UDK: 004.056.55

ZAŠTITA PODATAKA U RAČUNARSKIM SISTEMIMA KORIŠĆENJEM KRIPTOGRAFSKIH METODA

Doc. dr Mirsad Nuković
Richard Soti

Apstrakt: Podaci koji su uskladišteni u bazama podataka i koji se šalju putem računarske mreže, predstavljaju vredan resurs i zavređuju posebnu pažnju i zaštitu, kako bismo očuvali tajnost posla i projekata kojima se bavimo. Podaci i pravovremene i tačne informacije olakšavaju rad pravnika, menadžera i drugih lica koje donose odluke, pa njihovo menjanje, krađa i druge zlonamerne radnje puno utiču na ishod, verodostojnost i tačnost tih odluka, kao i njihovo vreme donošenja, tako da je vrlo značajno obezbediti adekvatan i visok stepen zašite podataka.

Sigurnom komunikacijom bavili su se još Egipćani i Indijci pre više od 3000 god. i od tada pa do danas, ta problematika i ideja se nisu menjale - preneti informaciju sa jednog mesta na drugo što je sigurnije moguće, tj.napraviti algoritam, koji bi omogućio skrivanje originalne poruke tako da bude potpuno nerazumljiva osobama, koje bi neovlašćeno došle do nje. Razvojem savremene tehnologije te metode su se usavršavale, a uporedo sa njima usavršavale su se i metode dekripcije podataka.

U ovom radu autori će pokušati odgovoriti na neka savremena pitanja i algoritme enkripcije i dekripcije podataka i predložiti rešenja za što sigurniju zaštitu.

Ključne reči: zaštita podataka, računarski sistem, kriptografija.

1. Uvod

Razvojem nauke i tehnologije, a posebno ekspanzijom Interneta I njegovih servisa, potreba za sigurnosti prenosa podataka je sve značajniji problem. Odgovore na pitanja: kako znati da poruka prenosnim putem, bez obzira da li je pur bežični ili žičani, nije imenjena, I da li je sagovornik baš onaj za koga se predstavlja, i mnoga druga pitanja koja se tiču sigurnosti prenosa, sigurno moramo tražiti u sofisticiranim metodama zaštite.

Kada komuniciramo, često želimo da ta komunikacija ne bude prisluškivana, ali bez obzira na medij komunikacije, uvek postoji mogućnost presretanja, ili čak izmene naše poruke. Prisluškivanje je vrlo teško sprečiti, pa ko god želi poslati poverljivu, ili samo privatnu poruku mora napraviti bar minimum napora na zaštiti. Jedan od načina zaštite poruke je upotreba znanja kriptografije i šifrirati poruku tako da je može razumeti samo onaj kome je ona namenjena. Do 1970. kriptografija je bila “tamna vještina” koju su razumjeli i koristili samo vladini službenici i vojska. Sada

je to dobro poznata grana matematike koja se predaje na mnogim fakultetima i školama.
Dakle, kriptografija je naučna disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Kriptoanaliza je naučna disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa. Kriptologija je grana nauke koja obuhvata kriptografiju i kriptoanalizu.
Poruku koju pošiljalac želi poslati primaocu obično zovemo otvoreni tekst (eng. plaintext). Pošaljilac transformiše otvoreni tekst koristeći unapred dogovoreni ključ. Taj postupak se zove šifriranje, a dobiveni rezultat šifrat (eng. ciphertext). Nakon toga pošaljilac pošalje šifrat preko nekog komunikacijskog kanala. Presretač prisluškujući dozna sadržaj šifrata, ali ne može odrediti otvoreni tekst. Za razliku od njega, primalac koji zna ključ kojim je šifrirana poruka može dešifrirati šifrat i odrediti otvoreni tekst. Kriptografski algoritam ili šifra je matematička funkcija koja se koristi za šifriranje i dešifriranje. Kriptosistem je sistem koji se sastoji od kriptografskog algoritma, te svih mogućih otvorenih tekstova, šifrata i ključeva.
Primer, Cezarova šifra, je veoma jednostavan.
Znameniti rimski vojskovođa i državnik Julije Cezar u komunikaciji sa svojim prijateljima koristio se šifrom u kojoj su se slova otvorenog teksta zamenjivala slovima što su se nalazila tri mesta dalje od njih u abecedi (A→D, B→E, itd.).
Cezarovu šifru možemo pregledno zapisati na sledeći način:
Uporedo sa razvojem i implementacijom računarskih mreža Interenet tipa, razvijaju se i različiti mehanizmi zaštite specijalizovani za odbranu od pojedinih vrsta napada. U startu treba biti svestan da računarske mreže Internet tipa, pored toga što omogućavaju izuzetno povećanje efikasnosti rada i smanjenje troškova, predstavljaju kritičnu tačku bezbednosti date organizacije sa stanovišta bezbednosti informacija koje se u sistemu prenose.
Prve korišcene metode nisu bili složeni algoritmi, nego se počelo korišćenjem alterativnih jezika, koji su bili poznati samo malom broju ljudi.Razvoj složenije metode je počeo tek razvojem pisma, što je omogućilo da se bilo koja informacija prikaze određenim brojem znakova, koji bi nakon upotrebe određenog ključa, formirali ponovo početnu poruku. Vremenom se javila i ideja prikaza slova drugim simbolima. Primeri, koji su i danas u upotrebi su: *Morseov kod, Braille-ovo pismo i ASCII kod.*
Nikad nije tačno utvrđen početak kriptografije, ali se smatra da je počela pre više od 2000.god.p.n.e, jer iz tog vremena potiču prvi pronađeni tragovi šifriranja.Tačnije oko 1900 god.p.n.e je u Egiptu nastao natpis, koji se danas smatra prvim primerom pisane kriptografije. U 6. veku p.n.e u zapisu dela Biblije, Knjige o Jeremiji, korišćena je šifra koja izvrće abecedu naopako. Šifra je poznata pod imenom ATBASH, a bila je jedna od hebrejskih šifri, koje su u to vreme korišćene.

Dana je tablica "atbash" šifre za engleski jezik:

ABCDEFGHIJKLM
ZYXWVUTSRQPON

tj. slovo 'A' se mijenja sa 'Z' i obratno.

U srednjem veku kriptografija je često korišćena u službi Crkve, a jedan od primera toga je nomenclator-kombinacija malog koda i supstitucijske abecede, koga je na zahtev pape Clementa VII, stvorio Gabrieli di Lavinde. Ova šifra ostala je u upotrebi sledećih 450. godina, iako su u međuvremenu stvorene i sigurnije .1518.god. Johannes Trithemius je napisao prvu knjigu o kriptografiji. Oko 1790. Thomas Jefferson je uz pomoć matematičara Dr.Roberta Pattersona izumeo šifrarnik sa tačkom. On je kasnije ponovo izumljen u nekoliko različitih oblika i korišćen u II svetskom ratu od strane Američke mornarice.1861.god.u SAD-u je prijavljen prvi izum vezan za kriptografiju. Do 1980 .prijavljeno je 1769 takvih izuma. U 20. veku, kriptografija je odigrala značajnu ulogu u dva svetska rata i mnogo raznih sukoba.

William Frederick Friedman (kasnije poznat kao otac američke kriptoanalize) prvi je uveo pojam *"kriptoanaliza*". Kriptografiju su rado koristili i kriminalci, a jedan vrlo slikovit primer je iz razdoblja *prohibicije*. Da bi mogli švercovati alkohol, koristili su vrlo komplikovane sisteme šifriranja, koji su u to vreme bili vrlo napredni. 1923. Arthur Scherbius proizvodi svoj najslavniji proizvod - široko poznatu **Enigmu**. Ona je prvobitno trebala biti komercijalni proizvod, ali nije uspela, pa su je preuzeli nemački nacisti. Oni su je poboljšali pa je postala glavni uređaj za šifriranje u nacističkoj Nemačkoj. Prvi je njenu šifru slomio jedan poljski matematičar na osnovi ukradenog primerka šifriranog teksta i dnevnih ključeva za tri meseca unapred. Kasnije su uspešno razbijene i druge Enigmine šifre prvenstveno pod vodstvom Alana Turinga. 30-ih godina 20. veka nastaje Američki „suparnik" Enigme **SIGABA**. Važno je spomenuti da je bila tehnički naprednija od Enigme.

Nakon II Svetskog rata, razvoj računara daje novi zamah kriptografiji. Tako 1970. IBM razvija šifru pod nazivom Lucifer, koja kasnije, 1976. inspirše stvaranje **DES** (Data Encryption Standard) šifre. Široko je prihvaćena u svetu zbog svoje dokazane otpornosti na napade. 1976. se takođe pojavila ideja javnih ključeva. Godinu kasnije grupa početnika u kriptografiji Rivest, Shamir i Adleman stvorili su algoritam koji su po prvim slovima svojih prezimena nazvali **RSA** algoritam. To je bila praktična šifra sa javnim ključevima koja se mogla koristiti i za šifriranje poruka i za digitalni potpis, a bazirala se na težini faktoriziranja velikih brojeva. 1984.-1985. u softveru za čitanje novosti na USENET-u upotrebljena je *rot13 šifra* (rotiranje slova za 13) da bi se sprečio pristup dece, za njih neprikladnim sadržajima. Ovo je prvi poznati primer uspešnog korišćenja šifre sa javnim ključem. 1990. je u Švajcarskoj objavljen: "Predlog za novi Standard za šifriranje blokova podataka" tj. predlog za International Data Encryption Algorithm (**IDEA**), koji bi trebao zameniti DES. IDEA

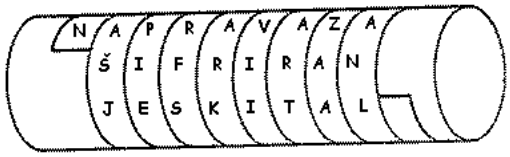
koristi 128-bitni ključ i koristi operacije koje je lako implementirati na računaru. 1991. Phil Zimmermann objavljuje prvu verziju svog **PGP**-a (Pretty Good Privacy) programa za zaštitu e-mailova i podataka uopšte. Zbog toga što je bio freeware, komercijalni proizvodi iste vrste su redom propali, a PGP je postao svetski standard. U prvo vreme koristio je RSA algoritam koji se dugo vremena smatrao dosta sigurnim. Računari su sve brži i brži, a razvoj svega vezanog uz njih sve je

otvoreni tekst	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
šifrat	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

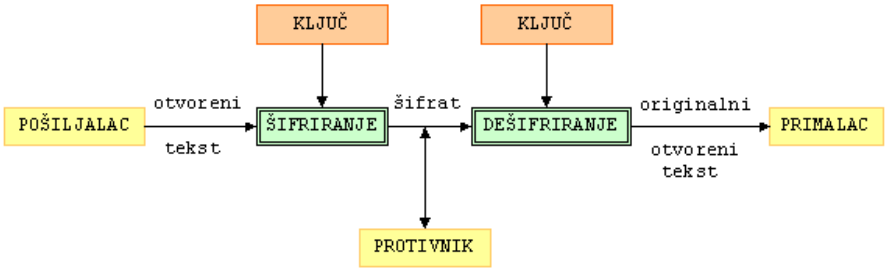
teže pratiti. Budućnost kriptografije je danas povezana s budućnošću računara.

2. Osnovni pojmovi kriptografije

Kriptografija je naučna disciplina, koja se bavi proučavanjem metoda za slanje poruka, u takvom obliku da ih samo onaj kome su namenjene može pročitati. Sama reč kriptografija je grčkog porekla i mogla bi se doslovno prevesti kao tajnopis.



Osnovni zadatak kriptografije je omogućiti dvema osobama (*pošaljilac* i *primalac* - u kriptografskoj literaturi su za njih rezervirana imena Alice i Bob) komuniciranje preko nesigurnog komunikacijskog kanala (telefonska linija, računarska mreža, ...) na način da treća osoba (njihov protivnik - u literaturi se najčešće zove Eva ili Oskar), koja može nadzirati komunikacijski kanal, ne može razumeti njihove poruke. Poruku koju pošaljilac želi poslati primaocu zvaćemo ***otvoreni tekst*** (engl. plaintext). To može biti tekst na njihovom maternjem jeziku, numerički podaci ili bilo što drugo. Pošalilac transformiše otvoreni tekst koristeći unapred dogovoreni ***ključ.*** Taj postupak se naziva ***šifriranje,*** a dobijeni rezultat ***šifrat*** (engl. ciphertext) ili ***kriptogram***. Nakon toga pošaljilac pošalje šifrat preko nekog komunikacijskog kanala. Protivnik prisluškujući može saznati sadržaj šifrata, ali ne može odrediti otvoreni tekst. Za razliku od njega, primalac koji zna ključ kojim je šifrirana poruka može dešifrovati šifrat i odrediti otvoreni tekst.



Proces kriptografije

Za razliku od dešifriranja, kriptoanaliza ili dekriptiranje je nučna disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa. Kriptologija je pak grana nauke, koja obuhvata kriptografiju i kriptoanalizu.
Kriptografski algoritam ili šifra je matematička funkcija koja se koristi za šifriranje i dešifriranje. Radi se o dve funkcije, jednoj za šifriranje, a drugoj za dešifriranje. Te funkcije preslikavaju osnovne elemente otvorenog teksta (najčešće su to slova, bitovi, grupe slova ili bitova) u osnovne elemente šifrata, i obratno. Funkcije se biraju iz određene familije funkcija u zavisnosti od ključa. Skup svih mogućih vrednosti ključeva nazivamo prostor ključeva. Kriptosistem se sastoji od kriptografskog algoritma, te svih mogućih otvorenih tekstova, šifrata i ključeva.
Najčešći vidovi napada na računarske mreže Internet/Intranet tipa su:

- Prisluškivanje – neovlašćeno pristupanje podacima u otvorenom obliku i lozinkama,
- Lažno predstavljanje – neautorizovani pristup podacima ili kreiranje neautorizovanih podataka,
- Napad tipa ukidanja servisa (denial-of-service) – onemogućavanje funkcionisanja mrežnih servisa i resursa,
- Ponavljanje poslatih poruka – neovlašćena kontrola komunikacije subjekata i ponavljanje, izmena ili sprečavanje prenosa podataka,
- Pogađanje lozinke – neovlašćeni pristup podacima uz pomoć otkrivene lozinke,
- Kriptoanaliza – otkrivanje tajnih ključeva – otkrivanje podataka u otvorenom obliku na bazi šifrata i otkrivenog tajnog ključa,
- Napadi tipa Trojanskog konja – distribucija zlonamernih programa na radne stanice,
- Virusi – uništenje podataka.

Iako pomenuti napadi nisu specifični samo za TCP/IP računarske mreže oni su tu najviše ispoljeni jer se daleko najveći broj računarskih mreža u svetu bazira na Internet tehnologijama.
Mogući načini odbrane od navedenih napada su sledeći:

- Šifrovanje – zaštita tajnosti podataka i lozinki,

- Primena tehnologije digitalnog potpisa – provera autentičnosti, zaštita integriteta podataka i obezbeđenje neporecivosti za sadržaj poslate poruke,
- Procedura jake autentikacije – bezbedna međusobna autentikacija strana u komunikaciji,
- Korišćenje jakih ključeva i česta izmena ključeva – sprečavanje metoda kriptoanalize,
- Zaštita adresa servera – zaštita od napada tipa ukidanje servisa,
- Korišćenje digitalnih certifikata kao jednoznačnih identifikacionih parametara subjekata u komunikaciji,
- Korišćenje smart kartica za generisanje digitalnog potpisa i bezbedno čuvanje ključeva i drugih kriptografskih parametara,
- Višenivoska antivirusna zaštita.

U cilju odbrane od navedenih potencijalnih napada na mrežu, najsvrsishodnije je primeniti kombinovane metode zaštite koje se sastoje od većine gore navedenih metoda.

Najkvalitetnija kriptografska rešenja koja se primenjuju u savremenim računarskim mrežama baziraju se na primeni simetričnih kriptografskih sistema za zaštitu tajnosti (po mogućstvu uz korišćenje sopstvenih simetričnih algoritama višeg kriptografskog kvaliteta), asimetričnih kriptografskih sistema baziranih na tehnologiji digitalnog potpisa, digitalnih certifikata i hardverskih modula (kriptografski koprocesori i smart kartice). Ovakvi sistemi zaštite su projektovani da se uspešno odbrane od potencijalnih opasnosti i napada u cilju ugrožavanja bezbedno osetljivih resursa informacionih sistema.
Kriptografski algoritmi koji se primenjuju u sistemima zaštite Internet/Intranet računarskih mreža dele se u dve velike grupe:

- Simetrični kriptografski algoritmi,
- Asimetrični kriptografski algoritmi.

3. Simetrični i asimetrični kriptografski algoritmi

Podela je izvedena na osnovu posedovanja informacija neophodnih za šifrovanje i dešifrovanje. Primenom simetričnih kriptografskih algoritama se, kao i u tradicionalnim sistemima zaštite, ostvaruje funkcija zaštite tajnosti u savremenim informacionim sistemima.
Sa druge strane, primenom asimetričnih kriptografskih algoritama i tehnologije digitalnog potpisa ostvaruju se sledeće funkcije u savremenim računarskim mrežama:

4. Autentičnost strane koja je poslala digitalno potpisanu poruku,
5. Zaštitu integriteta podataka u poruci koja je poslata,
6. Neporecivost elektornskog potpisnika za sadržaj date poruke.

3.1. Simetrični kriptografski algoritmi

Grupu simetričnih kriptografskih algoritama predstavljaju algoritmi kod kojih je ključ za šifrovanje identičan ključu za dešifrovanje. Algoritmi iz ove grupe se takođe nazivaju i algoritmi sa tajnim ključem jer je tajnost ključa koji se koristi i za šifrovanje i za dešifrovanje esencijalna za bezbednost poruka u sistemu. Ovi sistemi predstavljaju osnovu tradicionalne kriptološke teorije i razvijaju se već veoma dugi niz godina. S obzirom da zaštita informacija težišnu primenu ima u poslovima vezanim za državne strukture (vojska, policija i diplomatija), ovi sistemi su bili isključivo tajni sistemi, namenski definisani i realizovani od strane nadležnih državnih institucija. Sa porastom intenziteta i primene elektronskih oblika komunikacija javila se potreba za definisanjem javnih simetričnih kriptografskih algoritama pa je u poslednjih desetak godina definisano više javnih simetričnih kriptografskih algoritama za primenu u aplikacijama u kojima za to postoji potreba.
Simetrični kriptografski sistemi
Ovi algoritmi se uglavnom koriste u aplikacijama vezanim za sisteme poslovnih i finansijskih komunikacija. Imajući u vidu eksplozivni razvoj poslovnih i finansijskih sistema u poslednje vreme, javni simetrični kriptografski algoritmi su postali dominantni u pogledu korišćenja. Međutim, nijedan od njih nije usvojen kao generalni standard već pomenuti sistemi uglavnom koriste odgovarajuće liste mogućih kriptografskih algoritama. Na taj način, kao parametar komunikacije, bira se i identifikator simetričnog šifarskog algoritma koji će se koristiti pri datoj transakciji.

Iako je po masovnosti komercijalna upotreba simetričnih kriptografskih algoritama daleko prevazišla upotrebu u tajnom sektoru (vezanom za državne strukture), glavni teorijski rezultati se i dalje dešavaju u oblasti tajne kriptologije i tajnih sistema. Velika većina država ima specijalizovane organizacije koje se bave dizajniranjem i analizom raznih vrsta šifarskih sistema (npr. NSA u SAD). Stepeni dostignuća u toj oblasti najčešće nisu javno poznati i nalaze se u sferi pretpostavki.
Postoje dve osnovne vrste simetričnih šifarskih sistema:

- blok šifarski sistemi,
- sekvencijalni šifarski sistemi (stream cipher).

Blok šifarski sistemi

Blok šifarski sistemi procesiraju blokove nešifrovanog signala - otvorenog teksta (OT) i šifrovanog signala – šifrata (ST), obično u blokovima čija je veličina 64 bita ili više. Sekvencijalni šifarski sistemi procesiraju nizove bita, bajtova ili reči (16 ili 32 bita) OT i ST. Ako se u toku procesa šifrovanja jedne poruke nekim blok šifarskim sistemom više puta pojavljuje isti blok otvorenog teksta (OT) rezultat će biti uvek isti blok šifrata (ST), što nije slučaj kod sekvencijalnih šifarskih sistema. Kod sekvencijalnih šifarskih sistema verovatnoća da isti niz bita, bajtova ili reči OT pri

svakom pojavljivanju u jednoj poruci proizvodi isti šifrat teži nuli ukoliko su niz za šifrovanje i otvoreni tekst nezavisni. Blok šifarski sistemi se veoma mnogo koriste u sistemima poslovnih i finansijskih transakcija, ali su njihove bezbednosne osobine dosta slabije od sekvencijalnih šifarskih sistema. I pored toga definisan je veliki broj javnih algoritama baziranih na blok šifarskim sistemima, kao što su DES, 3-DES, RC2, IDEA, i mnogi drugi koji su našli veoma široku primenu u savremenim informacionim sistemima. U 2001. godini, NIST organizacija u SAD je usvojila novi standard AES (Advanced Encryption Standard).

AES algoritam

Kao što je već rečeno, u toku 2001. godine, NIST (National Institute of Standards and Technology) organizacija u SAD je objavila standard za simetrične kriptografske algoritme AES (Advanced Encryption Standard) koji treba da zameni prethodni standard DES (Data Encryption Standard). Nakon duge selekcione procedure, za AES algoritam izabran je Rijndael algoritam koga su realizovali Belgijski istraživači: Joan Daemen i Vincent Rijmen. Rijndael predstavlja blok šifarski algoritam koji podržava promenljivu dužinu bloka informacije (128, 192 i 256 bita) kao i promenljivu dužinu ključa (128, 192 i 256 bita). Naime, poruke šifrovane DES algoritmom su se, zbog nedostataka u samom algoritmu (bezbedonosni nedostaci u supstitucionim s-tabelama), male dužine ključa (56-bita) i povećane procesne moći računara, mogle dešifrovati za samo par časova. Nakon selekcione procedure, za realizaciju AES standarda izabran je Rijndael algoritam koga su realizovali belgijski matečatičari: Joan Daemen i Vincent Rijmen. Rijndael je blok šifarski algoritam koji podržava promenljivu dužinu bloka otvorenog teksta (128, 192 i 256 bita) kao i promenljivu dužinu ključa (128, 192 i 256 bita). Rijndael algoritam je u odnosu na konkuretske algoritme (MARS, RC6, Serpent, Twofish) bio brži i zahtevao je manje operativne memorije u procesu šifrovanja i dešifrovanja poruka. Rijndael algoritam sa 128-bitnom dužinom ključa je brži za oko 2.5 puta u odnosu na 3-DES algoritam. AES algoritam realizuje operacije šifrovanja i dešifrovanja bloka podataka u promenljivom broju ciklusa. Broj ciklusa zavisi od veličine ključa i iznosi 10/12/14 za veličinu ključa 128/192/256 bita, respektivno. Pre početka šifrovanja ili dešifrovanja vrši se ekspanzija ključa.

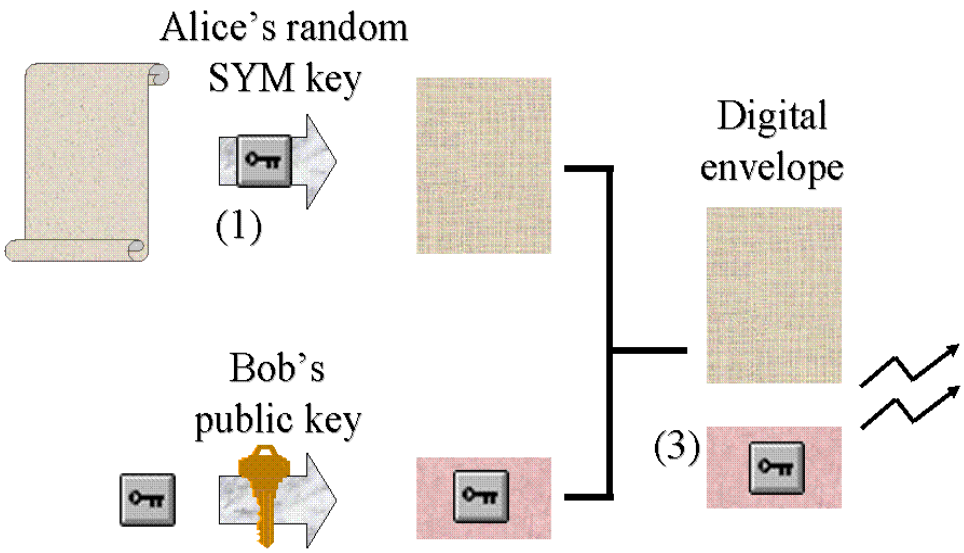
3.2. Asimetrični kriptografski algoritmi

Asimetrični kriptografski algoritmi predstavljaju jedno od najvećih dostignuća kriptologije druge polovine dvadesetog veka. Otkriveni su u procesu rešavanja problema vezanih za zaštitu tajnosti i distribuciju ključeva koji je često bio aktuelan u primenama simetričnih kriptografskh algoritama. Naime, u asimetričnim šifarskim sistemima se koriste različiti ključevi za šifrovanje i dešifrovanje, tzv. javni i tajni ključ, tako da ključ za šifrovanje može imati svako a samo posednik ključa za dešifrovanje može dešifrovati poruku. Međutim, visoka računarska zahtevnost ovih algoritama utiče na performanse sistema u kojima se primenjuju,

tako da se ne preporučuje primena za zaštitu tajnosti informacija u sistemima sa velikim protokom informacija. Ovo naravno ne dezavuiše automatski ove algoritme jer način na koji je uz korišćenje ovakvih algoritama moguće ostvariti funkcije integriteta, autentičnosti i neporicanja ima nesumnjivu prednost nad tradicionalnim tehnikama. U literaturi je opisano više algoritama sa javnim ključem ali sa stanovišta kvaliteta, otpornosti na razne vrste napada, efikasnost i lakoću implementacije te rasprostranjenost, nisu svi podjednako dobri. U tom smislu se kao prirodni izbor nameće RSA algoritam koji više od dvadeset godina odoleva svim teorijskim i tehnološkim napadima. Opis i način upotrebe ovog algoritma propisani su u standardu PKCS#1 verzija 2. Pored RSA algoritma moguće je koristiti i druga dva algoritma, DSA (Digital Signature Algorithm) i ECDSA (Elliptic Curve DSA), koja spadaju u standard digitalnog potpisa (NIST standard DSS (Digital Signature Standard).

PKCS#1 standard

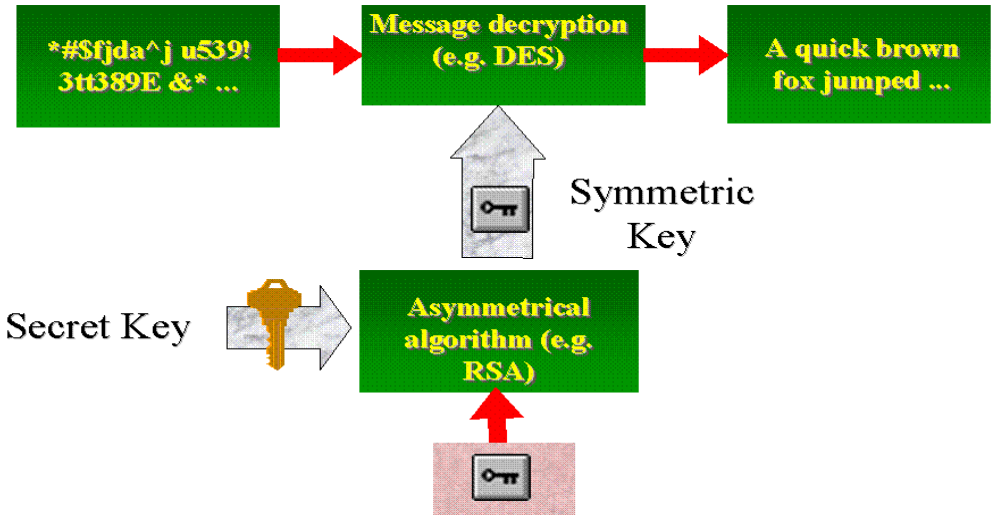
PKCS#1 standard opisuje metode šifrovanja podataka korišćenjem RSA asimetričnog algoritma i najčešće se koristi za konstrukciju digitalnog koverta i digitalnog potpisa.



Digitalna envelopa – šifrovanje

U slučaju digitalnog koverta, sadržaj poruke se prvo šifruje određenim simetričnim algoritmom (kao što su DES, 3-DES, RC2, RC4, IDEA, AES, ili neki namenski privatni algoritmi). Zatim se tajni ključ primenjenog simetričnog algoritma koji je upotrebljen za šifrovanje date poruke šifruje RSA algoritmom upotrebom javnog ključa korisnika kome je data poruka namenjena (RSA public key operacija). Tako šifrovan sadržaj poruke i tajni ključ kojim je ta poruka šifrovana zajedno

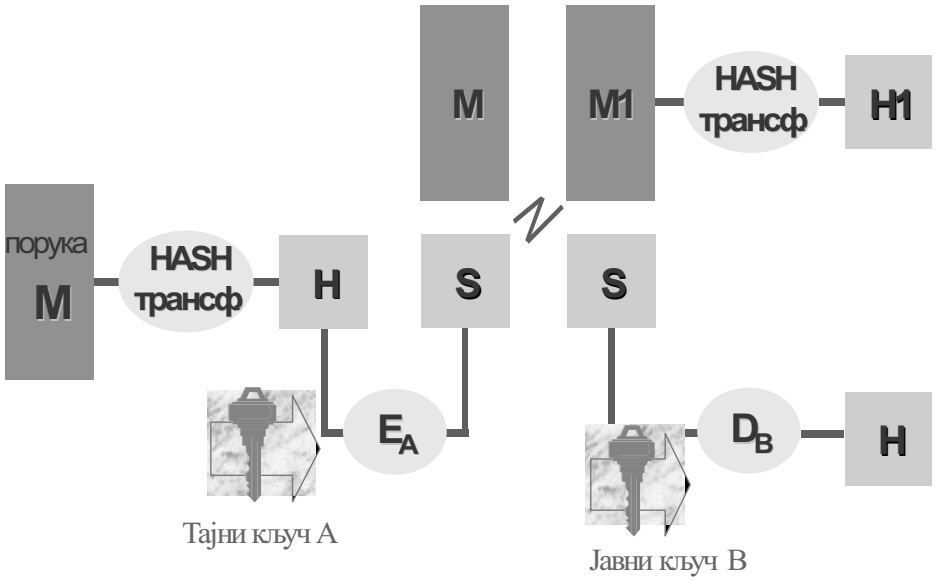
predstavljaju digitalni koverat. Postupak šifrovanja i dešifrovanja putem tehnologije digitalnog koverta je prikazan na sledecim slikama.



Digitalna envelopa – dešifrovanje

U slučaju digitalnog potpisa (sledeca slika), sadržaj koji treba da se potpiše, poruka M, prvo se redukuje u otisak poruke (message digest), H, primenom nekog od metoda za kreiranje otiska poruke, message-digest algoritma (kao što su na primer MD5 ili SHA-1 algoritmi), a zatim se dobijeni otisak poruke šifruje primenom, na primer, RSA algoritma koristeći tajni ključ potpisnika poruke (RSA private key operacija), ključ A. Šifrovani otisak poruke predstavlja digitalni potpis date poruke, S, i postaje njen pridruženi deo. Kada ovakva poruka stigne do primaoca kojem je namenjena izvršava se postupak verifikacije digitalnog potpisa. Ovaj postupak se sastoji od dešifrovanja otiska dobijene poruke primenom RSA algoritma uz upotrebu javnog ključa pošiljaoca poruke, ključ B. Po dešifrovanju digitalnog potpisa primalac poruke izvrši isti message digest postupak nad dobijenom porukom, M1. Ako je dobijeni otisak poruke, H1, identičan sa dešifrovanom vrednošću otiska, verifikacija je uspela, u protivnom verifikacija je negativna.
Ukoliko je verifikacija uspela, primalac poruke je siguran u sledeće:

- Autentičnost pošiljaoca – jer je uspešno dešifrovao otisak poruke primenom RSA algoritma sa javnim ključem datog pošiljaoca,
- Integritet poslate poruke – ako su izračunati i dešifrovani otisci date poruke identični zaključuje se da poruka na prenosnom putu nije menjana, i
- Nemogućnost da pošiljalac naknadno porekne da je tu poruku poslao jer je njegov digitalni potpis uspešno verifikovan.



Procedura digitalnog potpisa i verifikacije

Da bi dati primalac bio u mogućnosti da prima poruke od datog pošiljaoca i sprovede proces verifikacije digitalnog potpisa mora imati mogućnost pristupa javnom ključu pošiljaoca. Pristup i distribucija javnih ključeva se mogu organizovati na različite načine a najčešće se realizuju u procesu utvrđivanja identiteta putem razmene digitalnih certifikata.

PKCS#1 standardom se pored bezbednosnih mehanizama definiše i unutrašnja struktura validnih poruka čime se omogućava dodatni mehanizam verifikacije ispravnosti poruka. Naime, svaka poruka koja ima narušenu strukturu se smatra neispravnom i odbacuje se. Treba posebno naglasiti da je trenutno aktuelan i važeći PKCS#1 standard verzije 2 i da su njime značajno izmenjene preporuke date u PKCS#1 standardu verzije 1.5, koje se odnose na format bloka podataka koji podleže operacijama šifrovanja i potpisivanja. Razlog za ovakve drastične promene leži u činjenici da prema verziji 1.5 pri formiranju bloka za šifrovanje postoji niz bita na početku bloka koji je uvek isti. To se može iskoristiti da se bez poznavanja tajnih informacija, samo uz poznavanje šifrata dođe do otvorenog teksta. Ovde treba naglasiti da ovim nije kompromitovana bezbednost samog RSA algoritma već je, grubo govoreći, način njegove upotrebe bio takav da je pod određenim uslovima dolazilo do oticanja informacija.

U verziji 2 ovog standarda blok podataka koji se šifruje prethodno se kodira OAEP (Optimal Assymetric Encryption Padding) metodom koja ima dobre bezbednosne karakteristike tako da čak ni dva identična bloka podataka posle kodiranja ovim metodom ne daju isti rezultat. Time su izbegnute slabosti detektovane u verziji 1.5.

PKCS#1 standard verzije 2 je neophodno primeniti u mehanizmima zaštite u specijalizovanim računarskim mrežama i informacionim sistemima.

Zaključna razmatranja

Globalna svetska mreža kakva je Internet, otvorena je i dostupna svima, tako da uvek postoji mogućnost zlonamernih praćenja i izmena poruka, zbog toga je vrlo važno implementirati zaštitne aplikacije koje takođe prate taj razvoj. Dakle zaštita mora obuhvatiti :

- Zaštitu tajnosti informacija (sprečavanje otkrivanja njihovog sadržaja);
- Integritet informacija (sprečavanje neovlašćene izmene informacija);
- Autentičnost informacija (definicija i provera identiteta pošaljioca).

Kriptografija kao nauka koja se bavi metodama očuvanja tajnosti informacija pruža rešenje ovog problema. Najbitnije je da se tajni ključ u celom postupku komunikacije *nigde ne šalje* jer ne postoji potreba da bilo ko osim njegovog vlasnika bude upoznat s njim. Dakle, možete bilo kome da pošaljete šifriranu poruku ako znate javni ključ osobe kojoj šaljete, a samo primalac svojim tajnim ključem može da dešifruje poruku. Danas svi želimo da zaštitimo svoje podatke koji su nam važni, upravo ova nauka nam pomaže u tome.
Kriptografija je neophodna ako želimo da imamo svoju privatnost danas u globalnom svetu, u procesu elektronske trgovine (potpisivanje i upotreba čekova, anonimna kupovina), u privatnoj komunikaciji, u razmeni poslovnih informacija, ideja i zabavi.

Literatura

1. http://web.math.hr/~duje/kript/josblo,19.04,2008
- http://hr.wikipedia.org/wiki/Kriptografija,19,04,2008
- http://free-zg.t-com.hr/Davor-Sever/kriptografija.htm, 19,04,2008
- A. Dujella, M. Maretić: *Kriptografija*, Element, Zagreb, 2007.
- http://sr.wikipedia.org/sr
- http://alas.matf.bg.ac.rs/~pd00011/kript/kript.html
- Bruce Schneier: *Primenjena kriptografija, prevod drugog izdanja*, Mikro,knjiga,Beograd,2007.
- N. Begović: *Kriptografija*, Matematički fakultet, Beograd 2001.

CRYPTOGRAPHIC METHODS OF DATA PROTECTION IN COMPUTER SYSTEMS

Phd Mirsad Nukovic,
Richard Shoti

Abstract: The data stored in databases and sent over computer networks are a valuable asset and deserve special attention and protection in order to keep the secrecy of our business and projects. Data and due time information make work of jurists, managers and other people who make decisions much easier, so that the theft, alteration of such data and other malicious actions can affect the final outcome, authenticity, accuracy and promptness of such decisions and it is therefore really important to secure appropriate and high level data protection. The Egyptians and Indians used safe communication some 3000 years ago and from that moment the issues and ideas of it have not changed – transfer the information from one place to another as safe as possible, or in other words, make an algorithm that would hide the original message in such way that it is completely unintelligible for people who got access to it by illegal means. Such methods have improved along with the development of modern technology and so have had the methods of data encryption. The authors will try to give answers to some modern questions, encryption algorithms, data decryption and suggest possible solutions for a much safer protection.

Key words: data protection, computer system, cryptography