Internet i elektronsko poslovanje

- Proteklih godina povećanjem broja personalnih računara, upotrebom i širenjem javne mreže Interneta, kao posledica u praksi pojavilo se elektronsko trgovanje kao termin za sve transakcije ostvarene "elektronskim putem", odnosno putem računara.

- **Elektronsko poslovanje** predstavlja skup tehnologija i procedura koje automatizuju poslovne transakcije putem elektronskih sredstava
- **Elektronska trgovina** je svaka finansijska transakcija ostvarena razmjenom informacija elektronskim putem

Najvažnije društveno pozitivne karakteristike elektronske trgovine:

a) Brz pristup informacijama, što kao rezultat daje bolju dostupnost proizvoda i usluga koji se nude na tržištu
b) Transfer dokumenata uz minimalne troškove, bez nepotrebnih kašnjenja, oštećenja, gubitaka i sl.
c) Otvorenost informacionog prostora, što u smislu trgovanja ima za rezultat djelotvornije procese,
d) Mogućnost kreiranja vlastitih baza podataka i obrade njihovih informacionih sadržaja
e) Mogućnost analize proizvoda i usluga kao i razmjena iskustva i saznanja između učesnika u procesu trgovanja
f) Mogućnost analize tržišta
g) Permanentno stvaranje novih poslovnih prilika i njihovo iskorištavanje

- Elektronska trgovina smanuje troškove poslovanja i olakšava poslovanje.
- Postoje potencijalni rizici upotrebe te tehnologije
- Elektronska infrastruktura je osjetljiva na različite oblike napada

Sa ekonomske tačke gledišta, posledice otkaza tehnološke prirode ili zloupotrebe ove tehnologije od strane korisnika mogu biti sledeće:

a) **Direktni finansijski gubici kao posledica prevare** – Zlonamerna osoba može, na primer, da prebaci izvjesnu količinu novca sa jednog računa na drugi ili može da obriše podatke finansijske prirode.

b) **Gubljenje vrijednih i povjerljivih informacija** – Mnoga preduzeća memorišu i šalju informacije tehnološke prirode ili podatke o svojim kupcima i dobavljačima, čija povjerljivost je od najveće važnosti za njihovo postojanje. Ilegalan pristup takvim informacijama može prouzrokovati značajne finansijske gubitke ili štete druge vrste takvoj organizaciji.

c) **Gubljenje poslova zbog nedostupnosti servisa** – Elektronski servisi mogu biti nedostupni u dužem vremenskom periodu ili u periodu značajnom za obavljanje konkretnog posla, zbog napada na sistem od strane zlonamernih osoba ili zbog slučajnih otkaza sistema. Posledice takvih događaja (finansijske prirode ili druge vrste) mogu biti katastrofalne za jedno preduzeće.

d) **Neovlašćena upotreba resursa** – Napadač koji ne pripada organizaciji koju napada može neovlašćeno pristupiti nekim resursima njenog računarskog sistema i upotrijebiti ih radi pribavljanja imovinske koristi. Tipičan primjer resursa osjetljivog na takvu vrstu napada je telekomunikacioni servis. U opštem slučaju, "hakeri" koriste računar kome su neovlašćeno pristupili kako bi napali ostale računare u mreži.

e) **Gubljenje poslovnog ugleda i poverenja klijenata** – Preduzeće može pretrpjeti značajne gubitke zbog lošeg iskustva svojih klijenata ili zbog negativnog publiciteta koji mogu biti posledica napada na njegov servis elektronske trgovine, ili ponašanja zlonamjerne osobe koja se predstavlja kao pripadnik tog preduzeća.

f) **Troškovi izazvani neizvjesnim uslovima poslovanja** – Česti prekidi funkcionisanja servisa, izazvani napadima spolja ili iznutra, greškama i sl. mogu paralisati izvršenje poslovnih transakcija u značajnom vremenskom periodu. Na primjer, potvrde transakcija koje ne mogu da se prenesu komunikacionim kanalima, transakcije koje mogu biti blokirane od strane trećih lica itd. Finansijski gubici koje ovakvi uslovi poslovanja mogu izazvati mogu biti značajni.

Zbog navedenih problema, potrošači koji koriste takve servise elektronske trgovine mogu pretrpjeti direktne ili indirektne finansijske gubitke.

- Rizici koje sa sobom nosi upotreba elektronske trgovine mogu se izbjeći upotrebom odgovarajućih mjera bezbjednosti
- mjere mogu biti tehnološke i pravne

Osnovni ciljevi mjera bezbjednosti u informacionim sistemima su:

a) **Povjerljivost** – obezbjeđuje nedostupnost informacija neovlašćenim licima.

b) **Integritet** – obezbjeđuje konzistentnost podataka, sprečavajući neovlašćeno generisanje, promjenu i uništenje podataka.

c) **Dostupnost** – obezbjeđuje da ovlašćeni korisnici uvijek mogu da koriste servise i da pristupe informacijama.

d) **Upotreba sistema isključivo od strane ovlašćenih korisnika** – obezbjeđuje da se resursi sistema ne mogu koristiti od strane neovlašćenih osoba niti na neovlašćen način.

Glavne naučne discipline čiji rezultati se koriste da bi se ostvarili pomenuti ciljevi su nauka o bezbjednosti komunikacija i nauka o bezbjednosti u računarima

- **Bezbjednost komunikacija** označava zaštitu informacija u toku prenosa iz jednog sistema u drugi
- **Bezbjednost u računarima** označava zaštitu informacija unutar računara ili sistema – ona obuhvata bezbjednost operativnog sistema i softvera za manipulaciju bazama podataka

Potencijalne prijetnje jednom informacionom sistemu koji sadrži podsistem za elektronsku trgovinu su:

a) **Infiltracija u sistem** – Neovlašćena osoba pristupa sistemu i u stanju je da modifikuje datoteke, otkriva povjerljive informacije i koristi resurse sistema na nelegitiman način. U opštem slučaju, infiltracija se realizuje tako što se napadač predstavlja kao ovlašćeni korisnik ili korišćenjem slabosti sistema (npr. mogućnost izbjegavanja provjera identiteta i sl.). Informaciju neophodnu za infiltraciju, napadač dobija koristeći neku drugu vrstu napada. Primjeri takvih napada su "dumpster diving attack", kod koga napadač dobija potrebnu informaciju pretražujući korpu za otpatke svoje žrtve, i "socijalni inženjering" kod koga napadač dobija neophodnu informaciju primoravajući na neki način (ucjena, prijetnja i sl.) svoju žrtvu da mu je da.

b) **Prekoračenje ovlašćenja** – Lice ovlašćeno za korišćenje sistema koristi ga na neovlašćeni način. To je tip prijetnje koju ostvaruju kako napadači iznutra ("insiders") tako i napadači spolja. Napadači iznutra mogu da zloupotrebljavaju sistem radi sticanja beneficija. Napadači spolja mogu da se infiltriraju u sistem preko računa sa manjim ovlašćenjima i nastaviti sa infiltracijom u sistem koristeći takav pristup radi neovlašćenog proširenja korisničkih prava.

c) **Suplantacija** – Obično poslije uspješno izvršene infiltracije u sistem, napadač ostavlja u njemu neki program koji će mu omogućiti da olakša napade u budućnosti. Jedna od vrsta suplantacije je upotreba "trojanskog konja" – to je softver koji se korisniku predstavlja kao normalan, ali koji prilikom izvršenja otkriva povjerljive informacije napadaču. Na primer, tekst procesor može da kopira sve što ovlašćeni korisnik unese u jednu tajnu datoteku kojoj može da pristupi napadač.

d) Prisluškivanje – Napadač može da pristupi povjerljivim informacijama (npr. lozinci za pristup sistemu) prostim prisluškivanjem protoka informacija u komunikacionoj mreži. Informacija dobijena na ovaj način može se iskoristiti radi olakšavanja drugih vrsta napada.

e) Promjena podataka na komunikacionoj liniji – Napadač može da promijeni informaciju koja se prenosi kroz komunikacionu mrežu. Na primer, on može namjerno da mijenja podatke finansijske prirode za vreme njihovog prenošenja kroz komunikacioni kanal, ili da se predstavi kao ovlašćeni server koji od ovlašćenog korisnika zahtijeva povjerljivu informaciju.

f) **Odbijanje servisa** – Zbog čestih zahtjeva za izvršenje složenih zadataka izdatih od strane neovlašćenih korisnika sistema, servisi sistema mogu postati nedostupni ovlašćenim korisnicima.

g) **Negacija transakcije** – Poslije izvršene transakcije, jedna od strana može da negira da se transakcija dogodila. Iako ovakav događaj može da nastupi usled greške, on uvijek proizvodi konflikte koji se ne mogu lako riješiti.

Najčešći vidovi transakcija u okviru elektronskog poslovanja su:

1. **između poslovnih subjekata**
2. **Poslovni subjekt - korisnik (kupac)**

   a) transakcije prema bankama (direktno raspolaganje korisnikovim računom)

   b) kupovina proizvoda preko web prodavnica, odnosno kupovina proizvoda putem Interneta (kreditne kartice i sl.)

Da bi se ostvarila neporecivost elektronskih transakcija, zaštita mora da osigura sledeće osnovne pretpostavke:

a) **Autentifikacija**

- Omogućava utvrđivanje identiteta korisnika, pri čemu su na raspolaganju tehnologije od korisničkog ID-a i statičke lozinke, preko tokena i biometrijskih tehnologija, do rešenja koja se temelje na asimetričnoj kriptografiji i sertifikatima, softverskim ili hardverskim (pametne kartice)

b) **Privatnost**

- Sprečava neautorizovani pristup podacima, ili presretanje istih tokom komunikacijskog procesa i ostvaruje se enkripcijom podataka

c) **Integritet podataka**

- osigurava se izvornost podataka, odnosno sprečavanje promene podataka primjenom digitalnog potpisa

Ispunjenje ovih pretpostavki osigurava se prije svega **kriptografski**, a time se postiže i pravno valjani dokaz o inicijatoru, kao i o samoj transakciji.

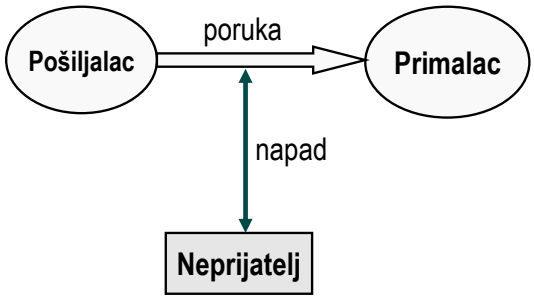
- Tehnologije koje su se nametnule kao opšte prihvaćeno rešenje za sigurnost elektronskih transakcija, odnosno realizaciju neporecivosti informacija su koncept **Digitalnog potpisa** i **Public Key Infrastrukture (PKI)**

OSNOVE KRIPTOGRAFIJE I KRIPTOGRAFSKE TEHNOLOGIJE

Kriptografija je stručni naziv za proces pretvaranja informacija u gomilu nepovezanih podataka koje niko osim primaoca ne može pročitati.

Namjena kriptografije je da:

- zaštiti memorisanu informaciju bez obzira ako je neko pristupio podacima
- zaštiti prenijetu informaciju bez obzira ako je prenos bio posmatran ("monitoring")



Ciljevi kriptografije su da se obezbijedi:

- **Povjerljivost (tajnost)** – prevencija od neautorizovanog pristupa informacijama (obezbjeđuje privatnost za poruke)
- **Integritet** – prevencija od neautorizovanog menjanja informacija (obezbjeđuje potvrdu da poruka ostaje nepromijenjena)
- **Raspoloživost** – prevencija od neautorizovanog onemogućavanja pristupa informacijama ili resursima
- **Autentifikacija** – prevencija od lažnog predstavljanja (identifikacija izvora poruke i verifikacija identiteta osobe
- **Neporicanje** – prevencija od lažnog poricanja slanja date poruke/dokumenta (može se dokazati da poruka/dokument dolazi od datog entiteta iako taj entitet to poriče)

Mjere zaštite podrazumijevaju:

- **Prevencija** – preduzimanje preventivnih aktivnosti za zaštitu podataka i računarskih sistema od mogućeg uništenja
- **Detekcija** – otkrivanje kako je narušena zaštita, kada je narušena i ko je narušio
- **Reakcija** – preduzimanje aktivnosti koje dovode do restauracije podataka ili do restauracije računarskog sistema

Na konkretnom primeru e-Commerca pomenute mjere zaštite mogu podrazumijevati sledeće:

- **Prevencija** - Šifrovanje broja kreditne kartice
- **Detekcija** - Listing svih transakcija u toku mjeseca urađenih datom kreditnom karticom
- **Reakcija** - Blokiranje stare kartice i podnošenje zahtjeva za izdavanje

Kriptografija i vrste algoritama

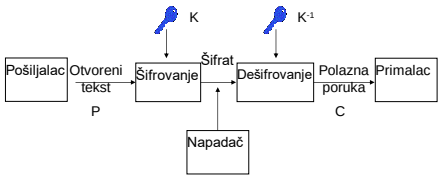
- Osnovni element koji se koristi u kriptografiji naziva se **šifarski sistem** ili **algoritam šifrovanja**
- Svaki šifarski sistem obuhvata par transformacija podataka, koje se nazivaju **šifrovanje** i **dešifrovanje**.

- **Šifrovanje** je procedura koja transformiše originalnu informaciju u šifrovane podatke (šifrat)
- **Dešifrovanje**, rekonstruiše originalnu informaciju na osnovu šifrata
- U šifarskoj transformaciji se koristi jedna nezavisna vrijednost koja se naziva **ključ** šifrovanja

Šema šifrovanja ima 5 komponenti:

1) Tekst koji se šifruje (plaintext)
2) Algoritam šifrovanja
3) Tajni ključ
4) Šifrovani tekst (ciphertext)
5) Algoritam dešifrovanja

Šematski prikaz kriptovanja (Encryption) i dekriptovanja (Decryption)



- Kriptografski algoritmi zasnovani su na matematičkoj funkciji koja se koristi za šifrovanje i dešifrovanje.
- Razlikuju se dvije vrste algoritama:
  A) **Ograničeni algoritmi**: bezbjednost se zasniva na tajnosti algoritma (istorijski interesantni)
- B) **Algoritmi zasnovani na ključu**: bezbjednost se zasniva na ključevima, a ne na detaljima algoritma koji se može publikovati i analizirati (algoritam je javno poznat, a ključ se čuva tajnim).

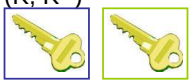
- Šifrovanje je, pojednostavljeno, matematička funkcija čiji izlaz zavisi od dva ulazna parametra :
  1.originalna poruka koja se šifrira P **(**Plaintext)
  2.ključ K

Rezultat je niz naizgled nepovezanih brojeva koji se mogu, bez straha od mogućnosti da poruka dođe u neželjene ruke, prenositi do osobe kojoj je namijenjena.

Da bi šifrovanu poruku druga osoba mogla da koristi potrebno je sprovesti obrnuti postupak od šifrovanja, dešifrovanje.

- Dešifrovanje je, pojednostavljeno, matematička funkcija čiji izlaz zavisi od dva ulazna parametra:
  1. šifrovana poruka C (Chipertext)
  2. ključ K^{-1}
- kao rezultat funkcije dobija se originalna poruka

- Minimalna i potrebna informacija koju dvije osobe moraju da dijele, ako žele da razmjenjuju podatke na siguran način, skup ključeva (K, K^{-1})

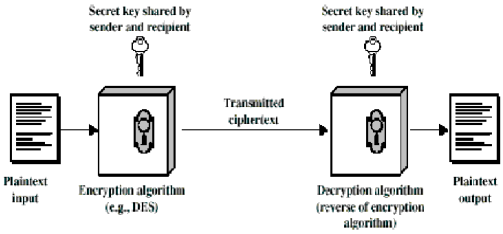


- Prema odnosu ključeva K i K^{-1} kriptografske sisteme dijelimo na simetrične i asimetrične.

Zaštita ključa

(zaštita zavisi od zaštite ključa a ne od zaštite algoritma)

Kirkohov (Kerckhoff) princip: Važan kriterijum za ocjenjivanje kriptografskih algoritama; napadač poznaje kriptosistem ili algoritme, koje upotrijebljavamo, ali ne i ključeve koji nam obezbjeđuju sigurnost.



Sigurnost kriptovanog algoritma

- Vrijeme potrebno za "razbijanje" algoritma mora da bude duže od vremena u kome podaci moraju da ostanu tajni.
- Takođe, potrebno je da bude zadovoljen i uslov da broj podataka šifrovanih jednim ključem bude manji od broja potrebnih podataka da se dati algoritam "razbije".

Simetrično šifrovanje

- Simetrično šifrovanje je šifrovanje tajnim ključem, pri čemu je ključ za šifrovanje identičan ključu za dešifrovanje:

$$K = K^{-1}$$

- u slučaju simetričnog šifrovanja pošiljalac i primalac poruke koriste isti tajni ključ

Poznati simetrični algoritmi su:

- DES (Data Encryption Standard) – ključ je dužine 56 bita
- Triple DES, DESX, GDES, RDES – ključ je dužine 168 bita
- (Rivest) RC2, RC4, RC5, RC6 – promenljiva dužina ključa do 2048 bita
- IDEA – osnovni algoritam za PGP – ključ je dužine 128 bita
- Blowfish – promenljiva dužina ključa do 448 bita
- AES (Advanced Encryption Standard) - radi sa blokovima od po 128 bita i koristi ključeve dužine 128, 192 i 256 bita

Data Encryption Standard (DES)

- DES je simetričan algoritam koji je IBM predstavio 1975
- Razvijan je od strane brojnih organizacija za kriptovanje poruka i podataka pa je postao najrasprostranjeniji komercijalni algoritam
- Des je blok šifra što znači da algoritam kriptuje podatke u 64-bitna bloka i koristi 64-bitni ključ
- U realnosti, samo 56 bitova se koristi za kriptovanje/dekriptovanje podataka gde preostalih 8 bitova rade kao analogni
- Upotreba 56 bita omogućava veliki prostor za ključ
- 2^{56} potencijalnih mogućnosti za ključ, čine razbijanje ovog koda (za to vrijeme) teškim kada su u pitanju napadi grubom silom (brute force)

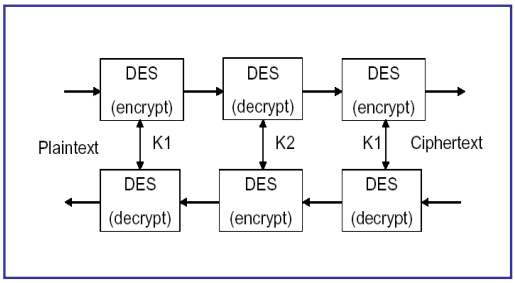
Triple DES algoritam

- U poslednjih nekoliko godina zabilježen je veliki broj probijanja DES algoritma razbijanjem ključa za kriptovanje.
- Vlada U.S. ne priznaje više DES kao standard, pa su mnoge organizacije prešle na Triple DES algoritam

- Tripl DES koristi tri ključa za kriptovanje podataka, što povećava veličinu ključa na 168 bita
- Postoji više metoda Triple DES algoritma
  I. Prvi metod: podaci se kriptuju tri puta sa tri odvojena ključa
  II. Drugi metod: podaci se kriptuju sa prvim ključem, dekriptuju sa drugim, i ponovo se kriptuje trećim ključem
  III. Treći metod: sličan je sa prethodna dva, sa tim što se isti ključ koristi u prvoj i trećoj operaciji.

- Vlada U.S razvija različite algoritme koji će postati AES (Advanced Encryption Standard) standardi

Tripl DES koristi tri ključa za kriptovanje podataka



Asimetrično šifrovanje

- Asimetrično šifrovanje je šifrovanje javnim ključem
- Svaki učesnik u komunikaciji koristi dva ključa
- Jedan ključ je javni i koristi se za šifrovanje, dok je drugi tajni i koristi se za dešifrovanje
- Tajni ključ je dostupan samo vlasniku

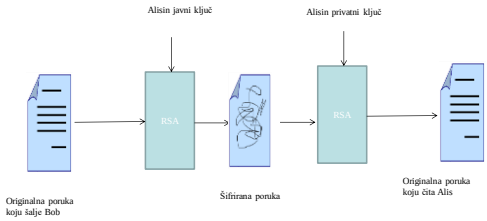
Ideja javnih ključeva

- zasnivaju se na funkcijama čiju je inverznu funkciju gotovo nemoguće odrediti
- kriptografisanje pomoću javnih ključeva je vrlo sporo
- Diffie i Hellman 1976. razvili metodu zasnovanu na ireverzibilnim funkcijama sa ključevima od 128, 256 i 512 bita

Princip javnih ključeva

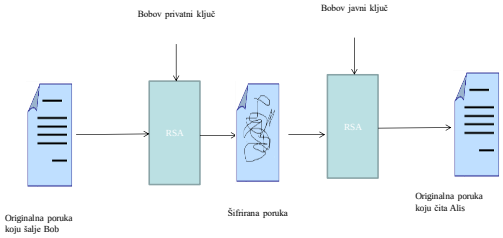
- uzmite telefonski imenik velikog grada:
  - pronađite telefonski broj određene osobe
  - pronađite osobu koja ima određeni telefonski broj
- koji ćete postupak sprovesti lako, a od kojeg ćete odustati?

Režim rada asimetričnog šifrovanja



- Oba ključa su vezana za entitet (računar ili korisnika) koji treba da dokaže svoj identitet, elektronski potpiše ili šifruje podatke

Režim rada autentifikacije



- Svrha javnog ključa je da bude svima dostupan.
- Kad šaljemo podatke nekoj osobi, šifrujemo ih javnim ključem
- Kada osoba primi podatke, dešifruje ih svojim privatnim ključem, koji samo ta osoba posjeduje.

RSA

- tvorci Ronald Rivest, Adi Shamir i Leonard Adleman
- ključevi dužine 1024 bita
- dva izuzetno velika prosta broja (sa približno po 100 cifara) je lako pomnožiti, ali gotovo nemoguće rastaviti na faktore
- proizvod – osnova za kriptografisanje, a faktori – za dešifrovanje

RSA Public Key Standard

- RSA Public Key je asimetrični algoritam šifrovanja koji koristi javni i privatni ključ za kriptovanje i dekriptovanje podataka
- RSA sistem je zasnovan na odgovarajućim matematičkim operacijama razvijen je na pretpostavci da je teško razložiti na činioce velike brojeve koji su proizvod dva prosta broja.
- RSA sistem sa javnim ključem i DES (ili neki drugi sistem sa simetričnim ključem) se obično koriste zajedno.

  Razlog: RSA je relativno spor za kriptovanje velikih blokova podataka, dok je DES pogodan za to.
- Sistemi koriste RSA da bi razmijenili DES ključeve međusobno, a zatim koriste DES algoritam da kriptuju blokove podataka. Ovakav protokol prepoznaje dvije strane i omogućava sigurnu razmjenu ključeva

- RSA sistem javnog ključa se koristi za kriptovanje i digitalni potpis

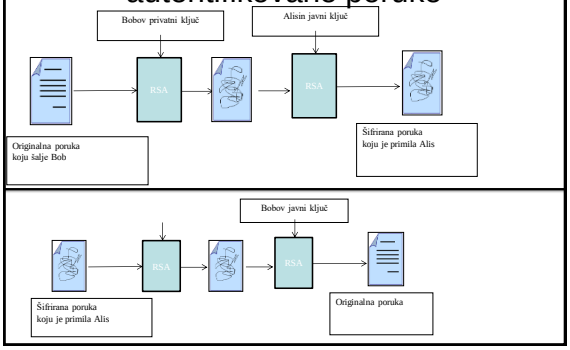
KRIPTOVANJE

- **Primjer 1**: Bob hoće da pošalje kriptovanu poruku Ani. On kriptuje poruku Aninim javnim ključem i šalje je. Pošto Ana ima privatan ključ (odgovarajući Aninom javnom ključu) koji dekriptuje podatke, podaci ostaju povjerljivi u toku tranzicije.

DIGITALNI POTPIS - prepoznaje pošiljaoca poruke.

- **Primjer 2**: Da bi se identifikovao, Bob šalje Ani poruku kriptovanu svojim privatnim ključem. Kada Ana dobije poruku, dekriptuje je upotrebom Bobovog javnog ključa. Uspješno dekriptovanje potvrđuje da je Bob pošiljalac, zato što je poruka kriptovana Bobovim privatnim ključem koji samo on ima u svom vlasništvu.

Način prenosa sigurne i autentifikovane poruke



Sledeći algoritmi koja imaju (imali su) široku upotrebu u komercijalnim sistemima su:

- RC2 – je blok šifra koja koristi ključeve promjenljive dužine
- RC4 – je niz šifra (radi sa nizom bitova, umjesto sa blokovima bitova)
- RC5 – koristi promjenljive ključeve koje primjenjuje na promenljive blokove podataka i uključuje pomjenljive operacije
- RC6 – koristi promjenljive ključeve koje primjenjuje na promenljive blokove podataka i uključuje pomjenljive operacije

Novi kriptografski sistem – Eliptičke krive (Elliptic Curves)

- Sistem je građen na drugačijoj matematičkoj osnovi
- Ovi algoritmi koriste kraće ključeve i ispoljavaju bolje performanse za pojedine operacije
- U poređenju sa RSA, u nekim slučajevima ovi algoritmi pokazuju bolje performanse za operacije dekripcije i potpisivanja
- RSA se pokazao boljim za operacije kriptovanja i verifikacije potpisa
- Algoritam eliptičkih krivih se pokazao ograničen za komercijalnu prodornost

ELEKTRONSKI POTPIS

Ručni potpis

- potpis je autentičan
- potpis se ne može falsifikovati
- potpis nije moguće koristiti više puta
- potpisani dokument je nepromjenljiv
- potpis ne može biti negiran

Da bi se omogućilo e-business poslovanje neophodno je osiguravanje istih poslovnih procesa u elektronskom svijetu kao i u "pravom" svijetu sa ličnim potpisom

Za digitalni potpis koriste se algoritmi izvoda poruke
Message Digest Algorithms–

- Message Digest (izvod poruke) je niz fiksne dužine koji se dobija od ulaza promenljive veličine
- Jednosmjerni (one-way) algoritmi izvoda poruke se koriste za provjeru celovitosti poruke.
- Jedan smjer omogućava da se datim izvodom poruke (hash vrednost), originalna poruka ne može ponovo kreirati.

NAČIN RADA

Primjer: Kada Bob šalje poruku Ani, on izračuna izvod poruke (hash vrednost), kriptuje dobijenu vrednost svojim privatnim ključem i to dodaje originalnoj poruci.

Kada dobije poruku, Ana dekriptuje izvod poruke upotrebom Bobovog javnog ključa i dobija originalni izvod poruke.Zatim Ana izračunava izvod poruke i upoređuje je sa prethodno dobijenom vrednošću.

Uspješno poređenje uvjerava Anu o cjelovitosti poruke i pokazuje da je Bob poslao poruku

Postoji više algoritama za izračunavanje izvoda poruke:

- SHA – stndard vlade U.S
- MD2
- MD4
- MD5

} MEĐU NAJPOPULARNIJIM ALGORITMIMA

Digitalnim potpisom se osigurava pouzdani dokaz identiteta potpisnika, i dokaz postojanja podataka.

Problemi koji se javljaju:

Šifarski sistemi sa javnim ključevima, kao i sistemi za digitalni potpis mogu biti veoma spori

- Takođe, u nekim slučajevima, dužina digitalnog potpisa može biti veća ili jednaka dužini same poruke koja se potpisuje

Da bi se riješili navedeni problemi koriste se hash funkcije

- Hash funkcije se definišu na sledeći način:

$$H: M \rightarrow M \qquad H(m) = m'$$

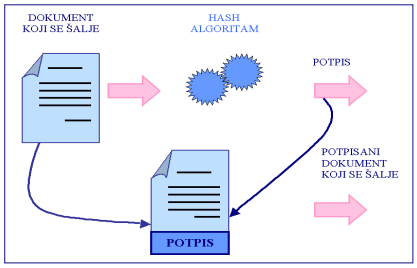
- Hash funkcija je izračunljiva funkcija koja primijenjena na poruku *m* promjenljive dužine daje njenu reprezentaciju fiksne dužine koja se naziva njenom hash vrijednošću H(*m*).

- Hash funkcija mora da bude bez kolizije (collision free) i samo u jednom smeru (one way function)
- Potpisana hash vrijednost se šalje sa nepotpisanim dokumentom

(primjer:“otisak prsta”)

Proces generisanja Digitalnog potpisa sastoji se od dva koraka:

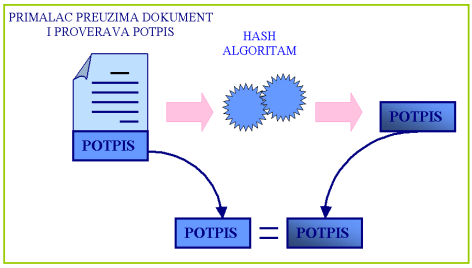
1. Generisanje HASH-a podataka ili dokumenta koji se potpisuje
2. Kriptovanje HASH-a privatnim ključem potpisnika



Da bi primalac digitalno potpisanog podatka ili dokumenta, bio u mogućnosti da provjeri Digitalni potpis, neophodan mu je pristup javnom ključu pošiljaoca, odnosno potpisnika

- Proces verifikacije se odvija u sledećim koracima:
  1. Digitalni potpis se dekriptuje pomoću javnog ključa pošiljaoca što kao rezultat daje hash funkciju H_1
  2. Na poslatim podacima korisnik primenjuje istu hash funkciju koju je primenio pošiljalac i izračunava sada hash funkciju H_2
  3. Ukoliko je $H_1 = H_2$ to znači da je pošiljalac stvarni potpisnik podataka ili dokumenta, kao i da podaci ili dokument nisu izmijenjeni tokom procesa komunikacije.

Proces verifikacije digitalnog procesa



Digitalni potpisi - rezime

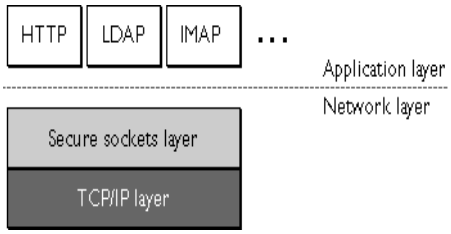
- zasnovani na asimetričnoj kriptografiji
- za šifriranje potpisa koristi se privatni ključ pošiljaoca poruke
- sprečavanje zloupotrebe digitalnog potpisa: u ključ se integrišu datum i vrijeme
- generiše se hash od 128 ili 160 bita koji se stavlja u poruku i šifrira javnim ključem primaoca
- primalac prvo svojim privatnim ključem dešifruje poruku, a onda primljenim ključem digitalni potpis

SECURE SOCKETS LAYER
SSL

- Upotreba SSL protokola je garancija sigurnog i pouzdanog prenosa podataka između dvije strane u komunikaciji jer su podaci kriptovani i procesiraju se certifikatima.

- SSL je razvijen od strane Netscape Communications Corporation.
- Za kriptovanje podataka SSL najčešće koristi dvije dužine ključeva: 40-bitni i 128 bitni ključ zavisno od željene zaštite i web browsera koji se koristi.

Prednost SSL protokola je što nije vezan za određeni informacioni servis (npr. WWW), već se koristi kao dodatak između pouzdanog prenosnog nivoa (TCP) i aplikacijskog nivoa (HTTP, FTP,...)



SSL protokol ima tri osnovna svojstva:

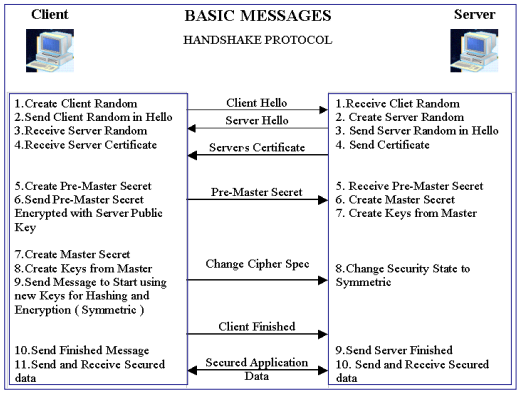
- *a)* **privatnost komunikacije** (za šifrovanje prenošenih podataka koristi se simetrična kriptografija DES, RC4 ...)
- *b)* **identitet strana u komunikaciji** (dokazuje se upotrebom asimetrične kriptografije javnog i tajnog ključa RSA, DSS ...)
- *c)* **pouzdanost prenosa podataka** (uključena je provjera integriteta podataka korišćenjem sigurnih HASH funkcija SHA, MDS ...)

Osnovni ciljevi koje SSL protokol želi da zadovolji su:

1) kriptografska sigurnost
2) interoperabilnost
3) proširivost
4) relativna delotvornost

- **Kriptografska sigurnost** postiže se upotrebom provjerenih algoritama za zaštitu podataka, ali i razvijenim protokolima za njihovu pravilnu upotrebu.
- **Interoperabilnost** garantuje komunikaciju između dvije strane (aplikacija) koje koriste različite implementacije SSL protokola (npr. između Netscape korisnika i Microsoft Web servera).
- **Proširivost** omogućuje dodavanje novih načina zaštite podataka u protokol uz istovremeno zadržavanje interoperabilnosti sa starijim verzijama protokola.
- **Relativna djelotvornost** odnosi se na opterećenje računara na kojima se SSL koristi. Kriptografski algoritmi su procesorski vrlo zahtjevni (zavisno od vrste algoritma), pa je poželjno korišćenje što jednostavnijih algoritama bez smanjenja stepena sigurnosti.

- Postupak prenosa podataka korišćenjem SSL protokola dijeli se u dva odvojena koraka:
  1. **uspostavljanje sigurne veze** (handshake)
  2. **prenos podataka**



U postupku uspostavljanja veze između strana dogovaraju se kriptografski parametri potrebni za uspješno kreiranje sigurnog komunikacijskog kanala.

Osnovni parametri koji se dogovaraju su:

- Verzija protokola (trenutna verzija protokola je 3.02)
- Kriptografski algoritmi koji će biti upotrijebljeni (koje obije strane podržavaju)
- Opciona provjera identiteta učesnika u komunikaciji (međusobna razmjena certifikata)
- Generisanje zajedničke tajne

Prenošenje podataka sastoji se od četiri koraka :

1. fragmentiranje podataka u pakete fiksne dužine
2. kompresija podataka
3. zaštita integriteta podataka
4. šifrovanje podataka

⇨ Takvi podaci prosleđuju se nižem nivou prenosa podataka (TCP), koji se brine za njihov siguran dolazak na ciljnu IP adresu i port.

- Asimetrični algoritmi koriste autentikaciju strana u komunikaciji i generisanje zajedničkih tajni i ključeva.
- Upotreba asimetričnih algoritama je minimizirana zbog njihovih velikih zahteva na procesorske resurse (tipično 100 puta sporiji od simetričnih algoritama).
- Simetrični algoritmi koriste se za šifrovanje podataka u paketima i zaštitu podataka od promjene (generisanje potpisanih sažetaka dokumenta jednosmjernim HASH funkcijama).

Sigurnost strana u komunikaciji

- Sigurnost klijentske strane
- Sigurnost serverske strane

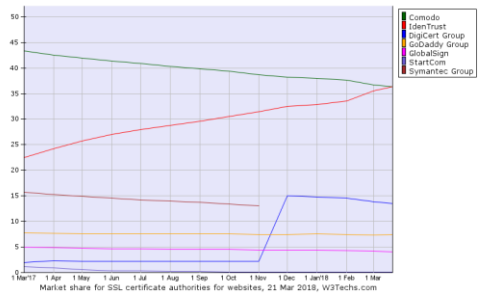
Sigurnost strana u komunikaciji

”Korišćenje kriptografije na Internetu ekvivalentno je angažovanju blindiranog auta da prenese informacije sa kreditne kartice od nekoga ko živi u kartonskoj kutiji do druge osobe koja živi na klupi u parku“

Eugene Spafford

- Sigurnost klijenske strane
  - Virusi, Fišing, farming,...
- Sigurnost bančinih sajtova i servera
  - SQL injection, XSS,...

79



	2017	2018
	1.mar	1.mar
Comodo	43.4%	36.7%
IdenTrust	22.4%	35.5%
DigiCert Group	2.0%	13.8%
GoDaddy Group	7.8%	7.4%
GlobalSign	5.0%	4.2%
Certum	0.5%	0.7%
Entrust	0.4%	0.4%
Actalis	0.1%	0.3%
Secom Trust	0.3%	0.3%
Trustwave	0.3%	0.2%
Let's Encrypt	0.1%	0.2%
StartCom	1.1%	0.1%
WISeKey Group		0.1%
Deutsche Telekom	0.1%	<0.1%
Symantec Group	15.8%	
Verizon	0.4%	

Sigurnost klijentske strane

- Fišing
- Farming
- Zlonamjerni programi
- ...

Sigurnost serverske strane

- Napad podmetanjem SQL upita (eng. *SQL injection*);
- XSS napad (eng. *Cross-site scripting*);
- CSRF napadi;
- Napad CRLF umetanjem;
- Napad promjenom direktorijuma;
- Napadi vezani za autentikaciju;
- Curenje informacija;
- Napadi vezani za prekoračenja promjenljivih;
- Napadi na sesije itd.