velikom stepenu sigurni, bilo da se radi o simetricnim ili asimetricnim, ali postoji sansa da se lozinka otkrije ako se ne pridrzavamo nekih pravila pri njenoj izradi.

Idealna kombinacija zastite je kombinacija hardver-softver i pridrzavanje dole nevedenog pravila o vise niza slucajnih slova i brojeva prilikom smisljanja lozinke.
Evo nekoliko pravila kojih bi trebalo da se pridrzavamo prilikom smisljanja lozinke:

- Idealno je da se za lozinku uzme niz slucajnih slova i brojeva. Pri tom bitrebalo da se koristi vise od jednog niza slucajnih slova i brojeva. Ovakve lozinke mnogi izbegavaju jer ih smatraju teskim za pamcenje i upotrebljavaju reci iz svakodnevnog govora. tom slucaju potrebno je pridrzavati se sledecih pravila:

- Ne koristiti reči koje se lako mogu pogoditi: na primer, godinu rođenja,devojačko prezime supruge (ili svoje, ako je u pitanju korisnik ženskog pola) , ime deteta, supružnika, roditelja, bliskog rodjaka, psa/macke/kanarinca ili nekog drugog kucnog ljubimca itd.

- Trebalo bi koristiti više od jedne reči. Izbegavajte upotrebu reci iz rečnika u neizmenjenom obliku. Korisno je upotrebiti barem kombinaciju jedne reči sa nekim brojem.

- Budite inventivni. Najbolja lozinka može biti deo citata iz neke knjige ili neka besmislena rečenica.

8. Zaključak

Kada su se pojavile računarske mreže, nije se mnogo vodilo računa o njihovoj sigurnosti, jer su se tada uglavnom koristile za razmjenu elektronske pošte između istraživača sa raznih univerziteta ili za štampanje dokumenata u kompanijama koje su posedovale više računara koji su preko mreže bili povezani na jedan zajednički štampač.

Danas, kada su računarske mreže dostupne svakome, njihovoj sigurnosti se posvećuje velika pažnja. Da nije toga, u današnje vrijeme se ne bi moglo kupovati preko mreže niti obavljati razne bankarske transakcije. Ne mali je broj ljudi koji na razne načine pokušavaju da naruše sigurnost mreža, želeći time da naude drugim ljudima i da prvenstveno steknu neku korist od toga. Oni pokušavaju da čitaju ili da menjaju sadržaj poruka dostupnih preko mreže, iako nisu ovlašćeni za to. Tako, na primer:

- učenik ili student će, čitajući tuđe e-mail poruke, sebi prekratiti vreme,
- haker će testirati nečiji sigurnosni sistem pokušavajući da mu ukrade podatke,
- poslovni ljudi će pokušati da otkriju planove konkurentne kompanije,
- otpušteni radnik će probati da se poslodavcu osveti zbog otpuštanja,
- računovođa će pronevjeriti novac od kompanije,
- lopov će pokušati da ukrade broj tuđe kreditne kartice da bi pomoću nje kupovao,
- špijun će pokušati da sazna sa kakvom vojnom silom raspolaže neprijatelj

Svi ovi primeri ukazuju na to da je neophodno stvoriti inteligentne mehanizme koji će računarsku mrežu učiniti sigurnom. Zadovoljavajući rezultati su postignuti upotrebom raznih algoritama šifrovanja, kojima se podaci maskiraju i tako budu osigurani za prenos. Korišćenjem protokola za autentifikaciju, osigurava se sigurna komunikacija između dve strane. Osim toga, pojavom digitalnih potpisa i SSL protokola omogućeno je da se razne bankarske transakcije i razmjena dokumenata od velike važnosti obavljaju na siguran način.

Literatura:

1. A. S. Tanenbaum: Computer networks, 3rd edition, Prentice-Hall International, 1996.
2. Vikipidija, http //sr.wikipedia.org/wiki/Kriptogtafija
3. Dragan Pleskonjić,Nemanja Maček,Borislav Đorđević,Marko Cajić:Sigurnost računarskih sistema i mreža
http://www.elitesecurity.org/f24-Kriptografija-enkripcija
http://imprimatur.weebly.com/kriptografija.html

Vedrana macanović
Nikola Abramović

CRYPTOGRAPHIC ALGORITHMS

Abstract
Security computer systems is becoming increasingly important, as more and more users in more ways used more and more information in the computer world. In such a system there is a growing risk of unauthorized use of information, planting false information or destroying information. In computer systems information is transmitted various open and insecure communication paths. Access to these roads can not be physically protected so every hostile attacker can disrupt the security system. Therefore, protective communication mechanisms over insecure communication channel becoming the most important form of achieving security. Indeed the most effective protection of their message encryption. In this article I'm going to explain the basic concepts related to encryption algorithms that have been used and that are used to protect the privacy of the network computers.

Keywords*: key encryption algorithms, security, encryption, cryptography and cryptography.*