PRINCIPI MODERNIH TELEKOMUNIKACIJA

Elektrotehnički fakultet
Katedra za telekomunikacije
Beograd, 2019/2020.

IV Osnovi kriptografije

Kriptografija – osnovni pojmovi

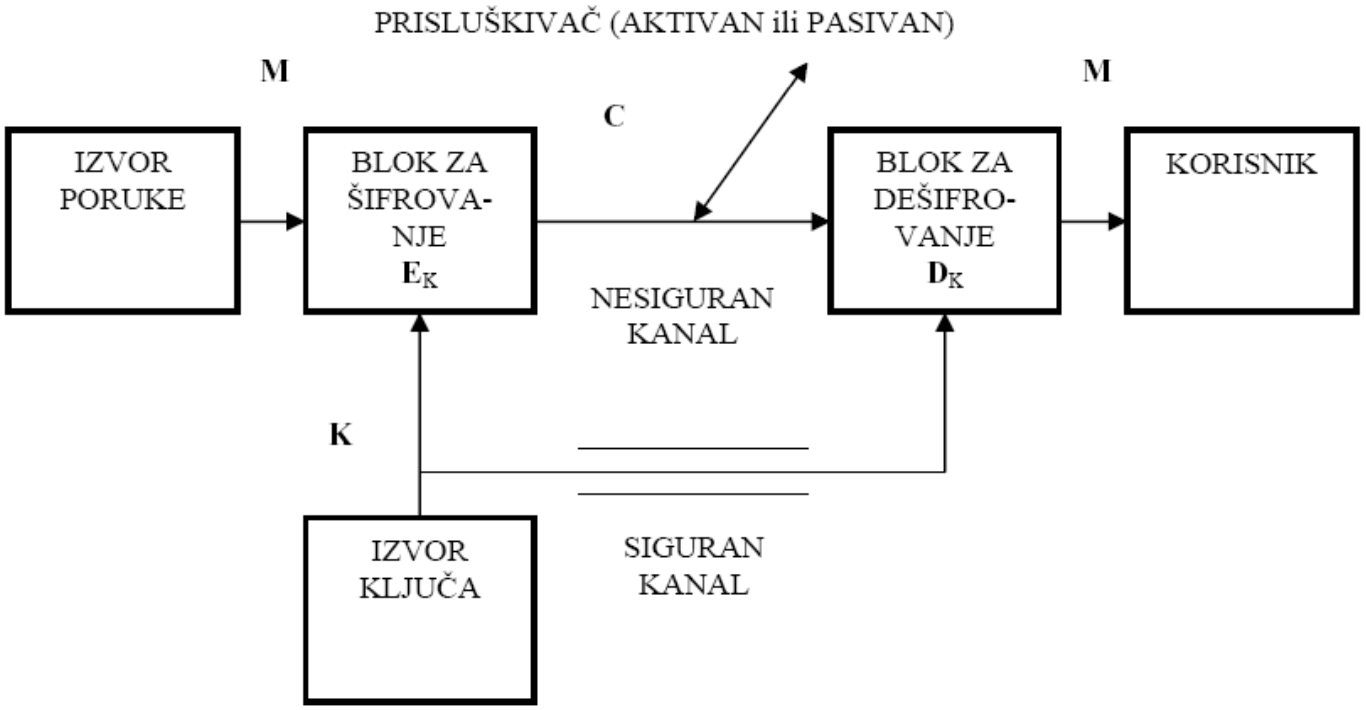
* **Kriptologija - nauka o “tajnom pisanju”.**
* **Sastoji se od**
  - *kriptografije* - nauke o konstrukciji šifara;
  - *kriptoanalize* – nauke o “razbijanju” šifara.
* **Istorijski**
  - Još u staroj Grčkoj koristile su se razne jednostavne šifre pri prenosu diplomatskih i vojnih poruka.
  - Korišćenje električnog telegrafa dovelo je u prvoj polovini XX veka do nastanka više složenih mehaničkih i elektromehaničkih uređaja za šifrovanje;
  - U toku II svetskog rata za jedne od takvih šifara konstruisan je uređaj (Enigma) koji se s današnje tačke gledišta može smatrati računarom;
  - Nakon 1950. Šenon je postavio kriptografiju na čvrstu matematičku osnovu koristeći pri tome niz pojmova iz Teorije informacija
    - tek tada je “kriptologija od umetnosti postala nauka”.

Kriptografija - ideja

* ***Šifrovanje*** **i** ***dešifrovanje*** **umesto** ***kodovanje*** **i** ***dekodovanje*****;**
  - Cilj šifrovanja je da se sadržaj poruka u kanalu što više "sakrije".
  - Zaštitno kodovanje je odbrana od šumova i smetnji u kanalu, dok je šifrovanje odbrana od prisluškivača u kanalu.
* **Osnovni zadatak - omogućiti dvema osobama komuniciranje preko nesigurnog kanala.**
  - Osoba koja šalje je pošiljalac (u kriptografskoj literaturi često Alisa);
  - Osoba kojoj je poruka namenjena je primalac (u kriptografskoj literaturi često Bob);
* **Pritom je poželjno da treća osoba, koja nadzire može kanal, ne može razumeti njihove poruke.**
  - Ova osoba presreće poruku i u literaturi se najčešće zove Eva ili Oskar
* **Poruku koju pošiljalac želi poslati primaocu je** ***otvoreni tekst*** **(***plaintext***).**
  - To može biti tekst na govornom jeziku, numerički podaci ili bilo šta drugo.
* **Pošiljalac transformiše otvoreni tekst koristeći** ***ključ*****.**
* **Taj postupak se naziva** ***šifrovanje*****, a dobijeni rezultat** ***šifrat*** **(***ciphertext***) ili** ***kriptogram*****.**

Osnovna blok šema

* **Parametri:**
  - **Skup poruka označen je sa *M*;**
  - **Skup kriptograma označen je sa *C*;**
  - **Skup ključeva označen je sa *K*;**
  - **Skup algoritama šifrovanja *E* (E_K koristi ključ $K \in K$);**
  - **Skup algoritama dešifrovanja *D* (D_K koristi ključ $K \in D$).**



Osnovni sigurnosni problemi

* **Tajnost - da li možete biti sigurni da neko nepozvan ne može pristupiti vašim podacima?**
  - treba da bude praktično neizvodljivo da se računarski sistematski određuje postupak dešifrovanja iz kriptograma, čak i ako se odgovarajuća poruka (kojoj odgovara kriptogram) zna;
  - treba da bude praktično neizvodljivo da se računarski sistematski određuje poruka iz kriptograma.
* **Autentičnost - da li možete biti sigurni da podaci koje ste primili zaista potiču od osobe od koje očekujete da vam ih je poslala (da li je neko ko pristupa vašim podacima/resursima zaista osoba kojom se predstavlja)?**
  - treba da bude praktično neizvodljivo da se računarski sistematski određuje postupak šifrovanja iz kriptograma, čak i ako se odgovarajuća poruka (kojoj odgovara kriptogram) zna;
  - treba da bude praktično neizvodljivo da se računarski sistematski generiše takav kriptogram da odgovarajući dešifrovani tekst pripada skupu poruka.
* **Integritet**
  - da li su podaci koje ste primili modifikovani od strane "trećeg" lica?

Elementarni postupci šifrovanja

- **Veoma jednostavne šifre koje se danas malo koriste u praksi.**
- **Ipak, one predstavljaju osnove ili delove nekih kompleksnijih algoritama.**
- **Dve osnovne vrste postupaka:**
  - **Blok šifre**
    - Transpozicija;
    - Šifra proste zamene (*monoalfabetska*).
    - Šifra višestruke zamene (*polialfabetska*).
  - **Niz šifre**
    - Vernamova šifra;
    - Tekući ključ (*running-key*);
    - Autoključ (*autokey*).

Transpozicija - kriptografija

* **Blok simbola poruke upisuje se po određenom pravilu u neku, obično dvodimenzionalnu, geometrijsku figuru kao što to je matrica i zatim iščitava opet po određenom pravilu.**

  - **Primer1:**

  reč **TELEKOMUNIKACIJE** se deli na blokove od po 4 slova i slova iz svakog bloka prenose u prema određenoj *permutaciji* – recimo 3-1-4-2

  TELE KOMU NIKA CIJE

  LTEE MKOU KNIA JCIE

  - **Primer2:**

  reč **TELEKOMUNIKACIJE** se upisuje po vrstama u matricu 4×4 i zatim se kolone iščitavaju po istoj permutaciji (3-1-4-2)

  T E L E

  K O M U

  N I K A

  C I J E

  LMKJ TKNC EUAE EOII

Transpozicija - kriptoanaliza

* **Ako se zna samo kriptogram a poruka nije iz govornog jezika, za veliku periodu čak ni ovako jednostavnu šifru nije lako razbiti (analogija sa *random* interliverom!).**
* **Tekst šifrovan transpozicionom šifrom može se prepoznati po tome što:**
  - statistika pojavljivanja pojedinih slova (simbola) ostaje nepromenjena.
  - uslovne verovatnoće (pojavljivanja slova posle slova) neće odgovarati statistici odgovarajućeg jezika.
* **Otkrivanje šifre se može postići anagramiranjem - dovođenjem slova u položaj koji je svojstven posmatranom jeziku.**
  - traži se takvo premeštanje slova da se pojave reči (ili delovi reči) karakteristične za dati jezik.
  - za engleski jezik su karakteristične kombinacije "*th*", "*he*", "*the*" i sl. Na taj način se može odrediti period permutacije, kao i odgovarajući redosled slova u njoj.
  - Zbog ovoga su izuzetno važne statistike pojavljivanja višeslovnih kombinacija (digrami, trigrami itd.) i reči u pojedinim jezicima.

Šifra proste zamene (*monoalfabetska*)

* **Zadržava se ista azbuka, ali se jedno slovo zamenjuje drugim.**
  - Sve se može shvatiti tako da je ispisana azbuka (od A do Š) a da je ispod nje ispisana jedna od mogućih (30!) permutacija, pa se gornja slova zamenjuju donjim.
  - Svaka permutacija je jedan od mogućih ključeva (a algoritam je prosta zamena – još jedan čest naziv: *supstitucijska* šifra).

* **Šifra Julija Cezara – najprostija monoalfabetska cifra:**

	T	E	L	E	K	O	M	U	N	I	K	A	C	I	J	E
	21	6	12	6	11	17	13	23	14	9	11	0	26	9	10	6
+	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
=	24	9	15	9	14	20	16	26	17	12	14	3	29	12	13	9
	F	I	N	I	M	S	O	C	P	L	M	G	Š	L	LJ	I

drugi način (posmatrajući samo slova):

	T	E	L	E	K	O	M	U	N	I	K	A	C	I	J	E
+	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
=	F	I	N	I	M	S	O	C	P	L	M	G	Š	L	LJ	I

* **Sve što treba zapamtiti je slovo G - pri dešifrovanju se slovo G(=3) oduzima od kriptograma.**

Šifra proste zamene - kriptoanaliza

* **Šifre jednostruke zamene se izuzetno lako "probijaju".**
* **Za određivanje ključa dovoljna je prosta statistika pojavljivanja pojedinih slova.**
  - Digrami mogu samo još da pokažu da se ne radi o transpoziciji, već o prostoj zameni.
  - Ovde i entropije višeg reda ostaju nepromenjene, što nije slučaj kod transpozicije (potrebno je da upotrebljeni statistički podaci odgovaraju tipu teksta - statistika pojavljivanja karaktera u nekom govornom jeziku ili programu...).
* **Kolika je količina teksta (dužina kriptograma) potrebna da bi se odredilo koji je ključ upotrebljen?**
  - Za engleski jezik se pokazuje da je potrebna dužina od najmanje 25 slova da se odredi ključ.

Šifra višestruke zamene (*polialfabetska*)

* **Ovakva šifra se često zove i *Vižnerova*. Primenjuje se sukcesivno (ali obično periodično) više različitih prostih zamena.**
* **Neka je period prostih zamena k (tj. koriste se zamene $n_1, n_2, \ldots, n_k$).**
* **One se lako mogu zapamtiti ako se predstave u obliku reči.**

  - **Primer:**
    Šifrovanje reči **TELEKOMUNIKACIJE** Vižnerovom šifrom koristeći reč KLJUČ (k=4):

	T	**E**	**L**	**E**	**K**	**O**	**M**	**U**	**N**	**I**	**K**	**A**	**C**	**I**	**J**	**E**
+	**K**	**LJ**	**U**	**Č**	**K**	**LJ**	**U**	**Č**	.	.	.	.	.	.	.	.
=	**V**	**R**	**Đ**	**G**	**T**	**B**	**Ž**	**Ć**	.	.	.	.	.	.	.	.

* **Za razbijanje periodične polialfabetske šifre mora se najpre utvrditi period ponavljanja (dužina ključa).**
  - U šifrovanom tekstu traže se identični trigrami, tzv. Kasiski test iz XIX veka, ili i duži blokovi i pretpostavlja se da je dužina ključa najmanji zajednički činilac pronađenih rastojanja trigrama;

Indeks koincidencije

* **Indeks koincidencije IC (*Index of Coincidence*) omogućava procenu varijacije pojavljivanja simbola u kriptogramu.**
* **Neka je N broj simbola u kriptogramu i neka je N_i broj pojavljivanja i-tog simbola. Tada je po definiciji**

$$IC = \frac{\sum_i N_i(N_i - 1)}{N(N-1)}.$$

* **IC se može koristiti da bi se dobila približna informacija o tome da li korišćena šifra monoalfabetska, polialfabetska s manjom periodom ili polialfabetska s većom periodom.**
  - Ako je primenjena monoalfabetska šifra biće velika varijacija u statistici pojavljivanja simbola i *IC* će imati veliku vrednost. S povećanjem periode varijacije se smanjuju i vrednost *IC* se takođe smanjuje.
* **Interesantne očekivane vrednosti (za engleski tekst sa 26 slova u alfabetu, verovatnoće simbola *pi*):**
  - za periodu ravnu jedinici (prosta zamena) – 0,065;
  - za dužinu ključa 2 – 0,052;
  - za dužinu ključa 5 – 0,044;
  - za veliku dužinu – 0,038≈26·(1/26)2=1/26.

Vernamova šifra

* **Ključ može se koristiti potpuno slučajni niz slova čija je dužina jednaka dužini poruke (*Vernamova šifra*).**
* **Ako se za svaku novu poruku bira druga sekvenca kao ključ (*one-time pad*) onda se stvarno dobija izuzetna šifra.**
  - Ova šifra se teorijski ne može razbiti.
  - Ako se ima dovoljno dugo vreme na raspolaganju mogu se u principu isprobati svi mogući ključevi kojih ima m^n (gde je n dužina presretnutog kriptograma a m broj slova u korišćenom alfabetu).
  - Upotreba ovakve šifre zahteva određene memorijske resurse i ona se ne može često primenjivati.
* **Postoje dosta efikasne metode za dešifrovanje i pri korišćenju veoma dugačkih ključeva koji u sebi sadrže statističku zavisnost (recimo, tekst neke knjige).**
  - Ovakva šifra se često naziva *tekući ključ* (*running-key*).

Autoključ (*Autokey*)

* **Jedan od načina da se jednostavno generiše tekući ključ.**
* **Kreće se od prvobitnog ključa (samo njega treba zapamtiti) i zatim se umesto ključa koristi sam tekst poruke.**
* **Pri korišćenju autoključa greške pri prenosu će se prostirati, dok u drugim slučajevima utiču samo na tekući simbol ili na odgovarajući blok simbola.**

- **Primer:**

1) Šifrovati reč **TELEKOMUNIKACIJE** koristeći autoključ (KLJUČ) s porukom

T E L E K O **M U N I K A C I J E**

\+ **K LJ U Č *T E L E K O*** **. . . . . .**

= **V R Đ G V U H Š P L . . . . . .**

2) Šifrovati reč **TELEKOMUNIKACIJE** koristeći autoključ (KLJUČ) s kriptogramom

T E L E K O M U N I K A C I J E

\+ **K LJ U Č *V R Đ G LJ E*** **. . . . . .**

= ***V R Đ G LJ E*** **. . . . . .**

Šenonovi doprinosi kriptologiji

* ***Difuzija*** **i** ***konfuzija*** **su pouzdane metode za konstruisanje praktičnih sistema za šifrovanje:**
  - U okviru difuzije postojeća statistička struktura poruke se maskira u kriptogramu tako što se uticaj jednog simbola (bita) proširuje na niz simbola (bita) kriptograma.
  - U okviru konfuzije vrše takve zamene koje čine vezu poruke i kriptograma što je god moguće kompleksnijom.
  - Ovi postupci se koriste u savremenim praktičnim kriptosistemima.

* **Predložio kombinovanje kriptositema formirajući njihov *proizvod* (*product*):**
  - Dok proste zamene i transpozicije kao blok šifre ne obezbeđuju veliku tajnost, njihovim kombinovanjem se mogu dobiti dobre šifre.
  - I ovaj postupak se danas često koristi.

* **I na kraju, jedna Šenonova misao, po rečima samog Helmana, ukazala mu je put do sistema javnih ključeva:**
  - "Pitanje konstruisanja dobre šifre je u suštini pitanje nalaženja teških problema, uz određene uslove. Našu šifru možemo konstruisati na takav način da je njeno razbijanje ekvivalentno rešavanju (ili u nekom trenutku razbijanja zahteva rešavanje) nekoga problema za koji je poznato da je težak".

Algoritmi sa simetričnim ključevima

* **Isti ključ se koristi za šifrovanje i dešifrovanje dokumenta.**
* **Postupak je veoma brz i jednostavan (baziran na permutacijama i sabiranju po modulu dva).**
* **Iz šifrovanog teksta je veoma teško rekonstruisati originalnu poruku ili odrediti primenjeni ključ.**

DES (*Data Encription Standard*)

* **Američki NSB (National Bureau of Standards) je 1972. raspisao konkurs za kriptografski algoritam za zaštitu računarskih i telekomunikacionih podataka .**
* **Zahtevi:**
  - visoki stepen sigurnosti
  - potpuna specifikacija i lako razumijevanje algoritma
  - sigurnost leži u ključu, a ne u tajnosti algoritma
  - dostupnost svim korisnicima
  - prilagodljivost upotrebi u različitim primenama
  - ekonomičnost implementacije u elektonskim uređajima
  - efikasnost
  - mogućnost provere
  - mogućnost izvoza (zbog US zakona)

DES - osobine

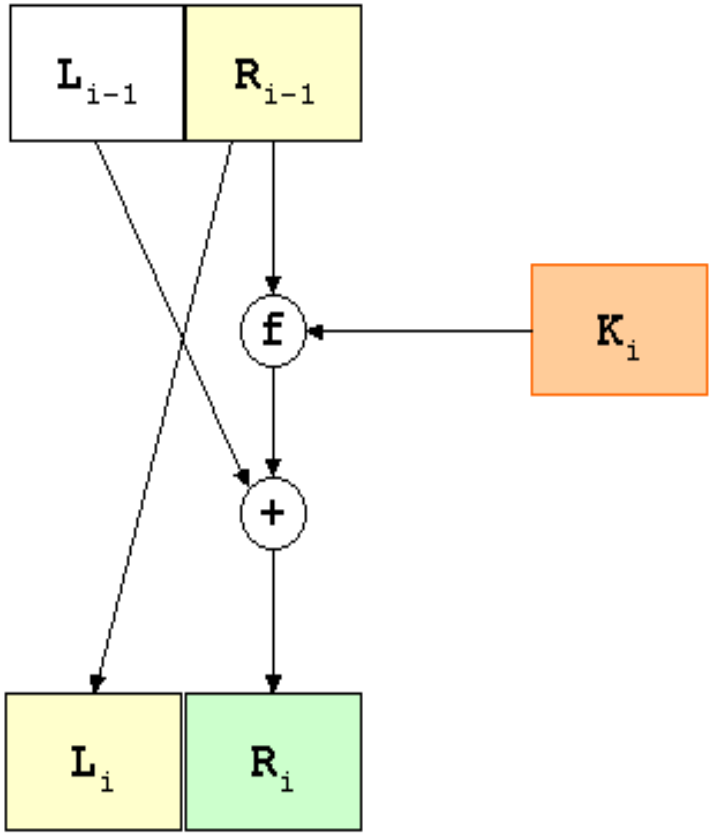
* **Stigao prelog algoritma koji je razvio IBM-ov tim kriptografa, zasnovan na tzv. *Feistelovoj šifri*.**
* **Uz modifikacije koje je predložila NSA (National Security Agency), prihvaćen je kao US standard 1976. godine**
* **Pri šifrovanju i dešifrovanju se koristi isti, 56-bitni ključ a šifrovanje se obavlja na 64-bitnom bloku podataka.**
  - sukcesivne zamene, transpozicija, brojna sabiranja po modulu 2,...
  - algoritam je složen (konfuzija) i svaki ulazni bit utiče na svaki od 64 izlazna bita (difuzija).
* **Koliko je DES siguran?**
  - Test DES algoritma: fraza ("Strong cryptography makes the world a safer place") šifrovana 56-bitnim ključem dešifrovana je (primenom brutalne sile) za 4 meseca,
  - Nije poznato da postoji drugi način za dešifrovanje ako ključevi nisu poznati (tzv. "*backdoor*" pristup).

Osnova DES algoritma

- **Dužina ključa K je fiksna i iznosi 56 bita.**
- **Algoritam se sastoji od faza.**
- **U svakoj fazi:**
  - **poruka od 64 bita deli se na dva jednaka dela;**
  - **ključ od 48 bita dobijen je**
  - **permutacijom nekih bitova iz *K*;**
  - **rezultat od 64 bita;**

$$\mathbf{L}_i = \begin{cases} \mathbf{R}_{i-1}, & i = 1,2,\cdots,15 \\ \mathbf{L}_{i-1} \oplus f(\mathbf{R}_{i-1}, \mathbf{K}_i), & i = 16 \end{cases}$$

$$\mathrm{R}_i = \begin{cases} \mathrm{L}_{i-1} \oplus f(\mathrm{R}_{i-1}, \mathrm{K}_i), & i = 1,2,\cdots,15 \\ \mathrm{R}_{15}, & i = 16 \end{cases}.$$



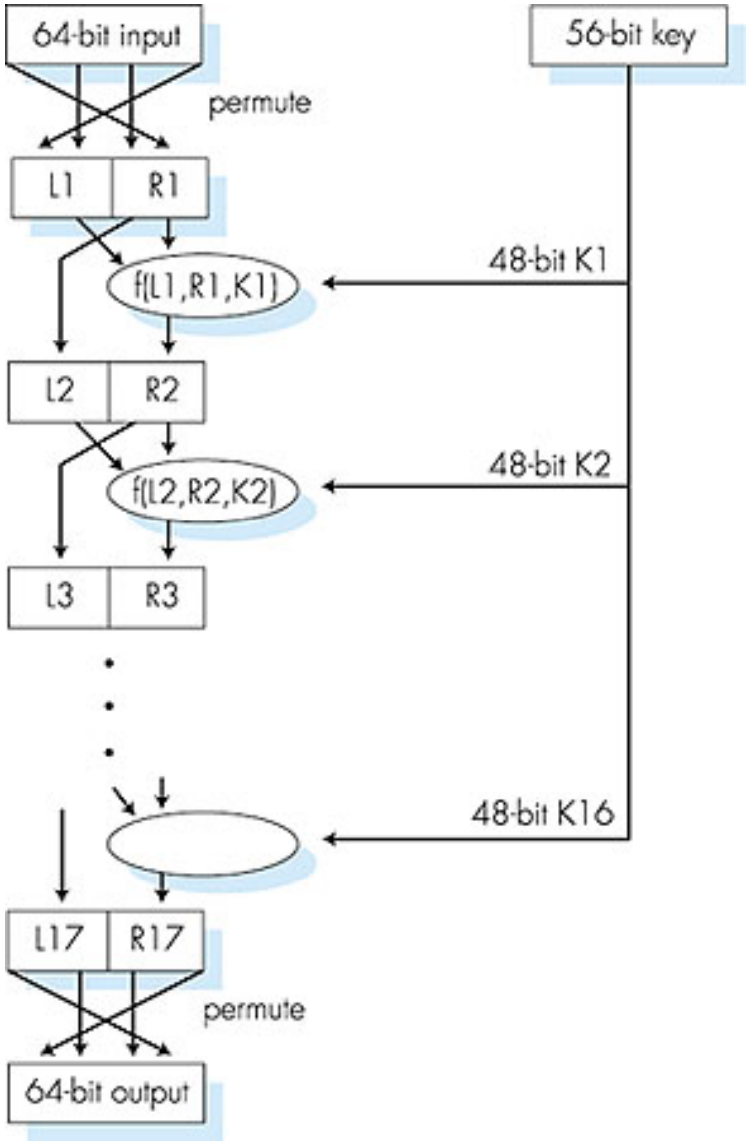
Kompletan DES algoritam

operacije u DES-u

- inicijana permutacija

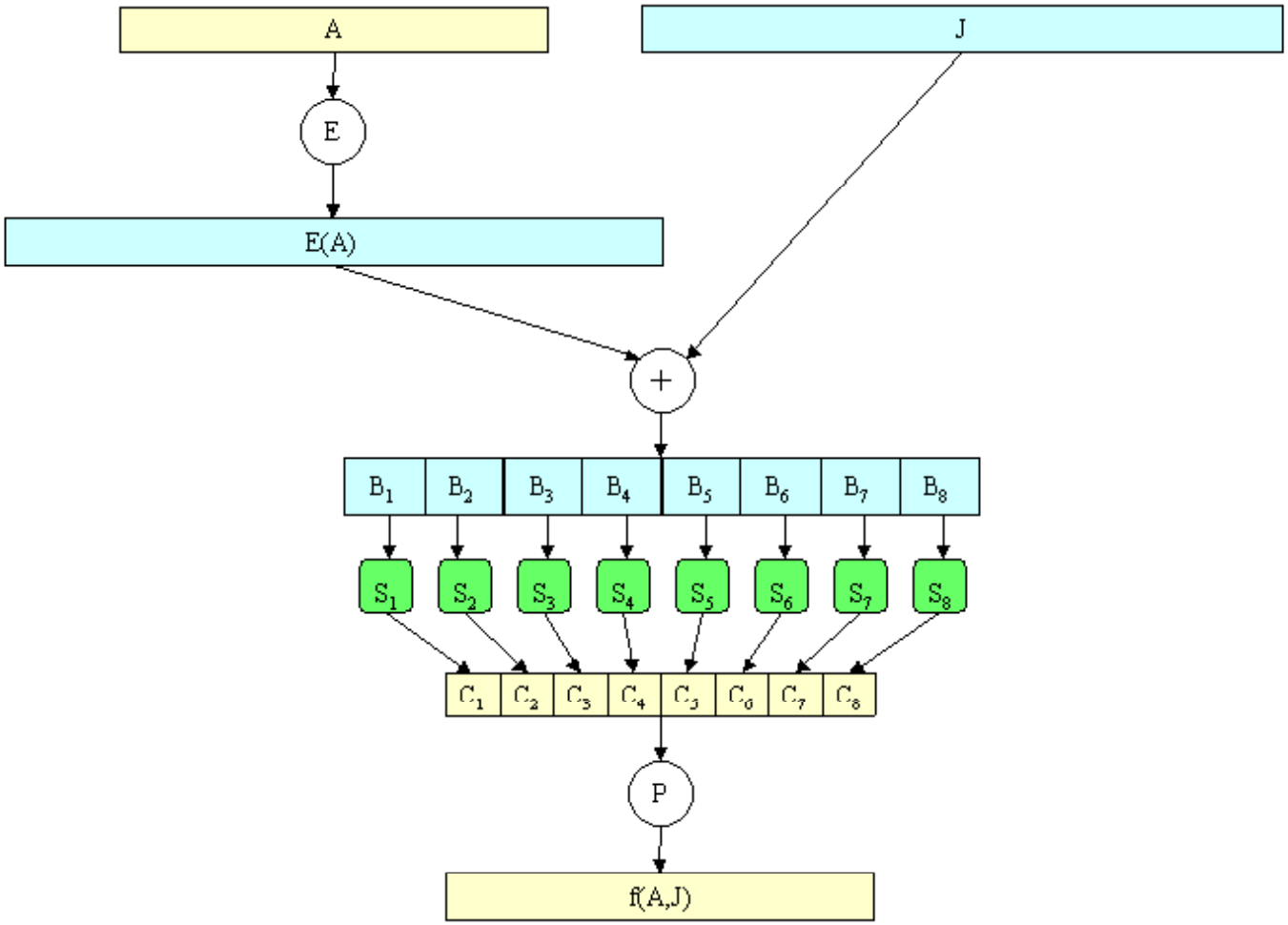
-16 puta se poziva jedna ista funkcija za različite ulazne parametre

- pritom se svaki put kao jedan od parametara koristi 48-bitni ključ izveden iz osnovnog 56-bitnog ključa



Računanje funkcije f(A,J)

* **Ulazi – A dužine 32 bita, J dužine 48 bita**



Računanje funkcije f(A,J) - objašnjenje

* **Objašnjenje prethodne slike**
  - **Prvi argument *A* se "proširi" do niza dužine 48 u skladu s fiksnom *funkcijom proširenja* E. Niz E(*A*) se sastoji od 32 bita iz *A*, permutovanih na određeni način, s tim da se 16 bitova pojavi dvaput.**
  - **Izračunamo E(*A*)+*J* i rezultat zapišemo kao niz od osam 6-bitnih blokova**

$$B = B_1B_2B_3B_4B_5B_6B_7B_8.$$

  - **U sledećem koraku koristi se 8 tzv. *S-kutija* (supstitucijskih kutija) S_1, ... , S_8.**
    - Svaki S*i* je fiksna 4 × 16 matrica čiji su elementi celi brojevi između 0 i 15.
    - Za dati niz bitova dužine 6, recimo $Bj = b_1b_2b_3b_4b_5b_6$, računa se S*j* (*Bj*) na sledeći način.
      – dva bita b_1b_6 određuju binarni zapis reda *r* od S*j* (r = 0,1,2,3),
      – četiri bita $b_2b_3b_4b_5$ određuju binarni zapis kolone *c* od S*j* (c = 0,1,2,...,15).
      – Sada je S*j* (*Bj*) po definiciji jednako S*j* (*r*,*c*), zapisano kao binarni broj dužine 4. Na ovaj način izračunamo *Cj* = S*j* (*Bj*), j = 1,2,...,8.
  - **Niz bitova C_1-C_8 dužine 32 permutuje se pomoću fiksne *završne permutacije* P. Tako se dobije P(*C*), što je po definiciji upravo *f*(*A*,*J*).**

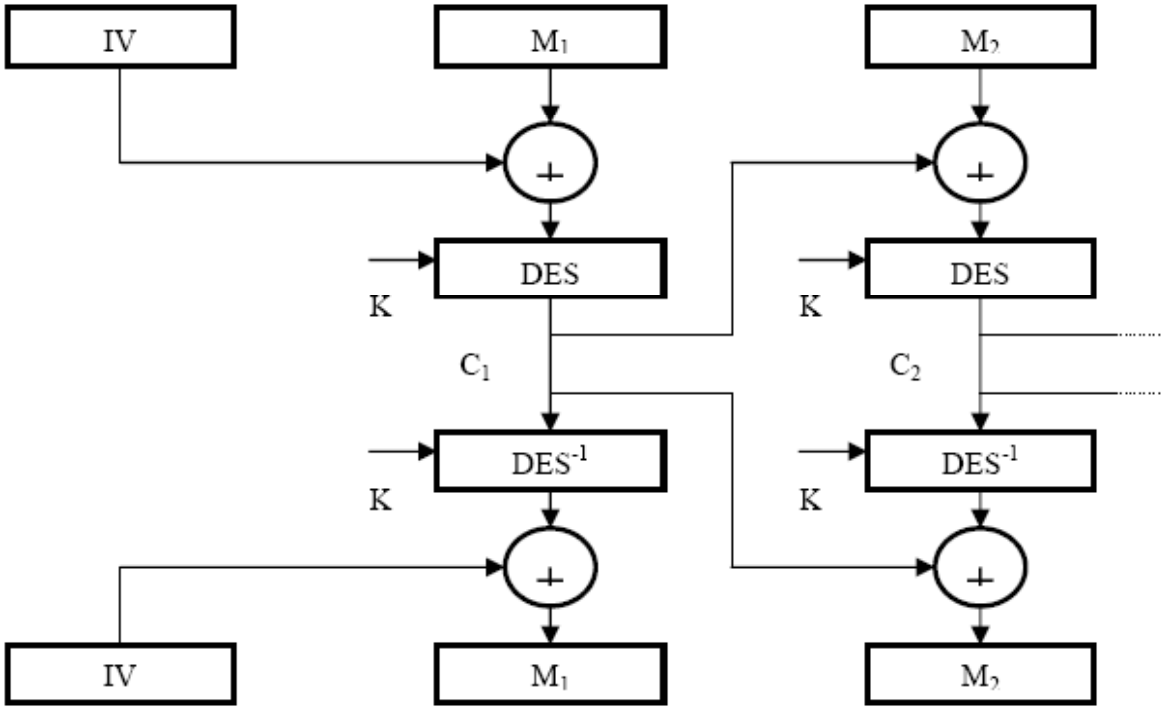
DES - kriptoanaliza

* **Originalna IBM-ova ponuda NBS-u je imala 112-bitni ključ.**
  - Prva IBM-ova realizacija Feistelove šifre – kriptosistem je imao 128-bitni ključ.
  - U verziji DES-a koja je prihvaćena kao standard duljina ključa je smanjena na 56 bitova (da bi ključ stao na tadašnje čipove, ali verovatno i pod uticajem NSA).
  - Mnogi kriptografi su bili protiv tako kratkog ključa jer su smatrali da ne pruža dovoljnu sigurnost protiv napada "grubom silom".

* **Uz 56-bitni ključ imamo $2^{56} \approx 7.2 \cdot 10^{16}$ mogućih ključeva, pa se na prvi pogled napad "grubom silom" čini sasvim nepraktičnim.**
  - Već 1977. godine Diffie i Hellman su ustvrdili da tadašnja tehnologija omogućava konstrukciju računara koji bi otkrivao ključ za jedan dan, a troškove su procenili na 20 miliona dolara.
  - Na osnovu toga su zaključili da je takav računar dostupan samo organizacijama kao što je NSA, ali da će oko 1990. godine DES postati sasvim nesiguran.
  - Godine 1993. Weiner je procenio da se za 100000 dolara može konstruirati računar koji bi otkrio ključ za 35 sati, a za 10 miliona dolara onaj koji bi otkrio ključ za 20 minuta.
  - Konačno (zvanično) razbijanje DES-a se dogodilo tek 1998. godine. Tada je Electronic Frontier Foundation (EFF) za 250000 dolara zaista napravila "DES Cracker", koji je razbijao poruke šifrirane DES-om za 56 sati.

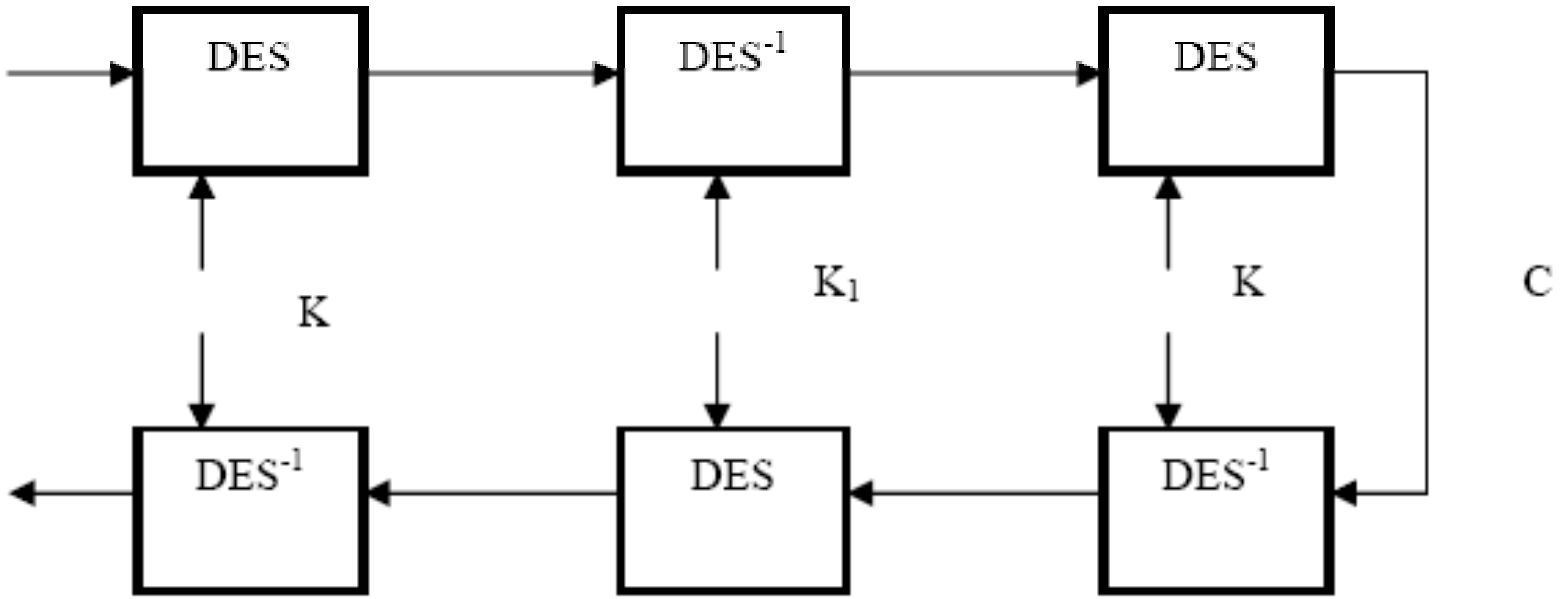
DES - *cipher-block chaining*

* **Osnovni ključ se koristi prvi put, zatim je iskorišćen princip autoključa.**
* **IV (*initialization vector*) označava početni ključ, dok su sledeći ključevi sami poslati kriptogrami.**
* **U ovome slučaju greška pri prenosu utiče na tekući i sledeći blok, ali se ne prostire dalje.**



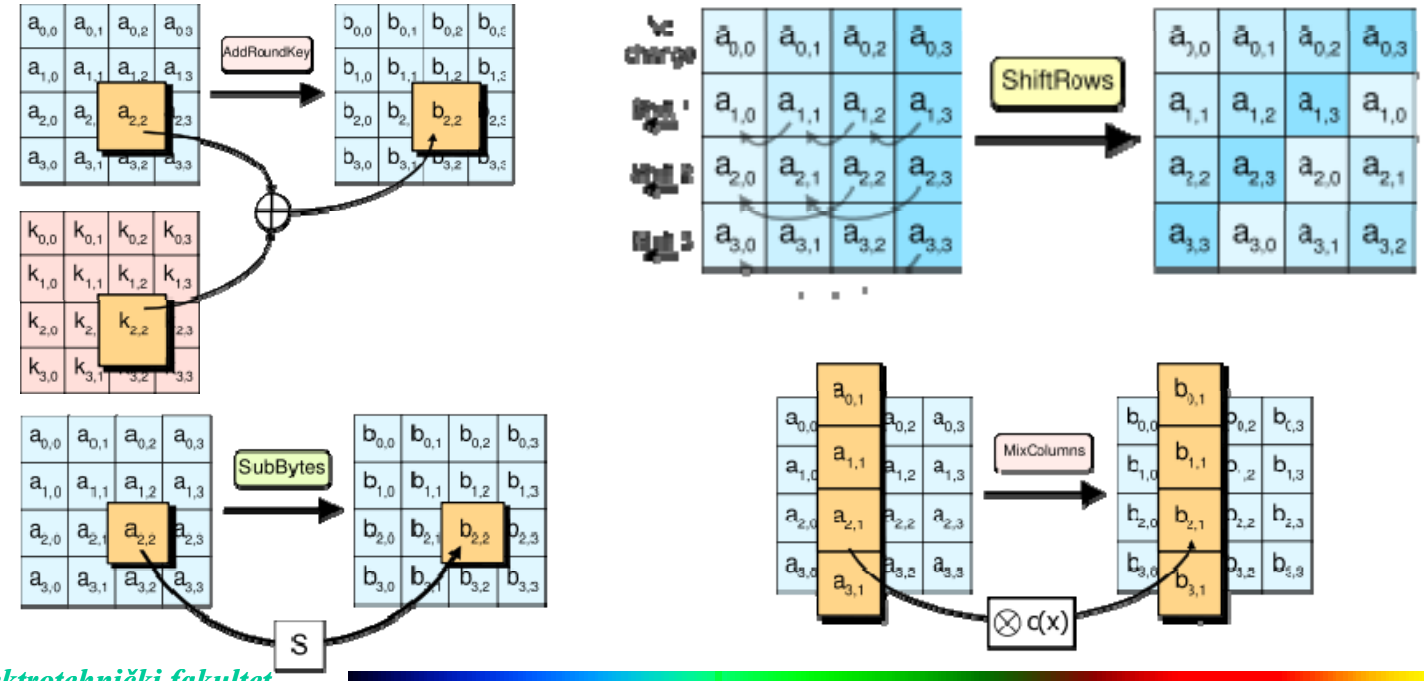
Triple DES (3DES)

* **Osobine**
  - Koristi tri ključa (sekvencijalno);
  - Dužina ključa 168 bita (u drugoj varijanti 112 bita).
  - Znatno je sigurniji od DES.



AES (*Advanced Encryption Standard*)

* **AES ili Rijndael**
  - Naslednik DES-a, standardizovan od strane NIST 2001. godine (konkurs raspisan 1997. – uslovi: simetričan, blokovski, duž. bloka i ključa);
  - Blokovi 4x4 bajta (128 bita) u 4 faze, dužina ključa 128, 192 ili 256 bita;
  - Formira se matrica ključeva, svaki je izveden iz osnovnog ključa;
  - Dodavanje ključa, nelinearna supstitucija, pomeranje, linearna transformacija.



Prednosti algoritama sa simetričnim ključevima

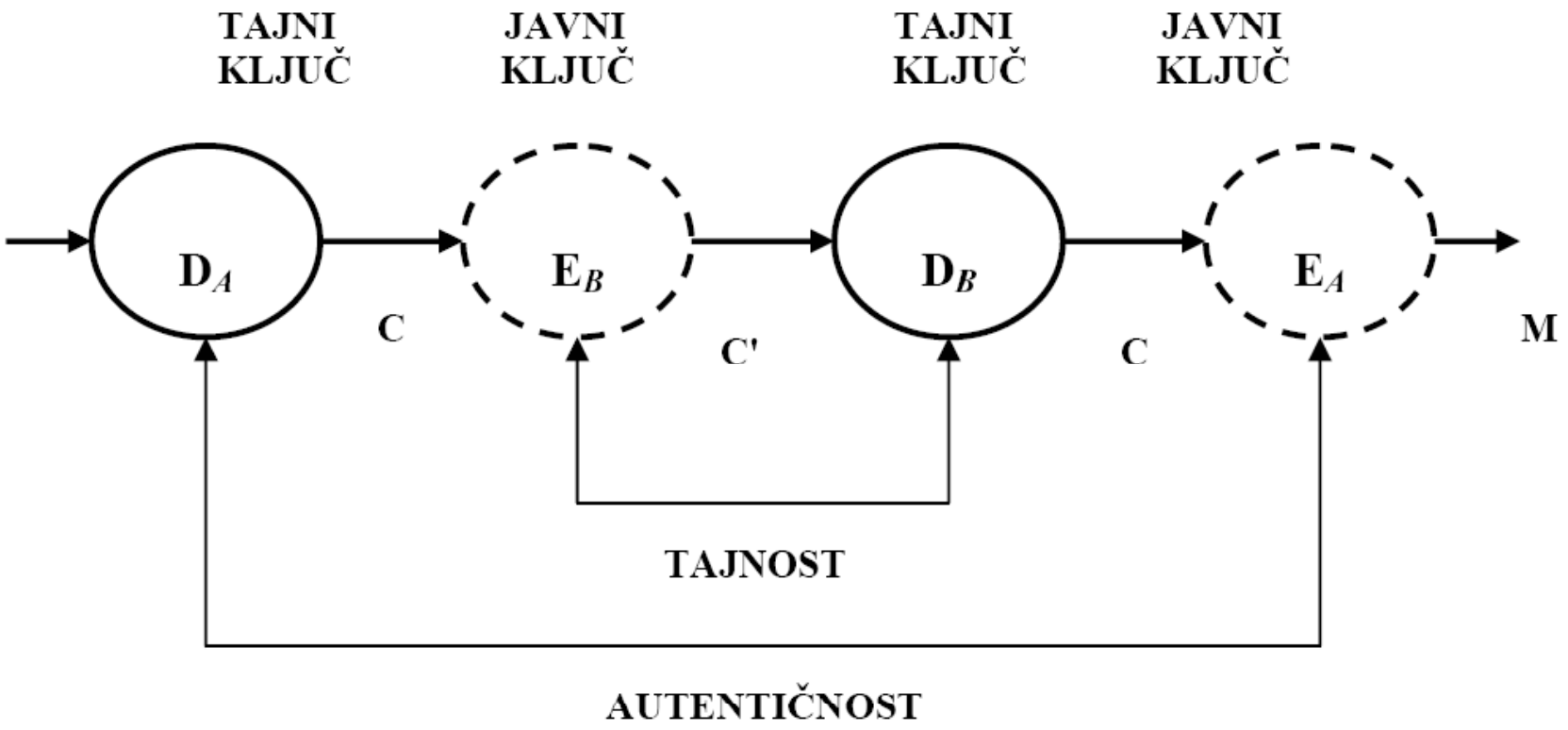
* Proces šifrovanja/dešifrovanja je veoma brz i pogodan za velike količine podataka.
* Jedini način da se dođe do šifre (ako nije poznata) je metod “grube sile”, tj. isprobavanja svih mogućih kombinacija.
* Trenutna preporuka je da šifra bude duga bar 90 bita – smatra sa da su tako podaci zaštićeni bar 20 godina.
* Jedini (ali veoma ozbiljan) problem je - kako prijemnoj strani dostaviti ključ?
* Problem presretanja šifre postaje ključan.

Algoritmi sa asimetričnim ključevima

* **Potpuno nov pristup u odnosu na DES, AES**
  - Tajni ključ nije poznat čak ni onome kome je poruka namenjena!
  - Ako se štiti tajnost javnim ključem (dostupan svima) se šifruje a tajnim dešifruje. Ako se štiti autentičnost, postupak je obrnut.
  - Nema potrebe za "sigurnim kanalom" kojim bi se dostavljao ključ onome ko treba da dešifruje dokument.

Asimetrični ključevi – tajnost i autentičnost

* **Istovremeno ostvarenje tajnosti i autentičnosti u sistemu sa javnim i tajnim ključevima:**



Algoritmi sa asimetričnim ključevima

* **Javni i tajni ključ su povezani na osnovu neke matematičke relacije**
* **Na osnovu poznatog "tajnog ključa" lako je odrediti "javni ključ". Obrnuti postupak nije jednostavan.**
* **Ovim je rešen problem distribucije ključeva a da nivo zaštite ne bude doveden u pitanje.**
* **Bitni događaji i najpoznatiji algoritmi:**
  - 1967., David Kahn *'The Codebreakers'*, podstiče razvoj kriptografije
  - 1976., Stanford, *Whitfield Diffie* i *Martin Hellman*: 'New Directions in Cryptography' - Diffie-Hellman76
  - 1977., MIT, *Ronald L. Rivest, Adi Shamir i Leonard M. Adleman*: RSA

Diffie – Helmanov algoritam

* **Godine 1976. Whitfield Diffie i Martin Hellman - u nekim grupama stepenovanje je puno jednostavnije od logaritmovanja.**
* **Pretpostavimo da se osobe A i B žele dogovoriti o jednom tajnom slučajnom elementu u cikličnoj grupi *G*, kojeg bi onda posle mogli koristi kao ključ za šifrovanje u nekom simetričnom kriptosistemu.**
  - oni taj svoj dogovor moraju provesti preko nekog nesigurnog kanala, bez da su prethodno razmenili bilo kakvu informaciju.
  - jedina informacija koju imaju jeste grupa G i njen generator g.
  - osoba A generiše slučajan prirodan broj a iz $\{1, 2, \ldots, |G| - 1\}$. Ona pošalje osobi B element g^a.
  - osoba B generiše slučajan prirodan broj b iz $\{1, 2, \ldots, |G| - 1\}$, pa pošalje osobi A element g^b.
  - osoba A izračuna $(g^b)^a = g^{ab}$.
  - osoba B izračuna $(g^b)^a = g^{ab}$.
  - sada je njihov tajni ključ $K = g^{ab}$.

RSA: formiranje javnog i tajnog ključa

1. Izabrati dva velika prosta broja p, q.
   (npr., svaki predstaviti sa po 1024 bita)

2. Izračunati $n = p \times q$, $z = (p-1) \times (q-1)$

3. Izabrati e *(pri čemu je* $e<n$*)* tako da nema zajedničkih faktora sa z (e, z su "relativno prosti").

4. Izabrati d tako da je $e \times d-1$ deljivo sa z bez ostatka
   (tj. $ed \bmod z = 1$).

5. Javni ključ (*Public key*) je tada (n,e).
   Tajni ključ (*Private* key) je (n,d).

RSA: Šifrovanje, dešifrovanje

1. Da bi se šifrovala poruka *m*, treba izračunati

$c = m^e \bmod n$ (tj. ostatak pri deljenju m^e sa n)

2. Da bi se dešifrovala sekvenca *c*, treba izračunati

$m = c^d \bmod n$ (tj. ostatak pri deljenju c^d sa n)

Ako je $p=5$, $q=7$ tada je $n=35$, $z=24$. Neka je još $e=5$ $d=29$.
(*tada su e, z* relativno prosti i *ed-1* deljivo sa *z* bez ostatka)

	m	m^e	$c = m^e \bmod n$
šifrovanje:	12	1524832	17

	c	c^d	$m = c^d \bmod n$
dešifrovanje:	17	48196857210675091509141182522307200 0	12

RSA - sposobnost zaštite

- **Ako su *p* i *q* 1024 – bitni prosti brojevi, najmoćniji računar današnjice bi faktorizaciju 2048 - bitnog broja *p*x*q* radio duže od životnog veka Zemaljske kugle,**
  - Pritom teorija još uvek ne nudi ništa više od Eratostenovog sita!
  - Time je invertovanje kriptujuće funkcije praktično onemogućeno.

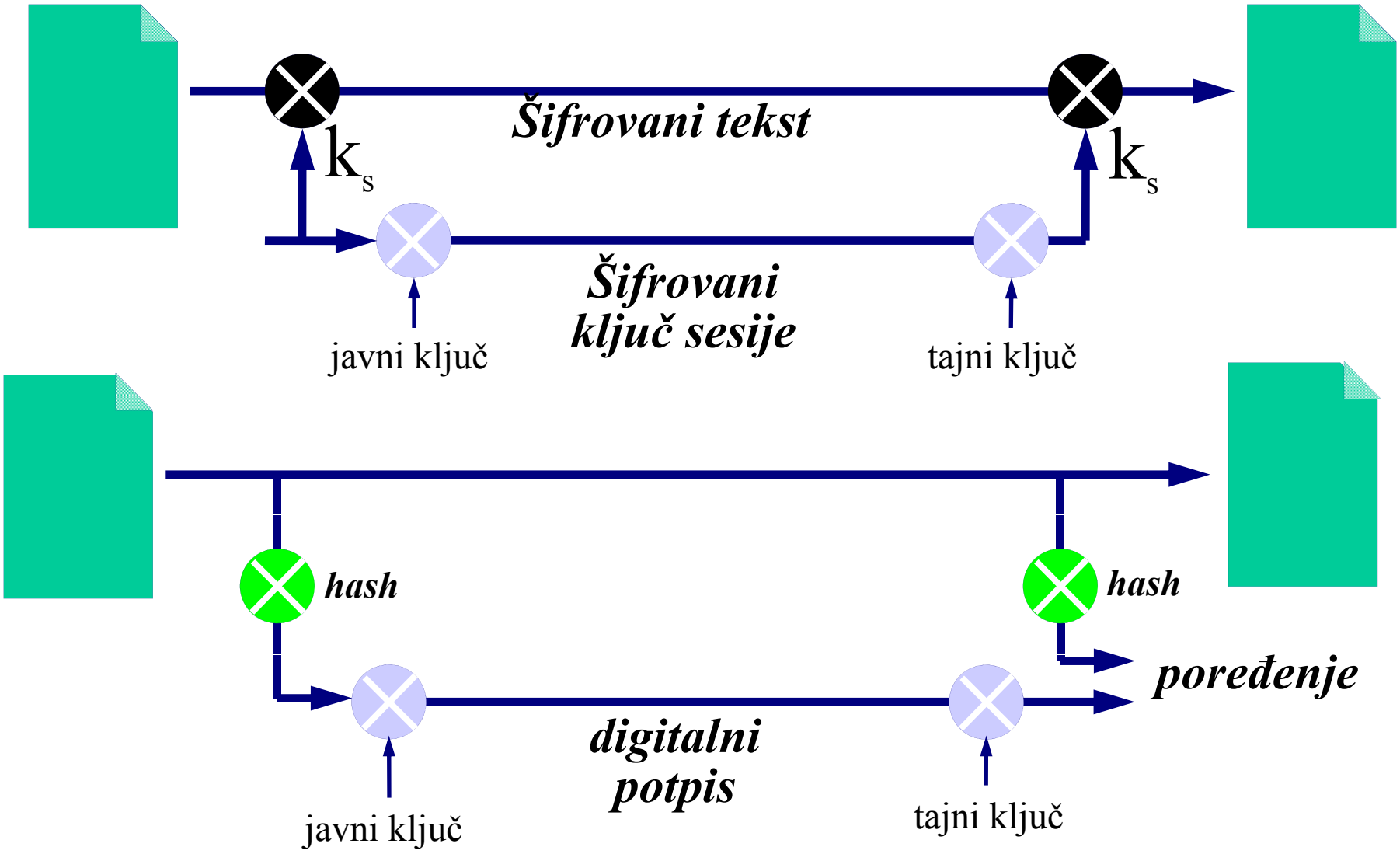
- **Ali, kako je moguće odabrati slučajni 1024 - bitni prost broj, tj. kako znati da je neki veliki broj prost? Problem nalaženja 1024 - bitnog prostog broja nije ništa lakši nego spomenuta faktorizacija! Problemi su ekvivalentni!**

Problem nalaženja velikog prostog broja

* **Ipak postoji mogućnost da se brzo proveri da li je veliki broj prost ili ne – ovu mogućnost pruža mala Fermatova teorema (*Pierre Fermat*):**
  - **Neka je *p* prost broj i *a* prirodan broj koji nije deljiv sa *p*.**
  - **Tada je broj $a^{p-1}-1$ deljiv sa *p*.**
  - ***Ron Rivest* je, ispitavši više od 700,000,000 256-bitnih brojeva, empirijski zaključio da je verovatnoća da 256-bitni broj *p* zadovoljava tvrdnju Male Fermatove teoreme za *a*=2, a da ujedno nije prost, manja od 10^{-6} !**

* **Činjenice**
  - **512-bitne šifre nisu više sigurne, 1024-bitne odolevaju napadima,**
  - **Preporučuje se korišćenje 2048-bitnih,**
  - **Preporučuje se da se fajl sa "privatnom šifrom" čuva šifrovan,**
  - **Zbog svega navedenog, nesimetrični sistemi su veoma zahtevni po pitanju procesorskog vremena.**

Kombinovanje dva pristupa
- primeri za tajnost i autentičnost -



Literatura

[1] Bruce Schneier , *Applied Cryptography*, Second Edition, John Wiley and Sons, 1996.

[2] D. Drajić, P. Ivaniš, "*Uvod u teoriju informacija sa kodovanjem*", treće izdanje, Akademska misao, Beograd, 2009.

[3] C. E. Shannon, "Communication Theory of Secrecy Systems", *Bell Syst. Tech. J.*, Vol. 28 (1949), pp. 656-715

[4] D. E. R. Denning, *Cryptography and Data Security,* Addison-Wesley Publishing Company, Reading, Massachusetts 1982.

[5] W. Diffie, M. E. Hellman, "New Directions in Cryptography", *IEEE Trans. Inform. Theory*, Vol. IT-22 (1976), pp. 644-654

[6] R. L. Rivest, A. Shamir, L. Adleman, "On Digital Signatures and Public Key Cryptosystem", *Comm. ACM*, Vol. 21 (1978), pp. 120-126

[7] David Kahn, *The Codebreakers: The Story of Secret Writing,* The New American Library, (1973; rev. ed, 1996)