DBBT
Digital Broadcasting & Broadband Technologies

Co-funded by the Erasmus+ Programme of the European Union

DIGITALNI KOMUNIKACIONI SISTEMI

Vežba 8
Kriptografija

Uvod

- Bezbednost komunikacionih sistema je široka tema, ali najjednostavniji oblik bezbednosnih mera je:
  - sprečiti radoznalce da tajno čitaju poruke
  - sprečiti radoznalce da tajno menjaju poruku namenjenu drugim osobama

- Bezbednost sistema pored tehničkih aspekata pre svega podrazumeva nadmudrivanje sa inteligentnim protivnicima. Policijsko istraživanje pokazuje da većinu napada ne izvršavaju osobe izvan firme već neki od njenih razočaranih ili poniženih zaposlenih...

Uvod

- Profil osoba koje mogu izazvati bezbedonosne pretnje (*A. Tanenbaum*)

Profil	*Cilj*
Student	Da se zabavi čitajući tuđe mejlove
Haker	Da proveri nečiji bezbedonosni sistem, da ukrade podatke
Trgovački predstavnik	Da uveri kupce da predstavlja celu Evropu, a ne samo Andoru
Poslovni čovek	Da otkrije strategiju svog konkurenta
Bivši nameštenik	Da se osveti za otkaz
Računovođa	Da prisvoji novac preduzeća
Berzanski posrednik	Da porekne obećanje koje je dao
Prevarant	Da ukrade brojeve kreditnih kartica i da ih zatim proda
Špijun	Da sazna vojne i industrijske tajne neprijatelja
Terorista	Da ukrade poverljive podatke o proizvodnji biološkog oružja

Bezbednost

- Bezbednosni problemi na mreži mogu se grubo podeliti u četiri tesno povezane kategorije:
  - **tajnost** – još zvana i poverljivost, vodi računa o tome da informacije ne dospeju u ruke neovlašćenih osoba
  - **provera identiteta** – treba da utvrdite s kim razgovarate pre nego što otkrijete osetljive poruke ili preduzmete poslovne poduhvate
  - **nemogućnost poricanja** – svodi se na potpisivanje; kako dokazati da je kupac naručio deset miliona proizvoda po ceni 89 dinara ako on kasnije tvrdi da je cena 58 dinara
  - **kontrola integriteta** – kako da budete sigurni da je poruku zaista poslao kupac a ne zlonamerni konkurent koji je presreo i izmenio poruku

Uvod u kriptografiju

- Izraz kriptografija potiče iz grčkog jezika i znači *tajno pisanje*

- Kriptografija je stara gotovo koliko i čovečanstvo, bilo je mnogo različitih načina za tajno prenošenje poruka (tetovaža ispod kose, poruka na spiralnoj kori drveta, Germanikus – izviđačka šifra, Cezarova šifra...)

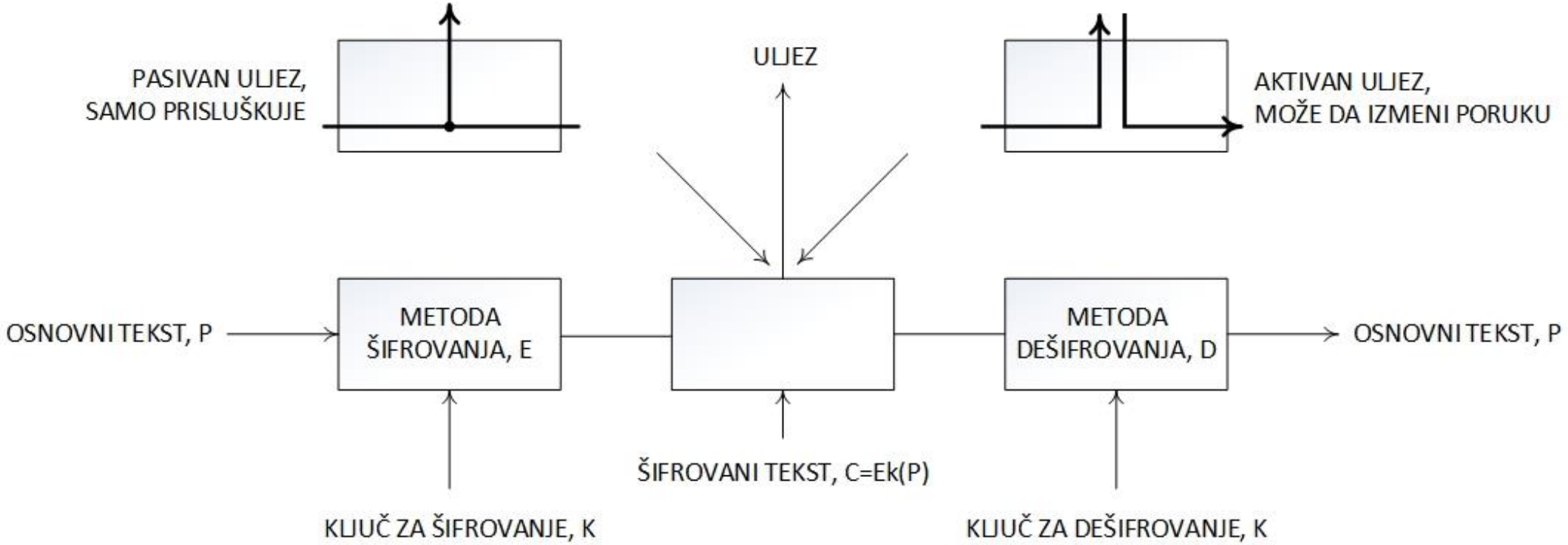
- Važno je uočiti razliku:

  - šifra (*cipher*) – omogućava zamenu znak za znak (bit za bit), bez obzira na jezičku strukturu podataka

  - kod (*code*) – jedna reč se zamenjuje drugom rečju, ili simbolom

Uvod u kriptografiju

- Kriptografski model



Uvod u kriptografiju

- Poruka koju treba šifrovati, poznata kao osnovni tekst (*plaintext*) transforimiše se pomoću funkcije čiji su parametri zadati ključem (*key*). Rezultat šifrovanja, šifrovani tekst (*chipertext*) prenosi se komunikacionim linkom.

- Pretpostavimo da neprijatelj, ili uljez (*intruder*) može da čuje i tačno zapiše ceo šifrovani tekst. Međutim, za razliku od potencijalnog primaoca, on ne zna ključ za dešifrovanje pa ne može lako da dešifruje poruku. Ako samo osluškuje komunikaciju to je pasivni uljez a ako presreće poruku, menja je i ponovo šalje, to je mnogo opasnije i to je aktivni uljez.

- Veština smišljanja šifre i algoritama naziva se kriptografija, veština razbijanja šifara naziva se kriptoanaliza; zajedno čine disciplinu koja se naziva kriptologija.

Uvod u kriptografiju

- *C=Ek(P)* – označava da je osnovni tekst, P, šifrovan ključem K i daje šifrovani tekst C
- *P=Dk(C)* – znači da je dešifrovanjem šifrovanog teksta C ponovo dobijen osnovni tekst P
- E i D su matematičke dvoparametarske funkcije, a jedan od parametara je ključ
- Kerkofov princip: Svi algoritmi moraju biti javni, samo su ključevi tajni
- Na ovom principu se zasniva kriptografija; kriptoanalitičaru su poznati algoritmi šifrovanja i dešifrovanja. Gotovo je nemoguće obezbediti da algoritam ostane u tajnosti (a kada mislite da je nešto tajna, što u stvari nije, imaćete mnogo više štete nego koristi)
- Algoritam se menja retko, a ključevi se mogu menjati koliko god je to često potrebno

Supstitucione šifre

- Kod supstitucionog šifrovanja svako slovo ili grupa slova šifruje se tako što se zamenjuju drugim slovom ili grupom slova.

- Jedna od najstarijih poznatih takvih šifara je Cezarova šifra; po toj metodi *a* postaje *D*, *b* postaje *E*, *c* postaje *F*...

napad -> QDSDG

- Umesto pomeranja slova za 3, možemo pomerati za *k* pozicija i tada je *k* ključ.

- Ovaj metod nema praktičnu primenu jer je isuviše jednostavan, statističkim metodama lako se „razbija“

Supstitucione šifre

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
Q W E R T Y I O P A S D F G H J K L Z X C V B N M

- Šifrovanje metodom zamena slova slovom gde je ključ tekstualni niz od 26 slova abecede, i sa ovim ključem je: *napad -> FQHQR*

- Ukupno ima 26! kombinacija. Kada bi svaka provera trajala 1ns, računaru bi trebalo 10 000 000 000 godina da proveri sve kombinacije.

- U praksi je period otkrivanja ključa mnogo kraći, ako kriptoanalitičar ima primer šifrovanog teksta na osnovu statistike pojavljivanja pojedinih slova (ili grupa slova). U engleskom jeziku najčešće se koristi ***e***, a zatim ***t***, ***o***, ***a***, ***n***, ***i***...

Transpozicione šifre

- Za razliku od suptstitucionog šifrovanja koje ne menja raspored već skriva slova, transpoziciono šifrovanje ne skriva slova već im menja redosled.

M	**E**	**G**	**A**	**B**	**U**	**C**	**K**
7	*4*	*5*	*1*	*2*	*8*	*3*	*6*
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

osnovni tekst:
pleasetransferonemilliondollarstomyswissbank accountsixtwotwo

šifrovani tekst:
AFLLSKSOSELAWAIATOOSSCTCLNMOMANT ESILZNTWRNNTSOWDPAEDOBUOERIRICXB

Transpozicione šifre

- Kada vidi statistiku pojavljivanja kriptoanalitičar zna da je u pitanju transpoziciona šifra.

- Sledeći korak je pogađanje broja kolona, što se uglavnom radi po parovima slova (digrafima: MO, IL...)

- Korak nakon toga je pogađanje redosleda kolona

- Najveća slabost ove metode je osobina jezika da se neki digrafi češće pojavljuju od drugih. Npr. ako se prisluškuje bankarska transakcija vrlo verovatno da će se pojaviti reč milliondollars, i na osnovu generisanih digrafa MO, IL, LL, LA, IA... može se otkriti ključ.

- U prethodnom primeru ključ je MEGABUCK, a ključ ustvari numeriše kolone: prva kolona se nalazi ispod slova najbližeg početku abacede, i tako redom...

Jednokratna zaštita

- Neprobojna šifra se ustvari može napraviti sasvim lako, tehnika je poznata decenijama.

- Najpre se za ključ izabere nasumičan niz znakova (koji ne mora biti nasumičan!). Zatim se osnovni tekst pretvori u niz bitova koristeći, npr. ASCII kodove slova. Nakon toga izvrši se isključiva disjunkcija (XOR) između dva niza bitova, bit po bit.

- Rezultujući niz ne može se provaliti jer se u dovoljno velikom uzorku svako slovo, svaki digraf ili trigraf pojavljuju približno isti broj puta.

- Ova metoda (*one-time pad*) otporna je na sve sadašnje i buduće napade, bez obzira kakvom opremom napadač raspolaže... isti osnovni tekst npr. IZADJI korišćenjem pogrešnog ključa može dati reč KNJIGA

Jednokratna zaštita

- Ova metoda je bez premca ali u praksi pokazuje mnogo nedostataka.

- Kao prvo, ključ se ne može zapamtiti, pa ga i pošiljalac i primalac moraju zapisati. Ako neprijatelj može da zarobi jednog od njih nije zgodno da pronađe šifru.

- Osim toga, ukupna količina prenetih podataka zavisi od dužine ključa.

- Najveći problem je osetljivost na ispuštene ili umetnute znakove (gubitak sinhronizacije), ako pošiljalac ili primalac izgube sinhronizaciju svi podaci od tog mesta postaju neupotrebljivi.

- Mnogo je različitih metoda kako dostaviti dovoljno dugačak ključ za metodu jedonkratne zaštite.

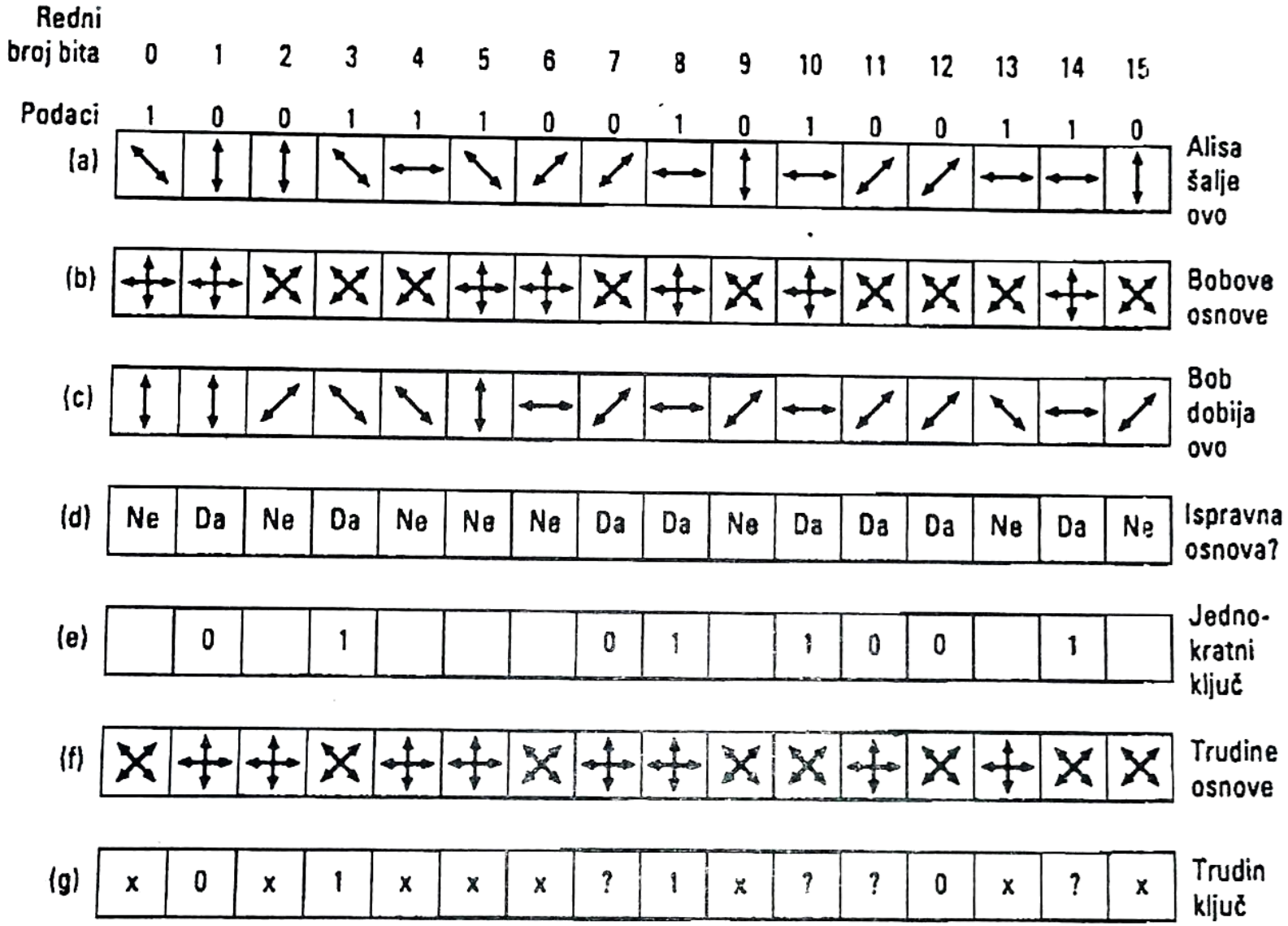
Kvantna kriptografija

- Relativno mlada oblast i relativno siguran način kriptogradije bazira se na kvantnim osobinama svetlosti.

- Ako je komunikacioni kanal optički kabal, dve strane koje komuniciraju svesne su da ih neko prisluškuje ali i pored toga mogu da imaju relativno sigurnu komunikaciju.

- Svetlost se prostire u obliku malih paketa – fotona, koji imaju neobična svojstva a najvažnije je da se ne mogu skladištiti. Propučtanjem svetlosti kroz polarizacioni filtar svetlost se polarizuje. U najjednostavnijem slučaju postoje dve osnove: pravougaona i dijagonalna

Kvantna kriptografija



Principi kriptografije

- Prvi princip kriptografije: ***Poruke moraju sadržati izvestan višak podataka***

- Primer: ako elektronska narudžbenica sadrži polje za ime kupca i 3 bajta, od čega je jedan bajt za količinu proizvoda a dva za kod proizvoda; poslednja tri bajta su šifrovana dugačkim ključem koji znaju samo kupac i proizvođač.

- Ako otpuštena radnica sa sobom ponese imena kupaca, i pošalje mnogo upita proizvođaču, statistički gledano jedan od tri trobajtna polja odgovara nekom proizvodu.

- Ako umesto poslednja 3 bajta postoje 12 bajtova, od čega 9 bajtova služi samo za zaštitu, mnogo je manja verovatnoća da će slučajnim slanjem pogoditi i zaštitne bite i kod proizvoda.

Principi kriptografije

- Drugi princip kriptografije: ***Potrebna je metoda za sprečavanje napada ponovnim slanjem poruka***

- Ovaj princip se još naziva i princip svežine, jer aktivnim slušanjem uljez može da snimi i ponovo reprodukuje stare poruke. Da bi se to sprečilo uvodi se trajanje svake poruke, npr. 10 sekundi. U tom periodu primalac sluša poruke, odbacuje duplikate i postupa po zahtevu.

- Sve poruke kojima je vremenska oznaka starija od 10 sekundi neće biti uzete u razmatranje.

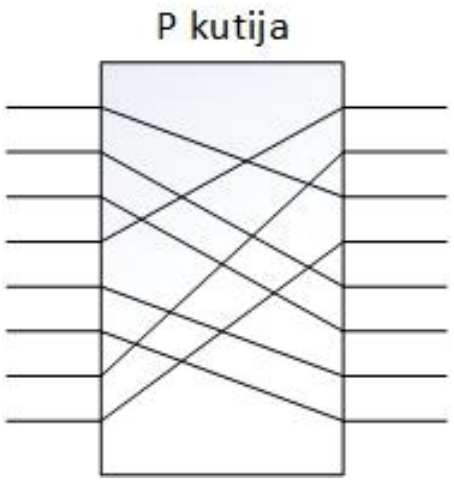
Algoritmi za šifrovanje simetričnim ključem

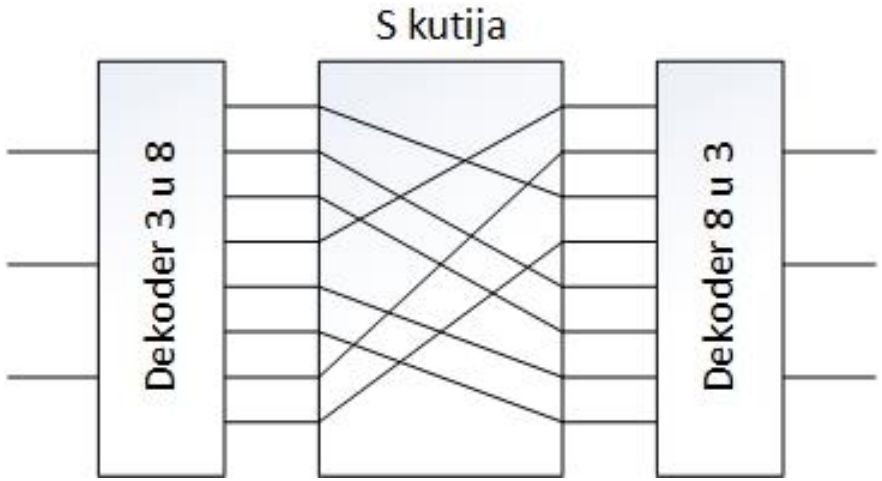
- Engleski naziv *symmetric-key algorithms*, i kod njih se koristi isti ključ za šifrovanje i za dešifrovanje. Ovde će biti reči o blok-šiframa (*block-chiper*) kod kojih se n-bitni blok osnovnog teksta pomoću ključa pretvara u n-bitni blok šifrovanog teksta

- Kriptografski blokovi se mogu realizovati hardverski (zbog brzine) ili softerski (zbog fleksibilnosti)

- U nastavku vežbe biće reči o algoritmima i protokolima ali treba imati na umu da se sklopovi za transponovanje i supstituciju mogu relativno lako izraditi od električnih kola, i to su prosta električna kola.

Algoritmi za šifrovanje simetričnim ključem





- Na slici je prikazana P kutija (P označava permutaciju), koja transponuje 8-bitni ulazni signal u 8-bitni izlazni signal

- Supstitucija se izvodi u S kutijama. Dekoder jednu ulaznu liniju spaja sa jednom izlaznom linijom, iza dekodera je P kutija koja radi transponovanje i na izlazu S kutije je Dekoder koji jednu od ulaznih linija spaja sa jednom izlaznom linijom

Algoritmi za šifrovanje simetričnim ključem

- Pravu moć ovi elementi pokazuju kada se međusobno povežu u kombinovani uređaj za šifrovanje (*product chiper*) kao na slici:

- U prvom stupnju vrši se transponovanje 12-bitnog ulaza. Drugi stupanj je supstitucija, i teorijski S kutije bi mogle da imaju 12 ulaza, ali to znači da bi imale 4096 ukrštanja pa se umesto njih koriste jednostavnije S kutije sa 3 ulaza i 3 izlaza

- U praksi se koriste uređaji koji imaju između 64 i 256 ulaza / izlaza i imaju barem 18 stupnjeva (umesto 7 kao na slici).

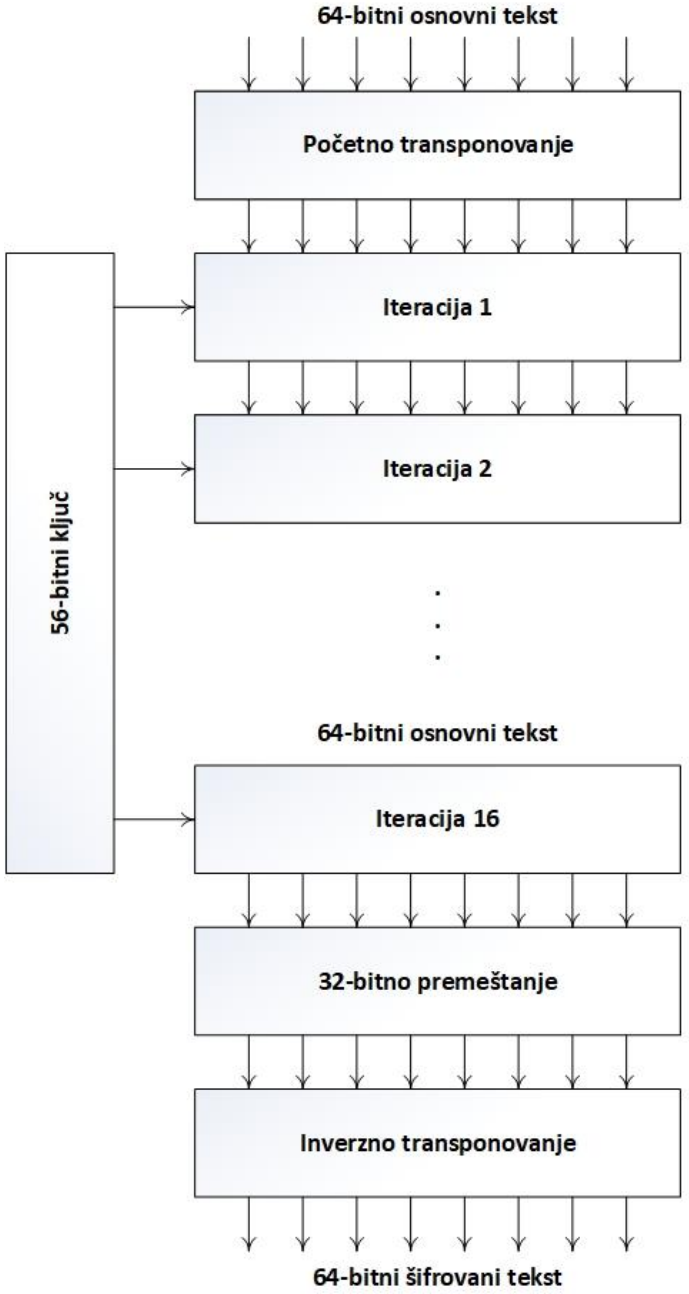
DES

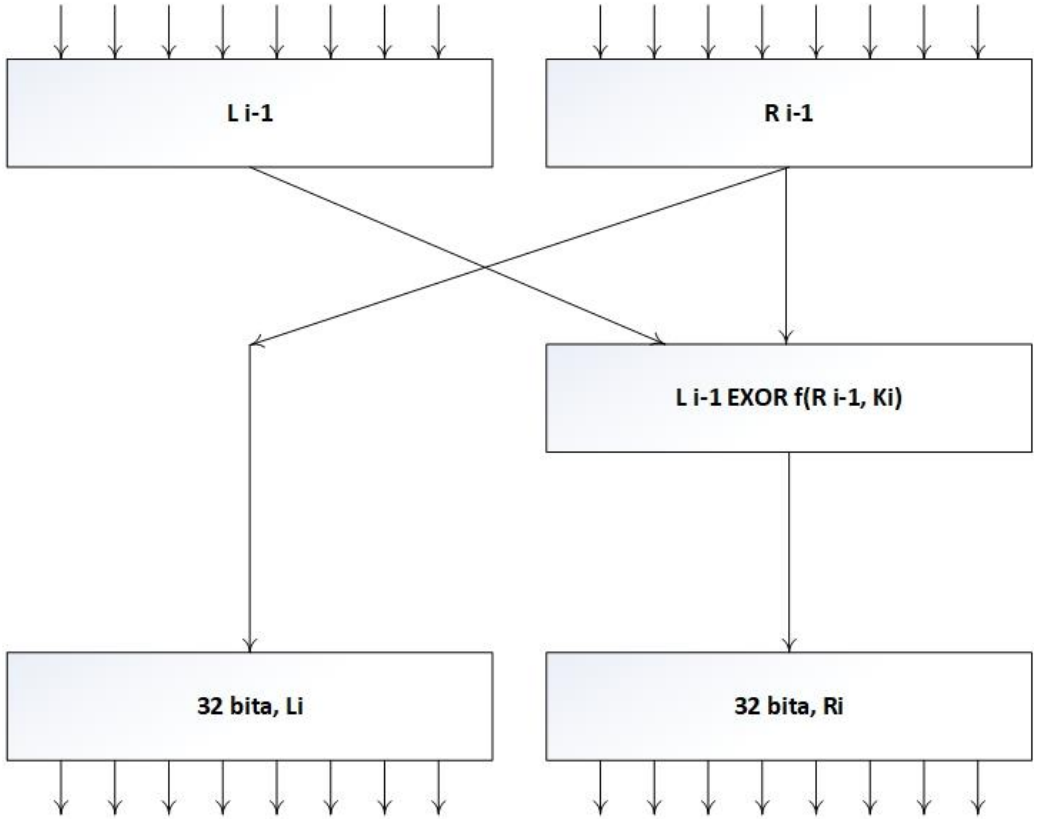
- IBM je razvio standars za šifrovanje podataka simetričnim ključem, i naziv je DES (*Data Encryption Standard*).

- Od samog nastanka ne prestaju rasprave o ovom standardu. IBM je razvio DES koji se zasniva na algoritmu Lucifer (Lucifer koristi 128-bitni ključ) dok DES koristi 56-bitni ključ. Zahtev za smanjenje ključa stigao je od američke vlade koja je preko NSA (NepoStojeća Agencija ili *National Security Agency*) „raspravio“ sa IBM-om i dogovorio da usvoje korišćenje kraćeg ključa.

- Kada je DES nastao samo NSA je imala računar (20 miliona dolara) koji je mogao da pronađe ključ, naravno NSA je sve to porekla.

DES


64-bitni osnovni tekst
Početno transponovanje
Iteracija 1
Iteracija 2
56-bitni ključ
64-bitni osnovni tekst
Iteracija 16
32-bitno premeštanje
Inverzno transponovanje
64-bitni šifrovani tekst


L i-1
R i-1
L i-1 EXOR f(R i-1, Ki)
32 bita, Li
32 bita, Ri

DES – princip rada

- Osnovni tekst se šifruje u blokovima od po 64 bita
- Ukupno ima 19 stupnjeva
- Detalj stupnjeva od 1 do 16 dat je na slici desno. Vrednost parametara u ovim stupnjevima zavisi od parametara ključa
- U jednoj iteraciji ulazna 64 bita se dele na dva dela: levi i desni. Na izlazu levi deo je kopija desnog ulaznog, a desni izlazni je je rezultat isključive disjunkcije (XOR) levog i desnog ulaznog dela i ključa za taj stupanj. Sva složenost algoritma zavisi od ove funkcije.
- Sa razvojem računaraske snage DES postaje sve više ranjiv, pa čak i njegove poboljšane varijante (trostruki DES) polako izlaze iz upotrebe

AES

- Kako je pouzdanost DES-a opdala, institucije sa američkom vladom na čelu, raspisali su konkurs. Zbog nesuglasica sa DES-om znali su da ne mogu da se mešaju i uslovi konkursa su bili:
  - 1. Algoritam mora raditi kao simetrična blok-šifra
  - 2. Ceo projekat mora biti javan
  - 3. Moraju se podržati ključevi dužine 128, 192 i 256 bitova
  - 4. Treba predvideti i softversku i hardversku realizaciju
  - 5. Algoritam mora biti javan ili se licencirati bez uslovljavanja

- Algoritam je, i pre nastanka, dobio naziv Napredni standard za šiforvanje – AES (*Advanced Encryption Standard*). Prilikom izbora prisutni su ohrabrivani da traže slabe tačke ponuđenih rešenja, i pobednički algoritam su predložili dvojica Belgijanaca i naziv je Rijndeal (čita se *rajndol*)

AES

- *Rijndeal* se zasniva na teoriji polja Galoa. Kao i DES koristi supstituisanje i broj rundi zavisi od dužine ključa (10 rundi za 128-bitni ključ, 14 rundi za 256-bitni ključ)

- Primer razbijanja grubom silom 128-bitnog AES-a: ako bi imali mašinu sa milijardu paralelnih procesora od kojih bi svaki mogao da za jednu pikosekundu proveri jedan ključ tada bi trebalo 10 000 000 000 godina da proveri sve ključeve.

- Za razliku od DES-a AES radi sa celim bajtovima kako bi bila omogućena i hardverska i softverska realizacija algoritma.

AES – princip rada

- Kod počinje tako što se ključ razvije u 11 nizova iste veličine.
- Od ključa se dobijaju ključevi za svaku rundu.
- Osnovni tekst se deli u blokove.
- U koraku 1 petlja izvršava 10 iteracija. Svaka runda se izvrši u 10 korka, i svi koraci su supstitucija.
- U koraku 2 vrši se rotiranje redova (vrsta)
- U koraku 3 se mešaju kolone po principu množenja matrica

Šifrovanje simetričnim ključem

- Pregled najčešće korišćenih šifri

Šifra	*Dužina ključa [bitovi]*	*Napomena*
Blowfish	1-448	Stara i spora
DES	56	Preslaba za današnje uslove
IDEA	128	Dobra, ali zaštićena patentom
RC4	1-2048	Neke šifre su preslabe
RC5	128-256	Dobra, ali zaštićena patentom
Rijndeal	128-256	Najbolji izbor
Serpent	128-256	Veoma otporna
Trostruki DES	168	Sledeći najbolji izbor
Twofish	128-256	Veoma otporna, često korišćena

Prenos ključeva

- Da bi komunikacija simitričnim ključevima bila funkcionalna Bob i Alisa (uobičajeni naziv za dve strane koje žele sigurnu komunikaciju) moraju razmeniti ključeve.

- Kako se vrši razmena ključeva?

- Postoje dva ključa:
  - 1. ključevi za šifrovanje podataka
  - 2. ključevi za šifrovanje ključeva

- Za razmenu ključeva koriste se mnogo jači algoritmi, a razmena ključeva za šifrovanje ključeva koristi pouzdanije metode (direktna razmena, pametne kartice, sertifikovani kurir, slanje preko više različitih kanala...)

Algoritmi za šifrovanje javnim ključem

- Istorijiski posmatrano, distribuiranje ključeva je oduvek bilo najslabija tačka kriptosistema.

- Bez obzira na snagu kriptosistema sa simetričnim ključevima, ključ se mora podeliti svim korisnicima sistema, pa tako ispada da sistemi šifrovanja pate od urođene unutrašnje slabosti.

- Objavljivanjem knjige *„The Codebreakers“* izložen je matematički aparat pogodan za opis kriptografskih sistema što je dovelo do procvata kriptografije.

- Na osnovu ove knjige, u akademskim krugovima pojavila se potpuno nova ideja, do sada nezamisliva u klasičnoj kriptografiji, a to je ideja asimetrične kriptografije.

Algoritmi za šifrovanje javnim ključem

- Istraživači Defi i Helman (*Deffie i Hellman*) predložili su kriptosisteme čiji algoritmi moraju da ispune sledeće uslove:

- 1. *D(E(P))=P* – primenom algoritma za dešiforvanje D na poruku koja je šifrovana algoritmom za šifrovanje E dobija se originalna poruka

- 2. *Tajni ključ odnosno algoritam za dešifrovanje izuzetno teško se može izvesti iz javnog ključa odnosno algoritma za šifrovanje*

- 3. *Algoritam za šifrovanje se ne može provaliti napadom zasnovanim na šifrovanju izabranog osnovnog teksta* – napadač može do mile volje da eksperimentiše sa algoritmom, to mu neće pomoći, pa nema razloga da ključ ne bude javan

Algoritmi za šifrovanje javnim ključem

- Postupak šifrovanja ide ovako:

- korisnik koji želi da primi poruku, npr. Alisa, prvo napravi dva algoritma koji ispunjavaju navedene uslove. Tada se algoritam za šifrovanje i Alisin ključ objave, npr. na web stranici ili u javno dostupnoj bazi ključeva.

- Alisin ključ, označen sa *Ea*, i pod njim podrazumevamo algoritam za šifrovanje čiji su parametri podešeni Alisinim javnim ključem.

- slično tome, sa *Da* označavamo algoritam za dešiforvanje čiji su parametri podešeni Alisinim privatnim ključem.

- Bob će uraditi isto, objaviće *Eb* a u tajnosti će sačuvati *Db*.

Algoritmi za šifrovanje javnim ključem

- Postupak uspostavljanja bezbednog kanala:

- I Alisin i Bobov ključ za šifrovanje, *Ea* i *Eb*, mogu se naći u javno dostupnim bazama.

- Alisa piše svoju prvu poruku *P*, izračunava *Eb(P)* i rezultat šalje Bobu.

- Bob ga dešifruje primenjujući na njega svoj tajni ključ *Db*, tj. izračunava *Db(Eb(P))=P*. Pritom, niko drugi ne može da pročita šifrovanu poruku *Eb(P)* zato što je sistem šifrovana tvrd orah, a *Db* se teško može izvesti iz javnog ključa *Eb*.

- Bob piše odgovor *R* i šalje Alisi *Ea(R)*.

- Alisa i Bob sada mogu da bezbedno komuniciraju.

Algoritmi za šifrovanje javnim ključem

- Za šifrovanje javnim ključem svaki korisnik mora da ima dva ključa, *javni* i *privatni*. U sistemima sa simetričnim ključevima koristi se termin *tajni* ključ.

- Matematička podloga za sisteme sa javnim ključem su tzv. jednosmerne funkcije, tj. funkcije koje se lako izračunavaju u jednom smeru dok je nalaženje inverzne funkcije veoma teško. Jedan primer je stepenovanje i logaritmovanje po modulu nekog celog broja: brojevi se pomnože na standardan način, pa se onda podele sa *n* i kao rezultat zadrži ostatak (koji je između *0* i *n-1*).

- U ovakvim matematičkim strukturama stepenovanje je relativno lako, svodi se na kvadriranje i množenje, dok je za računanje logaritma potrebno izvesti daleko veći broj elementarnih operacija.

RSA

- Metod koji zadovoljava sve navedene zahteve je RSA (*Rivest, Shamir, Adleman*) algoritam, koji su objavili istraživači Masačusetskog tehničkog instituta.

- RSA algoritam izdržava sve pokušaje provaljivanja više od 30 godina.

- Nedostatak ovog algoritma je potreba za dugačkim ključevima (barem 1024 bita, u odnosu na 128 bita koliko je potrebno za šifrovanje simetričnim ključem) i zbog toga ovaj algoritam radi prilično sporo.

- Za razumevanje principa šifrovanja javnim ključem potrebno je poznavanje principa teorije brojeva.

RSA

- Princip rada RSA algoritma:
  - 1. izaberite dva velika prosta broja, p i q (obično od po 1024 bita)
  - 2. izračunajte $n = p \times q$ i $z = (p - 1) \times (q - 1)$
  - 3. izračunajte broj koji je prost u odnosu na z i označite ga sa d
  - 4. pronađite takvo e da bude $e \times d = 1 \bmod z$
  - 5. osnovni tekst se grupiše u blokove od k bitova, gde k predstavlja najveći ceo broj za koji je ispunjen uslov da je $2^k < n$

RSA

- Princip rada RSA algoritma:
  - 6. kada želite da šifrujete poruku P, izračunajte $C=P^e (mod\ n)$
  - 7. kada želite da dešifrujete C, izračunajte $P=C^d (mod\ n)$
- Za svako P u zadatom intervalu može se dokazati da su funkcije za šifrovanje i dešifrovanje međusobno inverzne.
- Za šifrovanje su potrebni *e* i *n* pa prema tome javni ključ sadrži par (*e, n*) a za dešifrovanje su potrebni *d* i *n* pa privatni ključ sadrži par (*d, n*)

RSA

- Bezbednost metode se zasniva na problemima vezanim za razlaganje velikih brojeva na činioce. Kada bi kriptoanalitičar mogao (javno) *n* da razloži na činioce, došao bi do *p* i *q*, a odatle bi izračunao *z.* Kada ima *e* i *z*, do *d* će doći primenom Euklidovog algoritma. Na sreću, matematičari već preko 300 godina razlažu velike brojeve na činioce bez velikog uspeha jer je taj problem očigledno veoma težak.

- Primer: za razlaganje broja od 500 cifara na činioce primenom grube sile bilo bi potrebno 10^{25} godina, uz pretpostavku da se koristi najbrži računar i najbolji algoritam gde svaka instrukcija traje samo jednu mikrosekundu.

- Pored RSA još jedan algoritam za šifrovanje javnim ključem je algoritam „ranca“ (Merkle i Hellman), ali Rivest je uspešno razbio osnovnu verziju a Shamir pojačanu verziju algoritma...

Poređenje sistema sa simetričnim i sistema sa asimetričnim ključem

- Prednosti simetričnih sistema:
  - laka praktična implementacija, pogotovu hardverska, omogućava veoma velike brzine prenosa
  - ključevi su relativno kratki
  - sistemi se mogu kombinovati da obezbede jače šifre

- Nedostaci simetričnih sistema:
  - obe strane moraju čuvati ključ u tajnosti
  - za velike mreže potreban je ogroman broj ključeva
  - praksa nalaže promenu ključa za svaku sesiju

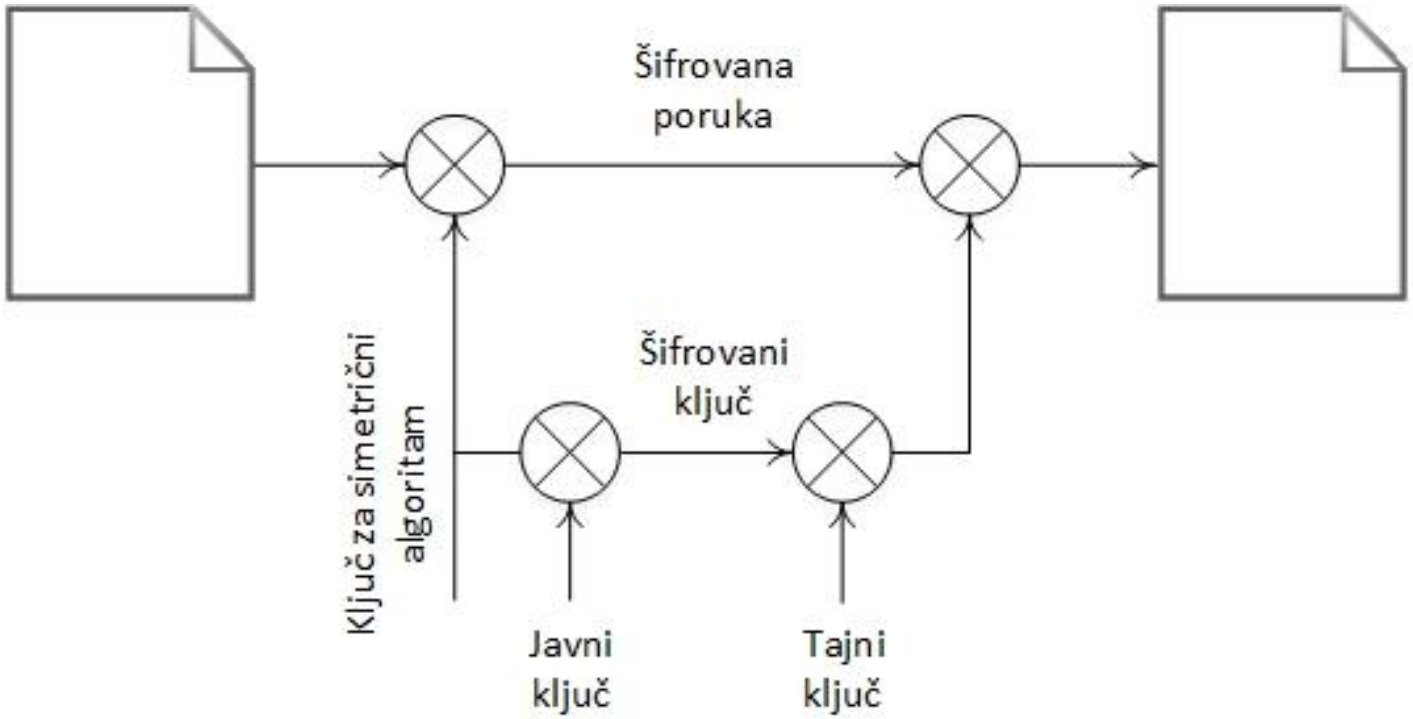
Poređenje sistema sa simetričnim i sistema sa asimetričnim ključem

- Prednosti asimetričnih sistema:
  - samo jedan deo ključa mora biti tajni
  - ključevi mogu ostati nepromenjeni duže vreme
  - u velikim mrežama broj potrebnih ključeva može biti znatno manji nego kod sismetričnih sistema

- Nedostaci asimetričnih sistema:
  - brzina rada je, zbog velikog broja operacija, za više redova veličina manja nego kod simetričnih sistema
  - veličine (dužine) ključeva su znatno veće nego kod simetričnih sistema
  - još ni za jedan ovakav sistem nije dokazano da je siguran; teškoća njihovog probijanja se zasniva na problemima za koje se pretpostavlja da su teški

Poređenje sistema sa simetričnim i sistema sa asimetričnim ključem

- Svaki od sistema ima svoje prednosti i mane; prema tome jedan od načina praktične realizacije dat je na slici (pomoću sistema sa javnim ključevima može se preneti simetrični ključ i zatim se može nastaviti komuniciranje znatno brže dogovorenim simetričnim ključem):



Pitanja