Kriptografija

Kriptografija

- Potiče od grčke reči kriptos što znači tajna
- Proučava tehnike korišćene za šifrovanja i zaštitu komunikacije
- Koristi se za zaštitu sledećih bezbednosnih ciljeva:
  - Poverljivost podataka
  - Integritet podataka
  - Autentičnost
  - Uračunljivost

Primeri korišćenja kriptografije

- VPN (virtual private network)
- E-komerc
- Siguran prenos email-a
- Sigurni web sajtovi
- Sigurne sesije
- Blockchain (kriptovalute)

Šifre i ključevi

Šifre

- Predstavljaju skup pravila ili algoritam po kome se obavlja šifrovanje ili dešifrovanje neke poruke uz pomoć **ključa**
- Postoje stotine javno poznatih šifri, a ima i vlasničkih za posebne namene

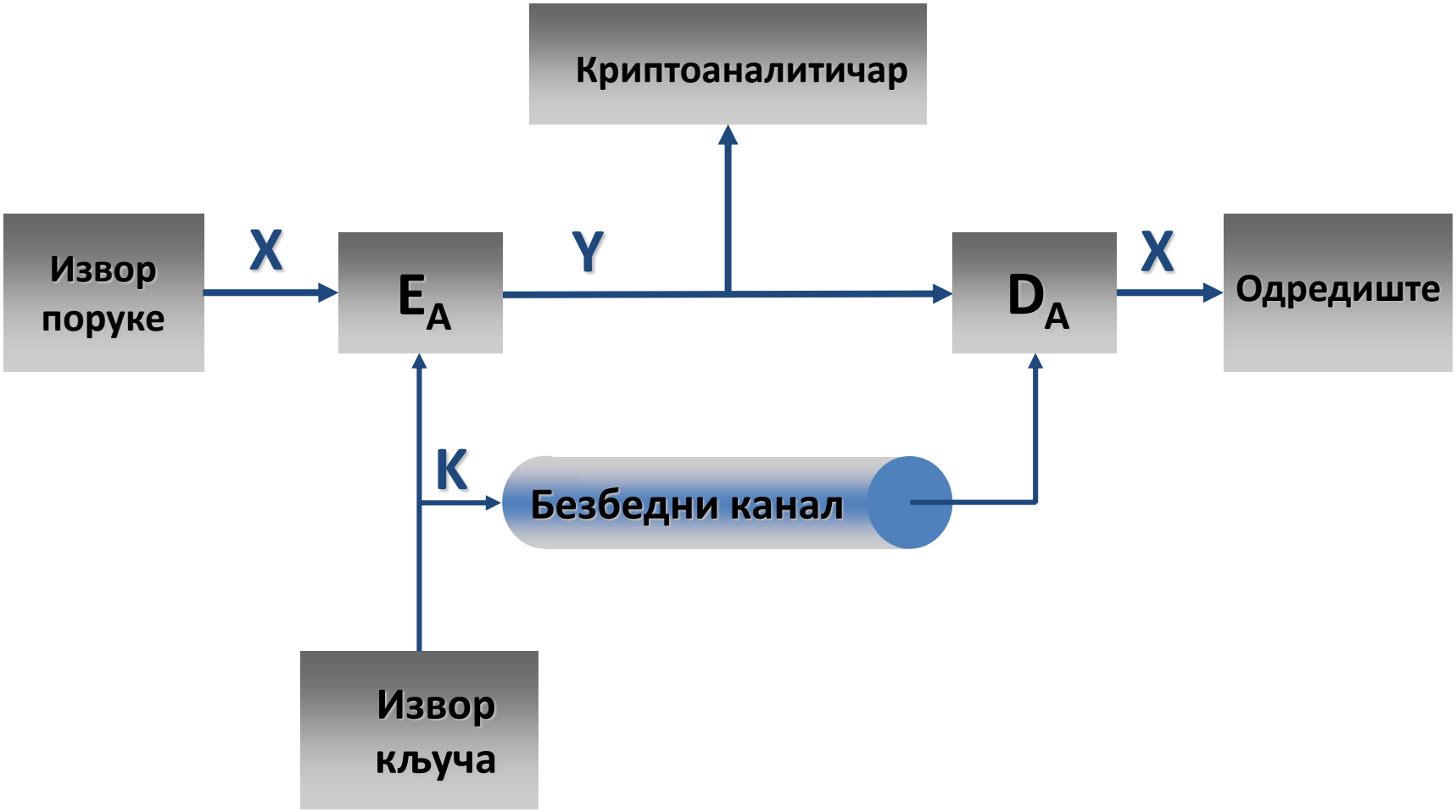
Ključevi

  - Simetrični (isti ključ se koristi i za šifrovanje i za dešifrovanje)
  - Asimetrični (koriste se različiti ključevi za šifrovanje i dešifrovanje)
- Ključevi mogu biti i jednokratni (OTP – one time pad)

Podela kriptografije

- Prema vrsti operacije koja se koristi za šifrovanje
  - Supstitucija (zamena)
  - Polialfabetik (zamena grupe slova drugom grupom)
  - Transpozicija (permutacija)
- Prema broju upotrebljenih ključeva
  - Simetričan (jedan ključ-tajni)
  - Asimetričan (dva ključa – jedan javni, jedan privatni)
- Prema načinu obrade otvorenog teksta
  - Blok šifra
  - Protočna šifra

Princip rada



Simetrični kriptosistemi

Princip simetričnog šifrovanja

Za simetrično šifrovanje neophodni su:

- Otvoreni tekst
- Algoritam šifrovanja
- Tajni ključ
- Šifrat
- Algoritam dešifrovanja

Kriptoanaliza

- Proces otkrivanja otvorenog teksta ili ključa
- Vrste napada
  - Samo šifrat
  - Poznat otvoren tekst
  - Odabran otvoreni tekst
  - Odabrani šifrat
  - Odabrani tekst

Blok šifre i protočne šifre

- Algoritmi za šifrovanje mogu obrađivati bite, bajtove ili blokove podataka
- **Blok šifre** koriste simetrični ključ i obrađuju grupe bita (blokove), generišući blokove šifrovanog teksta. Ako u poslednjem bloku nema dovoljno podataka, dodaje se tzv. peding
- **Protočne šifre** takođe koriste simetrični ključ (kao strim, npr. pseudoslučajni niz), ali obrađuju bit po bit, generišući šifrovani strim

Simetrični algoritmi

- Koriste isti tajni ključ i za šifrovanje i za dešifrovanje
- Podaci koji se prenose VPN-om šifruju se simetričnim algoritmom
- Simetrični algoritmi su mnogo brži i manje koriste procesor od asimetričnih algoritama
- Tipične dužine ključa su od 112 do 256 bita (duži ključ – veća sigurnost)
- 128 bita je minimalna dužina ključa za koju se smatra da je šifrovanje prilično pouzdano

Simetrični blokovski algoritmi šifrovanja

- DES
- 3DES
- AES
- IDEA
- RC2, RC4, RC5, RC6
- Blowfish

DES – simetrični blok algoritam

- Data Encryption Standard
- Radi sa blokovima podataka od 64 bita i ključem od 56 bita
  - Početni ključ
  - 16 podključeva
- Koristi Feistelove šifre
- Problem: distribucija tajnog ključa

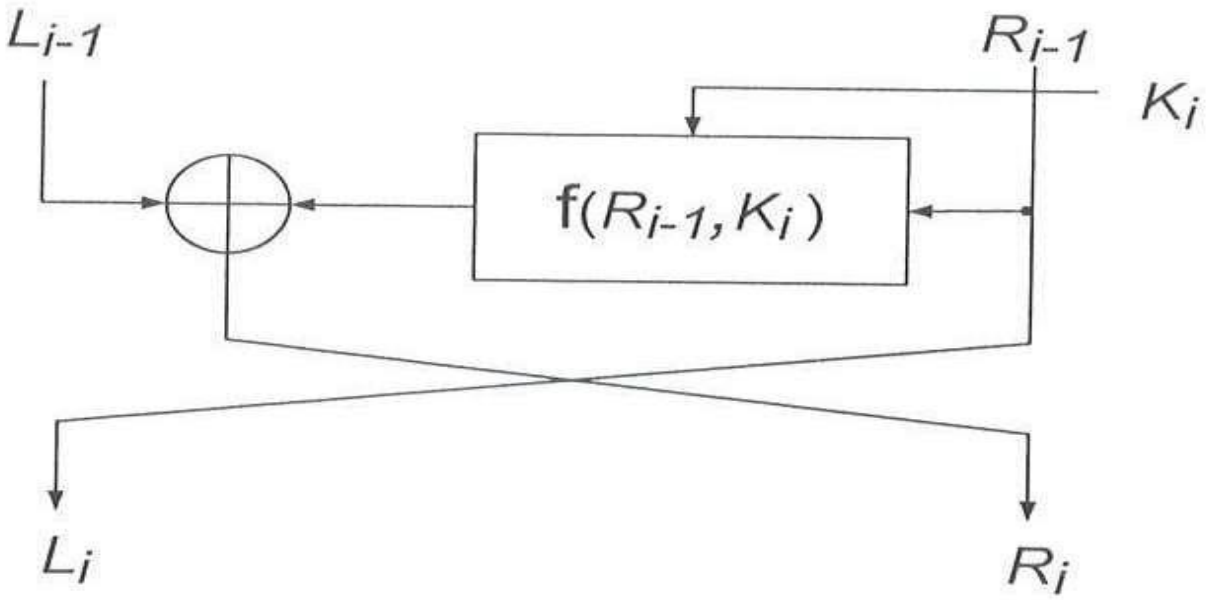
DES – šifrovanje

- Blok običnog teksta X se izloži inicijalnoj permutaciji IP
- Blok se deli na dve polovine (levi i desni blok), koje na kraju runde menjaju mesta
- U okviru jedne runde vrši se šifrovanje bloka običnog teksta pomoću jednog podključa
- Postupak se ponavlja 16 puta (ima 16 rundi) sa različitim podključevima
- Posle prolaska kroz 16 koraka ceo blok podataka se podvrgava inverznoj permutaciji i dobija se šifrovani blok podataka Y

DES – i-ti korak u šifrovanju

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f\left(R_{i-1}, K_i\right)$$

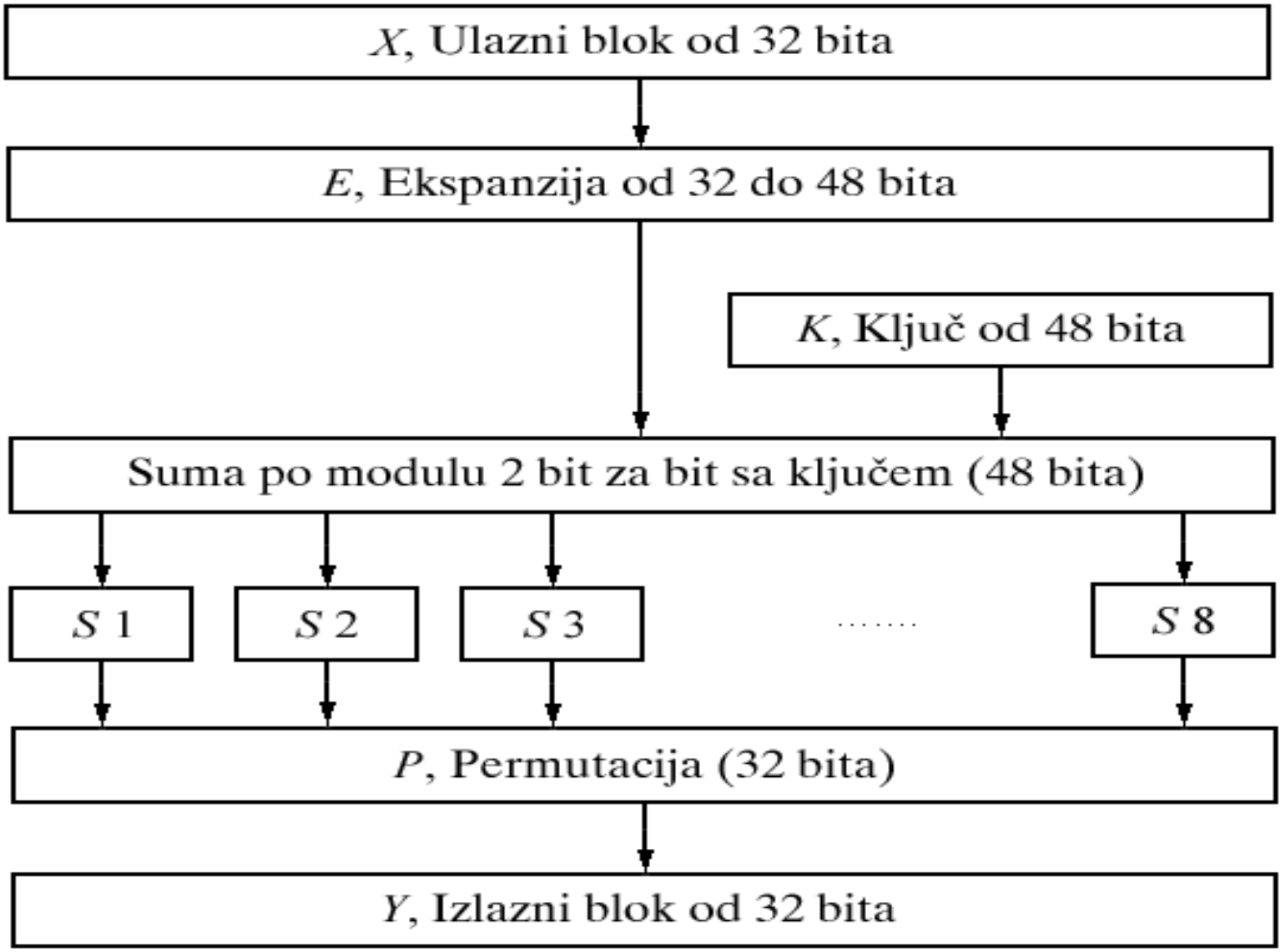


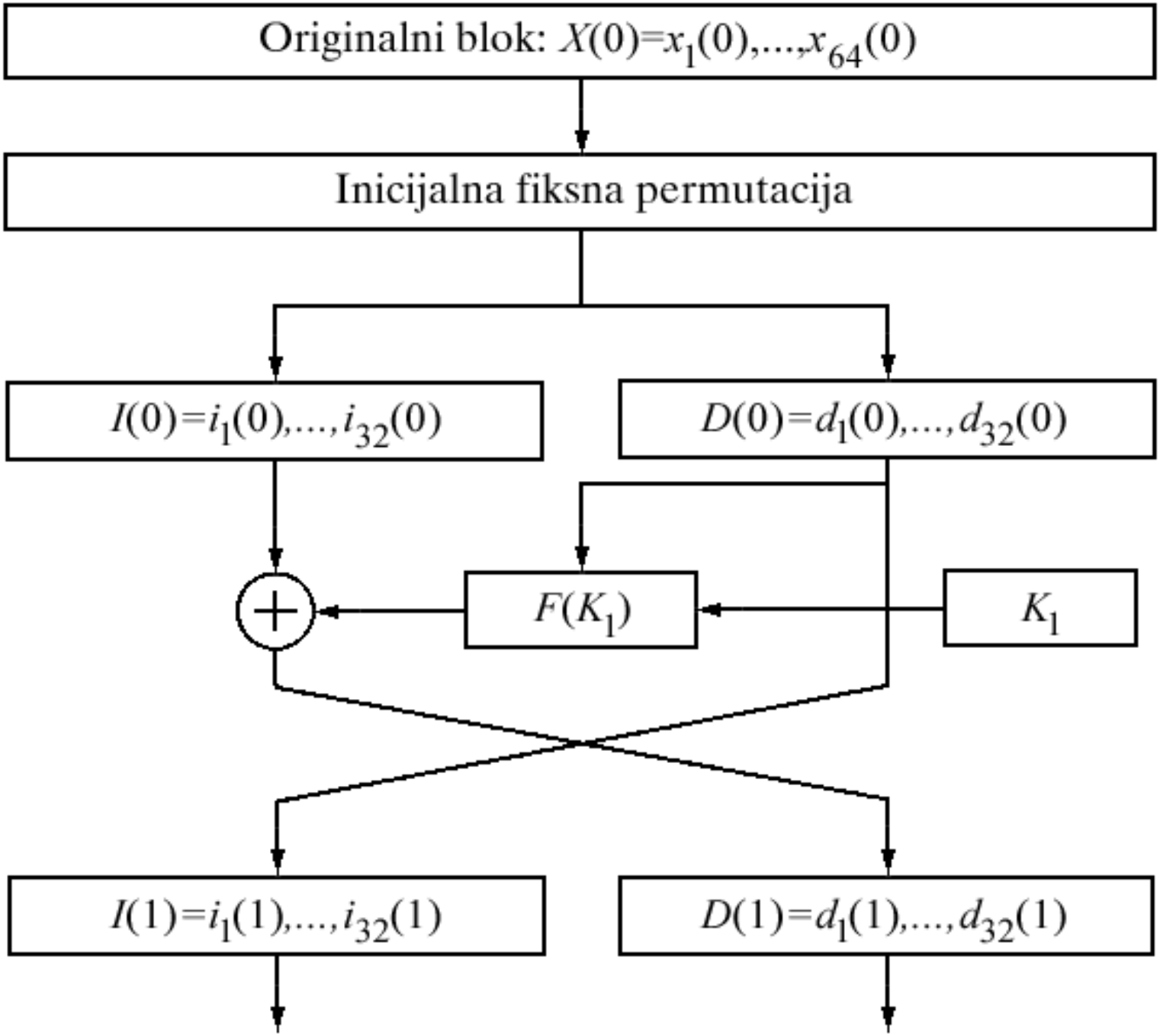
Slika 2.2 – i-ti korak u DES šifrovanju

Funkcija $F(R_{i-1}, K_i)$

- Funkcija u osnovi vrši sabiranje po modulu 2
- Pre toga radi se linearna ekspanzija niza od 32 bita na 48, koliko ima i svaki podključ
- Nakon sabiranja vrši se nelinearna kompresija na 32 bita
- Na kraju vrši se permutacija izabrana tako da difuzija bita u bloku bude maksimalna

Funkcija desne polovine niza i podključa




Originalni blok: $X(0)=x_1(0),...,x_{64}(0)$
Inicijalna fiksna permutacija
$I(0)=i_1(0),...,i_{32}(0)$
$D(0)=d_1(0),...,d_{32}(0)$
$F(K_1)$
K_1
$I(1)=i_1(1),...,i_{32}(1)$
$D(1)=d_1(1),...,d_{32}(1)$

DES - dešifrovanje

- Redosled procesiranja podključeva je obrnut
- i=16, 15, 14,….1

- $R_{i-1}=L_i$
- $L_{i-1}=R_i$ XOR $f(L_i,K_i)$

- XOR je ekskluzivno ili

	0	**0**	**1**	**1**
	0	1	0	1
XOR	0	1	1	0

Osnovne osobine DES-a

- **Međusobna zavisnost simbola –** Svaki bit šifrata je jedna složena funkcija svih bita i svih bita otvorenog teksta.
- **Promena ulaznih bita –** Promena jednog bita poruke prouzrokuje promenu približno 50% bita bloka šifrata**.**
- **Promena bita ključa –** Promena jednog bita ključa prouzrokuje promenu približno 50% bita bloka šifrata.

Nedostaci DES-a

- Slabi ključevi – Postoje četiri slaba ključa koji omogućavaju lako dekriptovanje šifrovane poruke, zato što su u slučaju upotrebe tih ključeva svi podključevi K1 do K16 međusobno jednaki.
- Postoji 28 “delimično slabih" ključeva koji omogućavaju lako dekriptovanje šifrovane poruke, zato što su u slučaju upotrebe tih ključeva samo dva ili četiri podključa međusobno različiti.
- Greška pri prenosu dela šifrata prostire se na ceo blok u kome je taj deo.

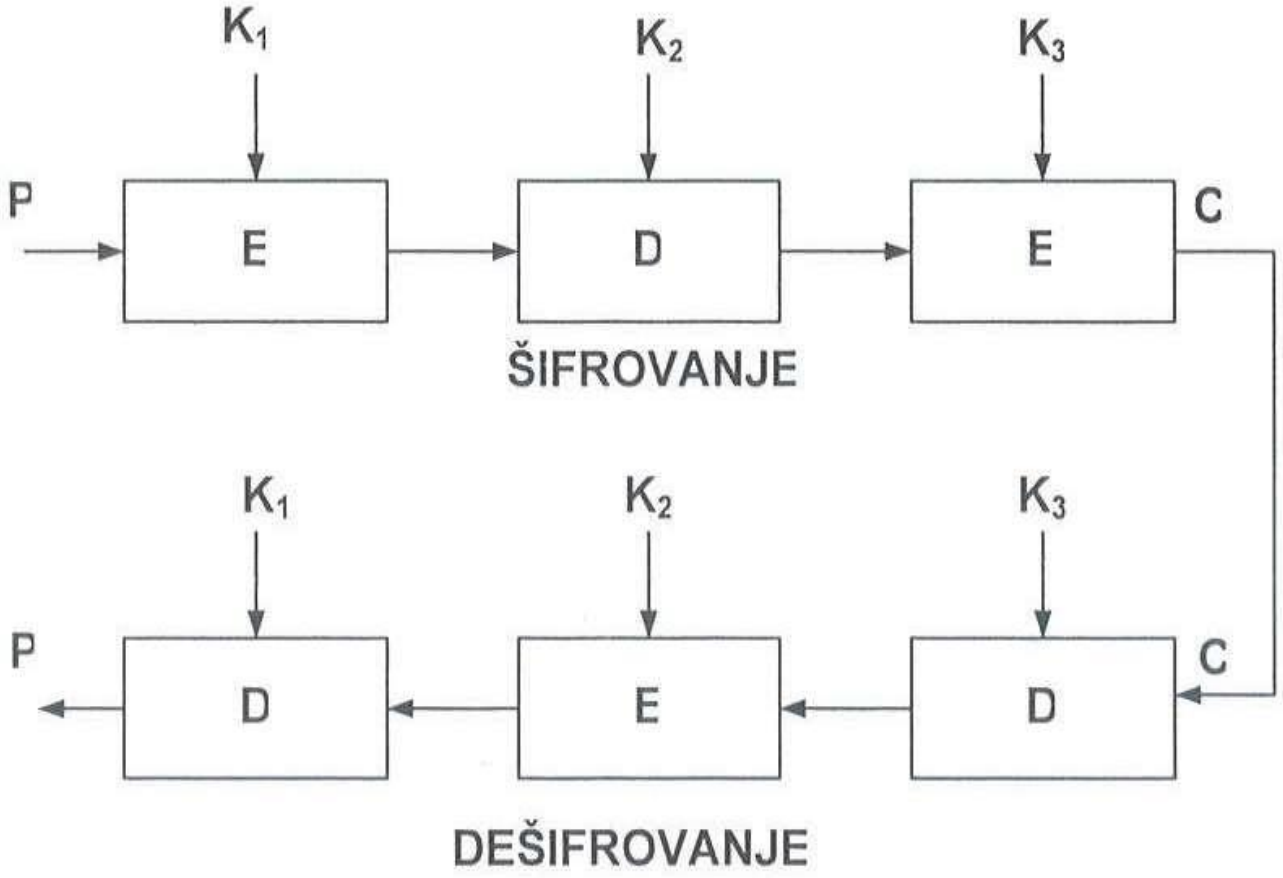
Nedostaci DES-a

- Jedan od problema pri upotrebi DES-a sastoji se u tome što je dužina ključa koji ova šifra koristi nedovoljna kada se ima u vidu današnje stanje razvoja tehnologije.
- Jasno je da ključ dužine 56 bita ne obezbeđuje dovoljan nivo bezbednosti imajući u vidu procesne mogućnosti savremenih računara i nivo integracije čipova.
- Takođe su objavljeni i specijalni napadi na blok šifre, na primer na DES, kao što su linearna i diferencijalna kriptoanaliza.

3DES algoritam

- 3DES algoritam radi sa trostrukim ključem ukupne dužine 168 bita (3 x 56 bita)
- K_1, K_2, K_3 – Tri različita početna ključa
- $C= E_{K3}[D_{K2}[E_{K1}(P)]]$ - izraz za dobijanje šifrovanog teksta C
- $P= D_{K1}[E_{K2}[D_{K1}(C)]]$ - izraz za dobijanje dešifrovanog teksta P
- Dešifrovanje u drugoj fazi 3DES šifrovanja omogućava kompatibilnost sa DES sistemima ($K_1 = K_2 = K_3 = K$)

3DES algoritam



Slika 2.4 – 3DES šifrovanje/dešifrovanje

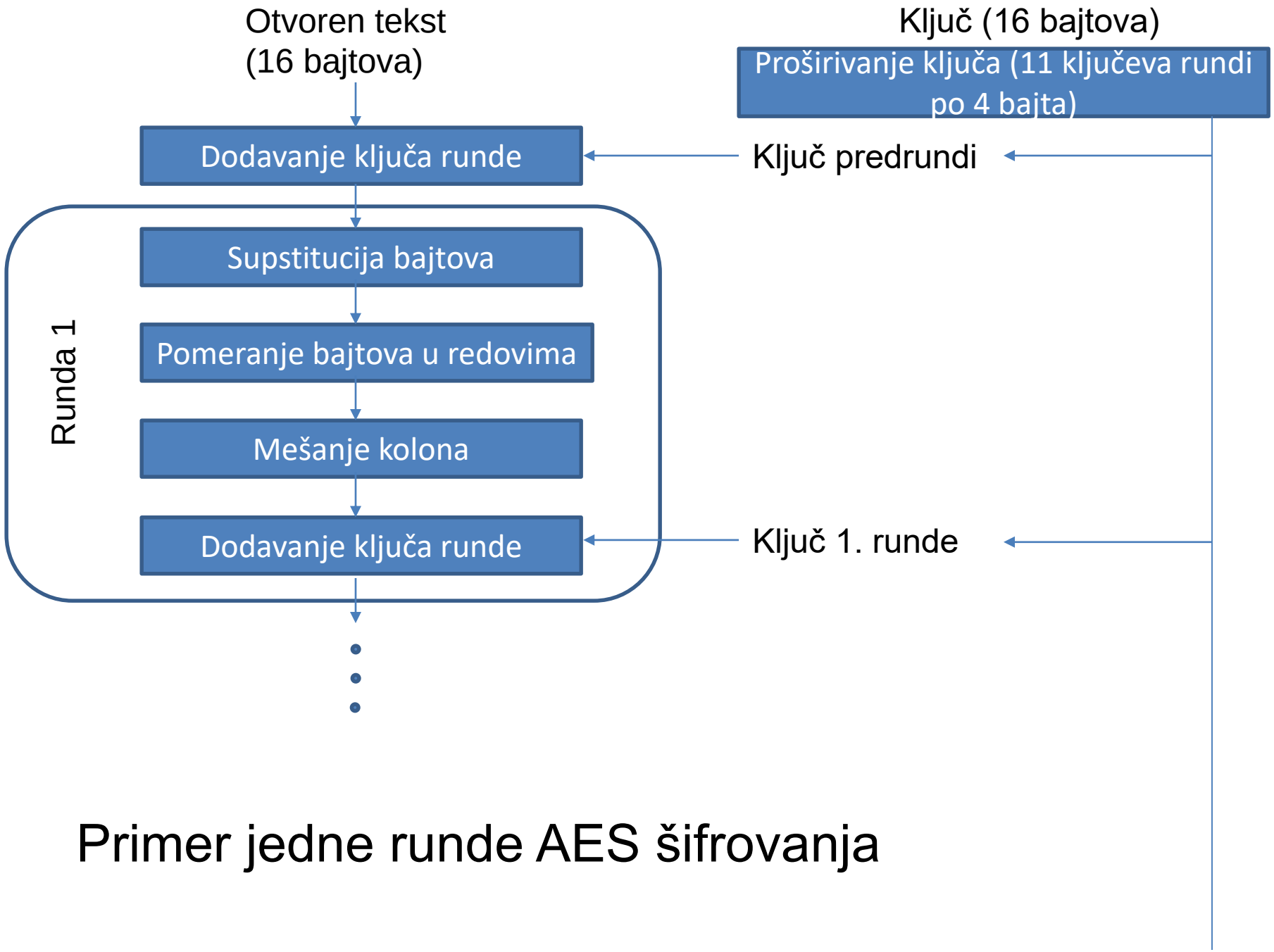
3DES - osobine

- Dužina ključa od 168 bita efektivno onemogućava napade grubom silom
- Generalno otporan na kriptoanalitičke napade
- Glavni nedostatak je tromost algoritma u softverskoj varijanti (projektovan za implementaciju hardverom i ne daje efikasan softverski kod) - 3DES tri puta sporiji od DES
- Poželjna je veća dužina bloka podataka (radi sa blokom od 64 bita) zbog efikasnosti i bezbednosti

AES (Rijndael)

- Zbog slabosti DES-a, u SAD su odlučili da ga zamene novom blok-šifrom, nazvanom AES (Advanced Encryption Standard).
- Konačna verzija algoritma AES bila je izabrana između 5 kandidata. Izabran je algoritam Rijndael (2001).

- Rijndael je iterativna blok-šifra sa dužinom bloka od 128 bita
- Dužina ključa je promenljiva i može biti 128, 192 i 256 bita.
- Osnovni element ove šifre se naziva Stanje (State). State je matrica sa 4 vrste i *Nb* kolona, gde je *Nb* jednako dužini bloka podeljenoj sa 32 (za blok od 128 bita *Nb=4*) – u svakom polju matrice je jedan bajt.
- Ključ je takođe dat matricom sa 4 vrste i *Nk* kolona, gde je *Nk* jednako dužini ključa podeljenoj sa 32.
- Broj rundi *Nr* kod ove šifre je takođe promenljiv i zavisi od vrednosti *Nb* i *Nk*. *Nr* uzima različite vrednosti u zavisnosti od dužine ključa: 128 - 10 rundi, 192 – 12 rundi i 256 – 14 rundi.



Primer jedne runde AES šifrovanja

Transformacija u okviru jedne runde sastoji se od 4 koraka

- Nelinearna supstitucija bajtova (ByteSub).
- Ciklični pomeraji u vrstama matrice State (ShiftRow).
- Množenje kolona matrice State fiksnim polinomom po modulu (MixColumn).
- Sabiranje ključa runde sa matricom State (RoundKey) - XOR.

- Slabi, kao i delimično slabi ključevi ne mogu da se pojave kod Rijndael-a, pošto algoritmi šifrovanja i dešifrovanja koriste različite komponente.
- Ova šifra je takođe otporna na linearnu i diferencijalnu kriptoanalizu, kao i na neke druge publikovane napade na blok-šifre.

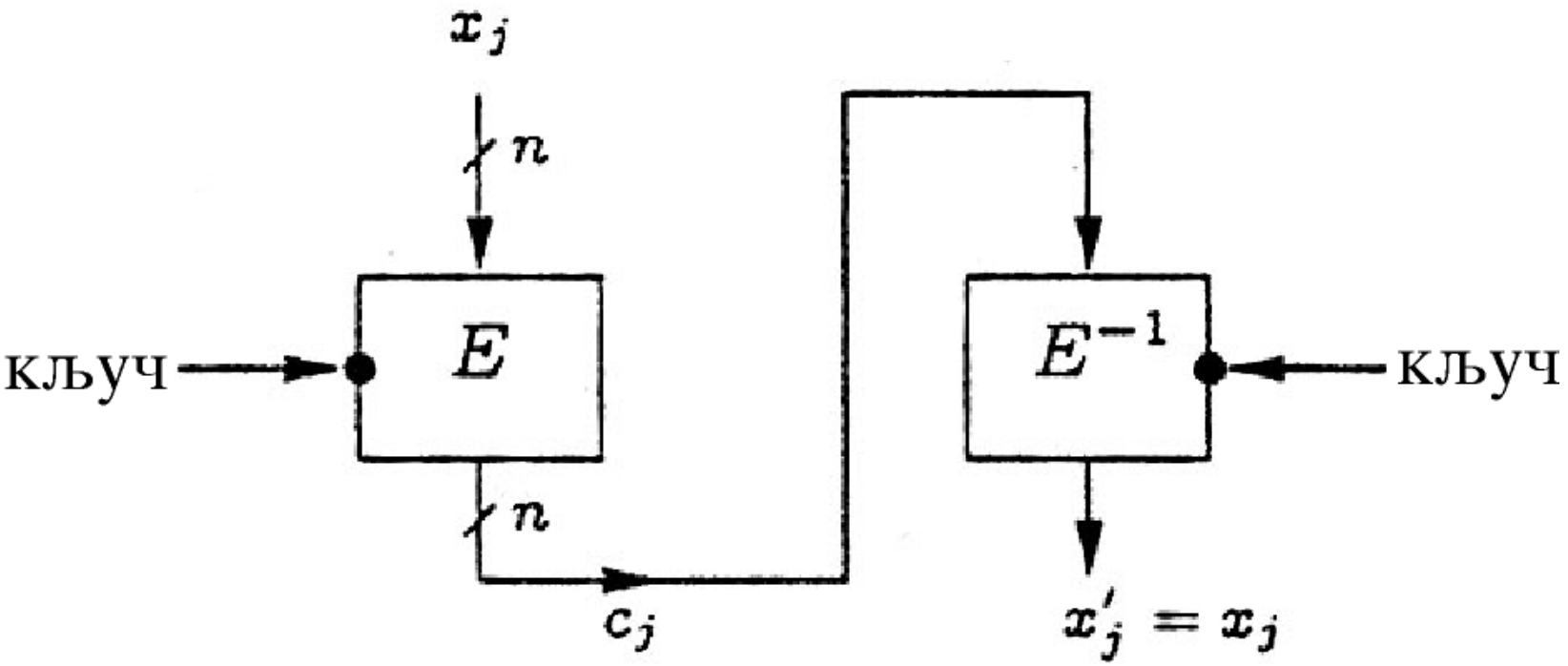
Područja primene blok šifara

- Blok-šifre su pogodne za šifrovanje kratkih poruka – ključevi, identifikacioni podaci, potpisi, lozinke, itd.
- Nisu pogodne za šifrovanje velikih količina podataka, kao što su formatirani tekst, listinzi programa, tabele, i naročito grafičke datoteke pošto se struktura takvih dokumenata lako određuje.

Načini rada blok šifara – kriptografski modovi rada

- Elektronska kodna knjiga (Electronic Codebook, ECB)
- Ulančavanje šifrovanih blokova (Cipher Block Chaining, CBC)
- Šifrat u povratnoj sprezi (Cipher Feedback, CFB)
- Izlazni niz u povratnoj sprezi (Output Feedback, OFB)

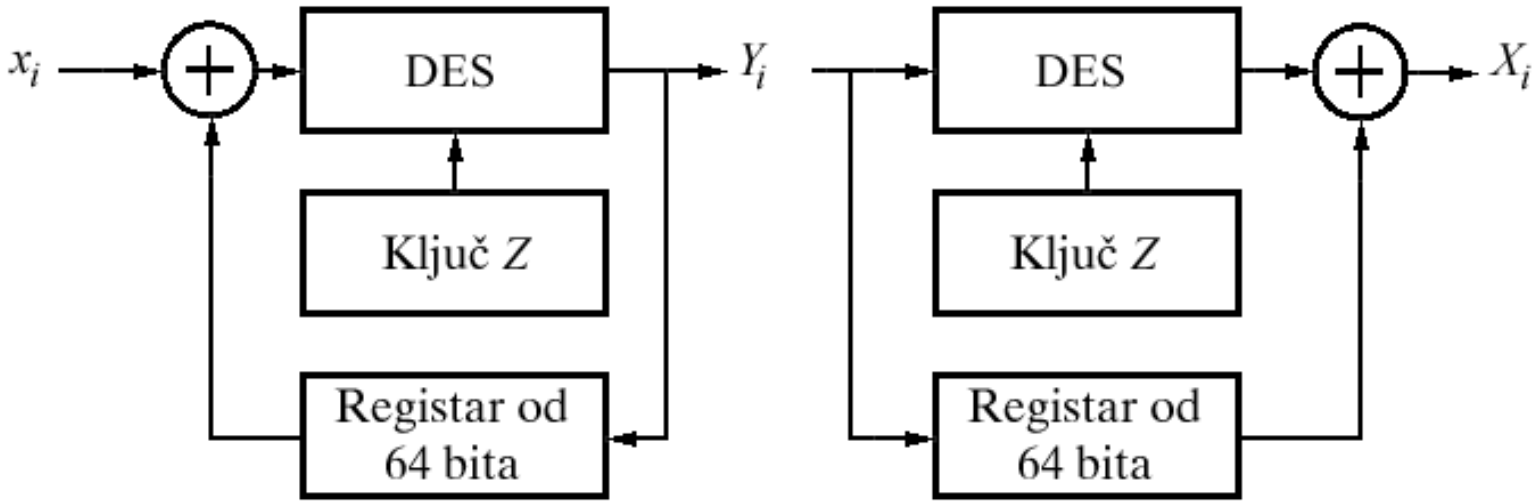
Elektronska kodna knjiga



Elektronska kodna knjiga

- Može se zamisliti džinovska knjiga šifara u kojoj za svaki uzorak otvorenog teksta postoji odgovarajući šifrat.
- Isti blok otvorenog teksta daće uvek isti šifrat
- Ako poruka sadrži blokove koji se sukcesivno ponavljaju, to je moguće prepoznati pri kriptoanalizi

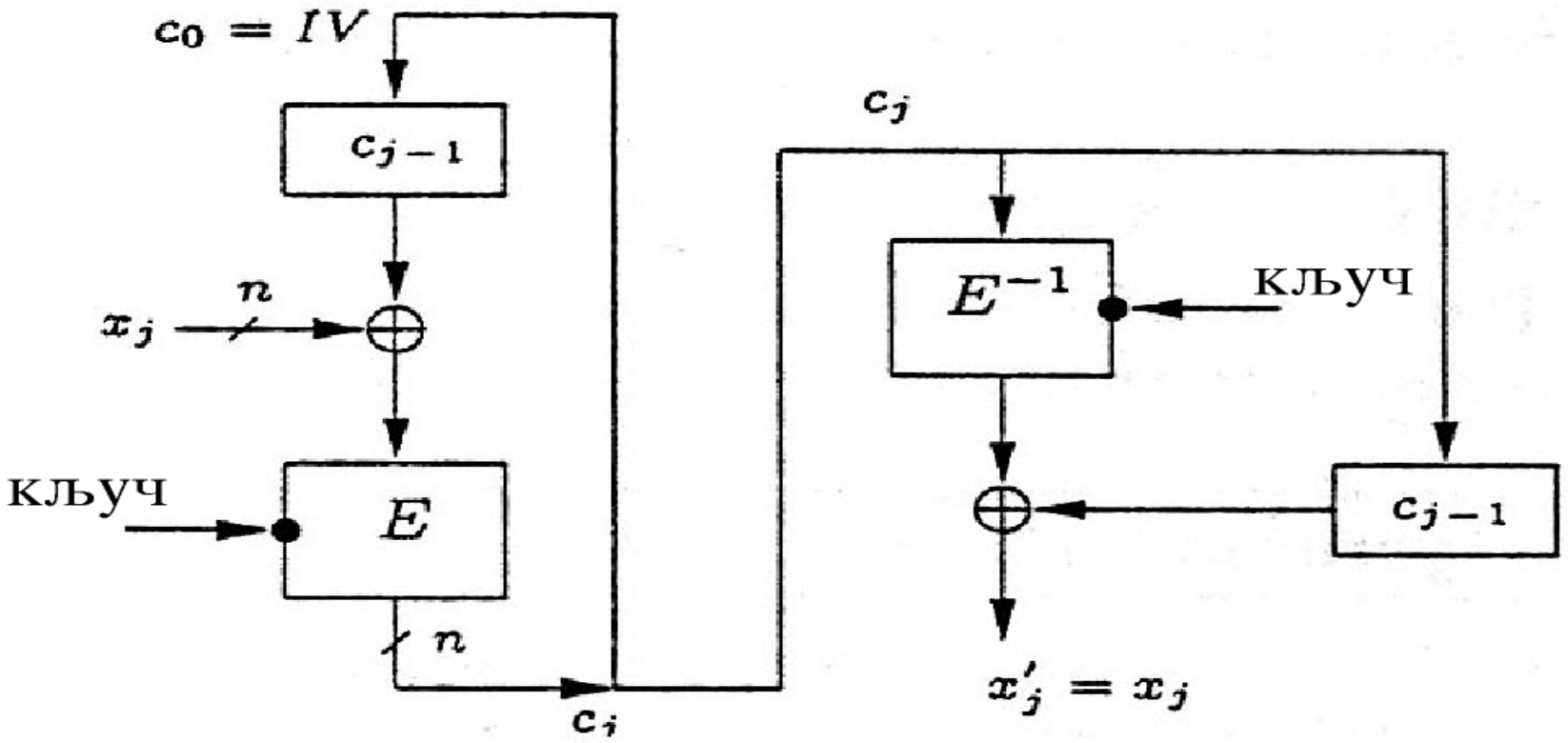
Ulančavanje šifrovanih blokova



Ulančane blok šifre

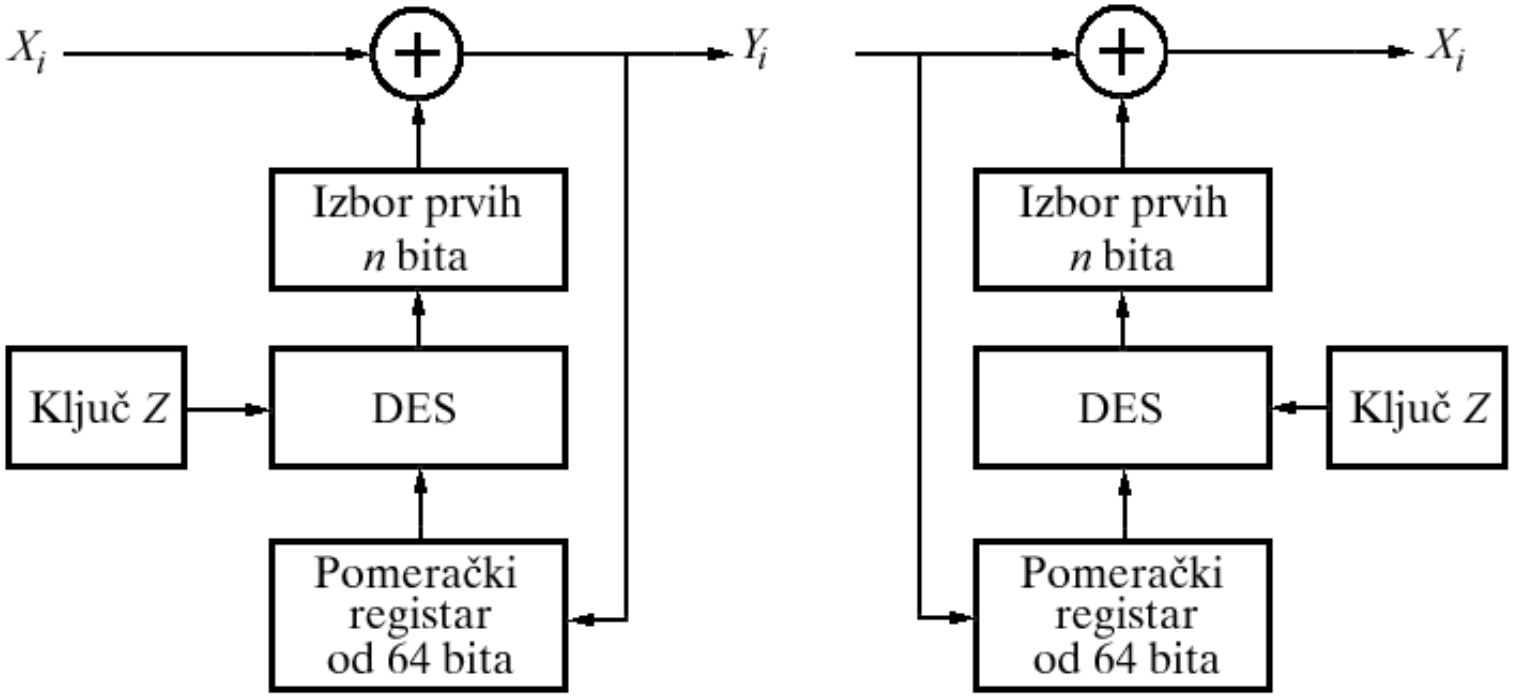
- Ulaz algoritam šifrovanja je rezultat operacije XOR tekućeg bloka poruke (otvorenog teksta) i prethodnog bloka šifrata
- Za sve blokove koristi se isti ključ
- Na početku se u pomerački registar uvodi n bita inicijalnog vektora (IV), koji ne mora da se deži u tajnosti ali je bitno da se generiše na slučajan način.
- Jednake poruke se šifruju na različite načine promenom sadržaja registra u povratnoj sprezi

Ulančavanje šifrovanih blokova



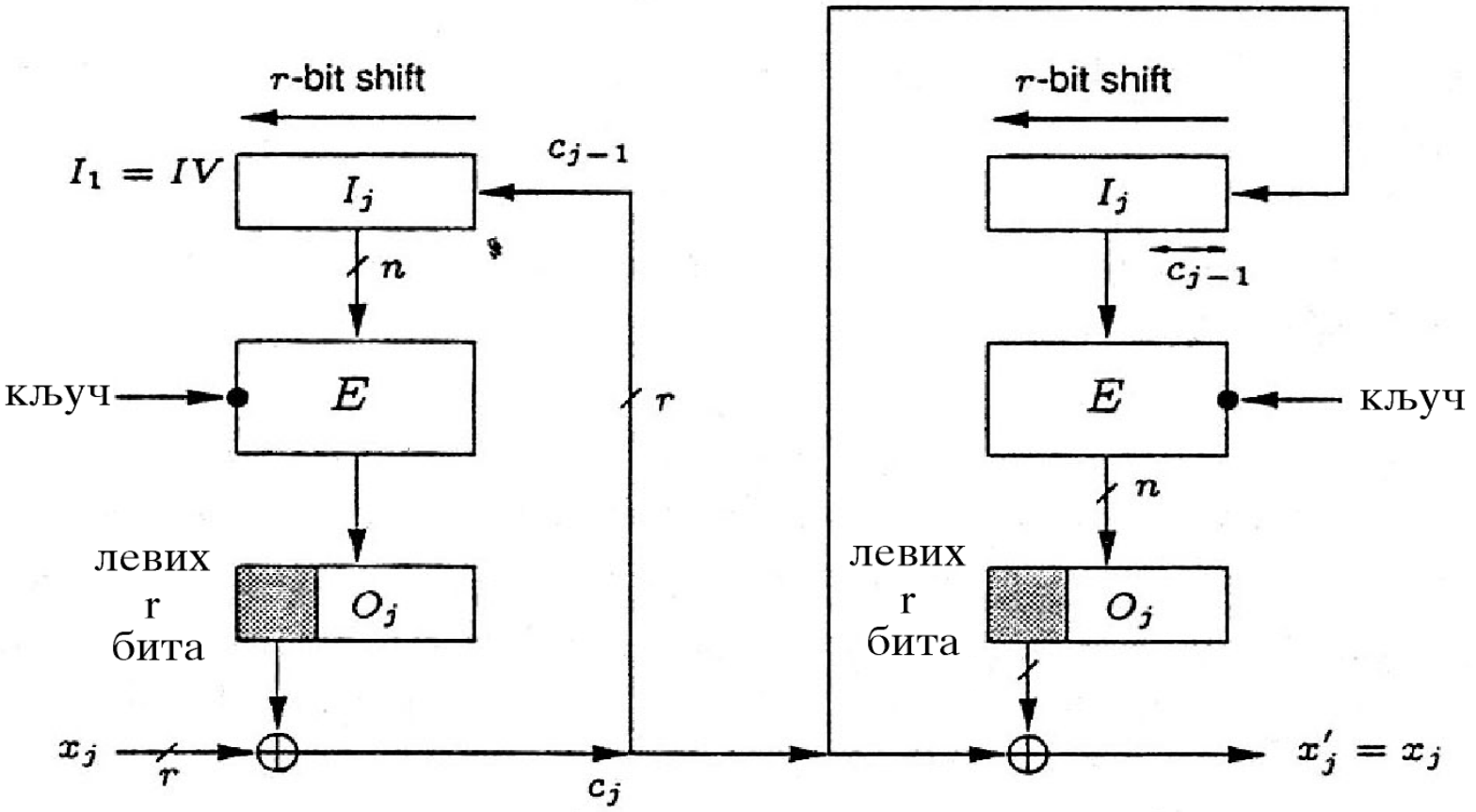
(I) šifrovanje (II) dešifrovanje

Šifrat u povratnoj sprezi



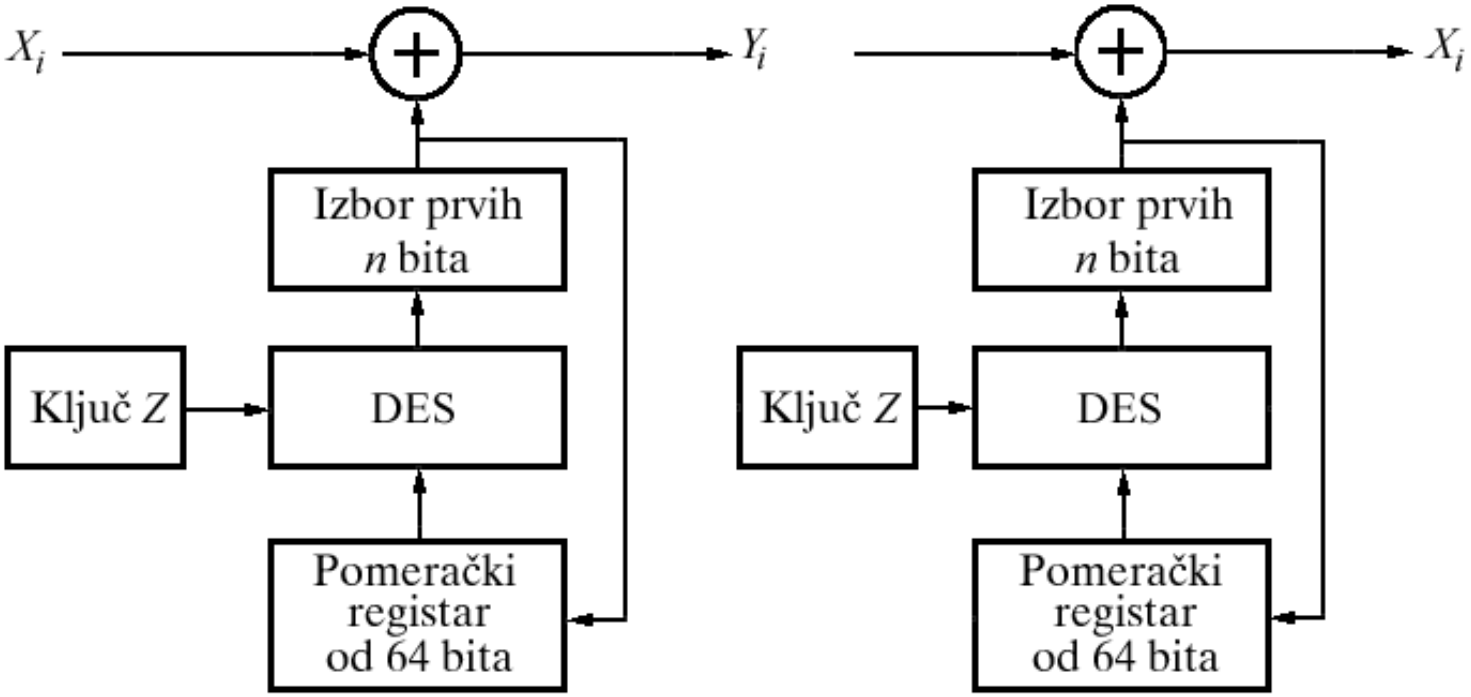
- Na početku se u pomerački registar uvodi n bita inicijalnog vektora (IV) koji ne mora da se drži u tajnosti, ali je pogodno da se generiše na slučajan način.
- Otvoreni tekst se deli na blokove od po *m* bita. Blokovi se sabiraju po modulu 2, bit za bit, gde *m* može da varira između 1 i *n*.
- Pomerački registar dužine *n* bita se pomera ulevo *m* bita posle šifrovanja svakog bloka.
- U ovom načinu rada blok-šifra se pretvara u sekvencijalnu šifru, jednake poruke se mogu šifrovati na različite načine promenom vektora IV, ograničava se propagacija grešaka u prenosu, prostor koji razapinje ključ ne menja se, a šifra je samosinhronišuća.

Šifrat u povratnoj sprezi

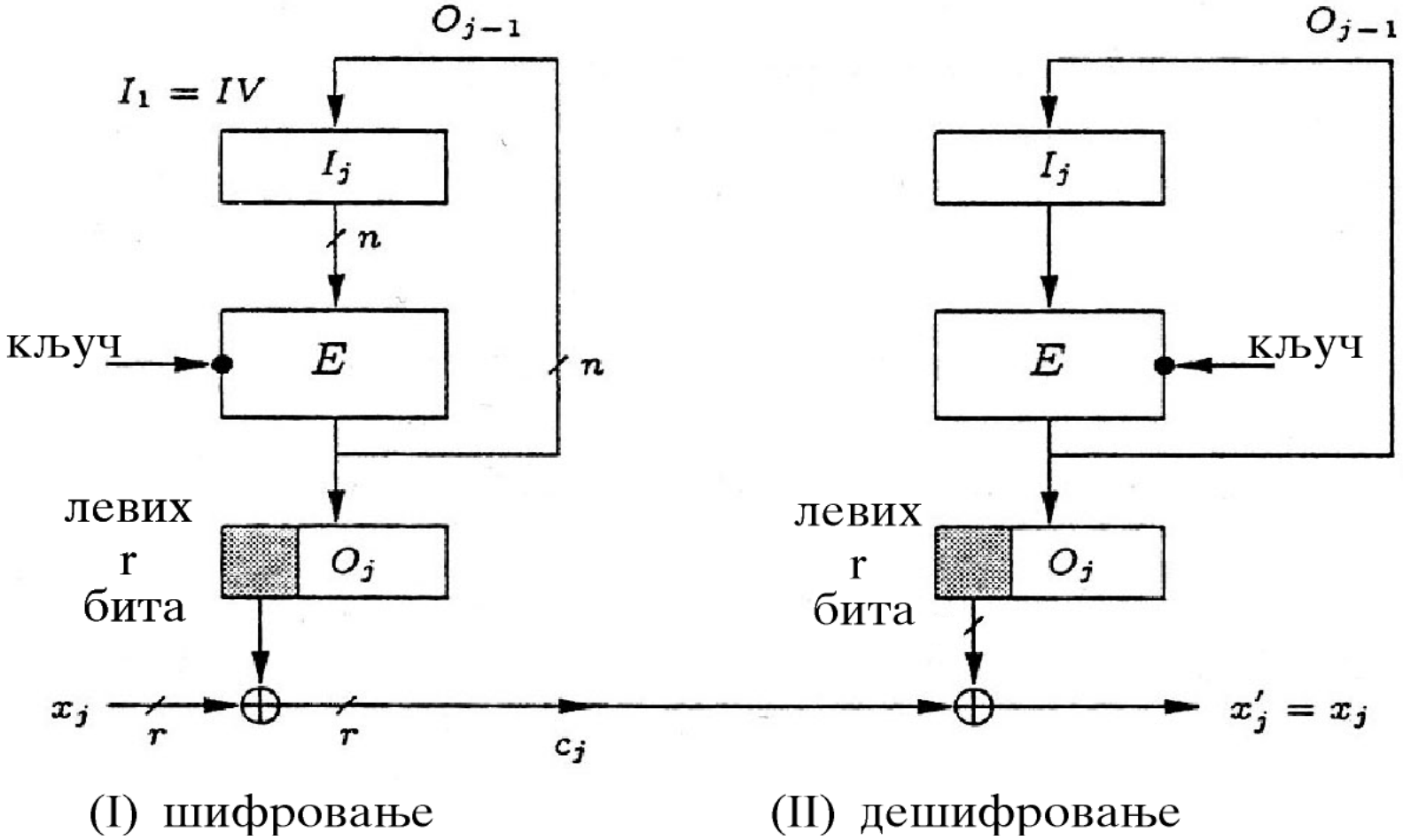


(I) šifrovanje (II) dešifrovanje

Izlazni niz u povratnoj sprezi



Izlazni niz u povratnoj sprezi



(I) шифровање (II) дешифровање

Brojački režim rada

- Koristi se brojač jednak veličini bloka poruke
- Vrednost brojača mora da bude različita za svaki blok poruke
- Nema ulančavanja i može se raditi paralelno na više blokova
- Sadržaj brojača se šifruje ključem, pa se na šifrovan sadržaj i blok poruke primeni XOR

Multiplikacija blok šifre

- Jedini način na koji se može povećati prostor koji razapinje ključ blok-šifre je procedura multiplikacije šifre.
- Radi se o ponavljanju šifre n puta, koristeći n međusobno nezavisnih ključeva.

PROTOČNE ŠIFRE

Slučajni i pseudoslučajni brojevi

- Protočne ili sekvecijalne šifre rade na principu pseudoslučajnih nizova

Osim ove primene koriste se i za:

- Generisanje ključeva kod asimetričnog šifrovanja
- Generisanje privremenih simetričnih ključeva sesija (bezbednost transportnog sloja, Wi-Fi, e-pošte, IP bezbednost...)
- Za distribuciju ključeva

Pseudoslučajni nizovi

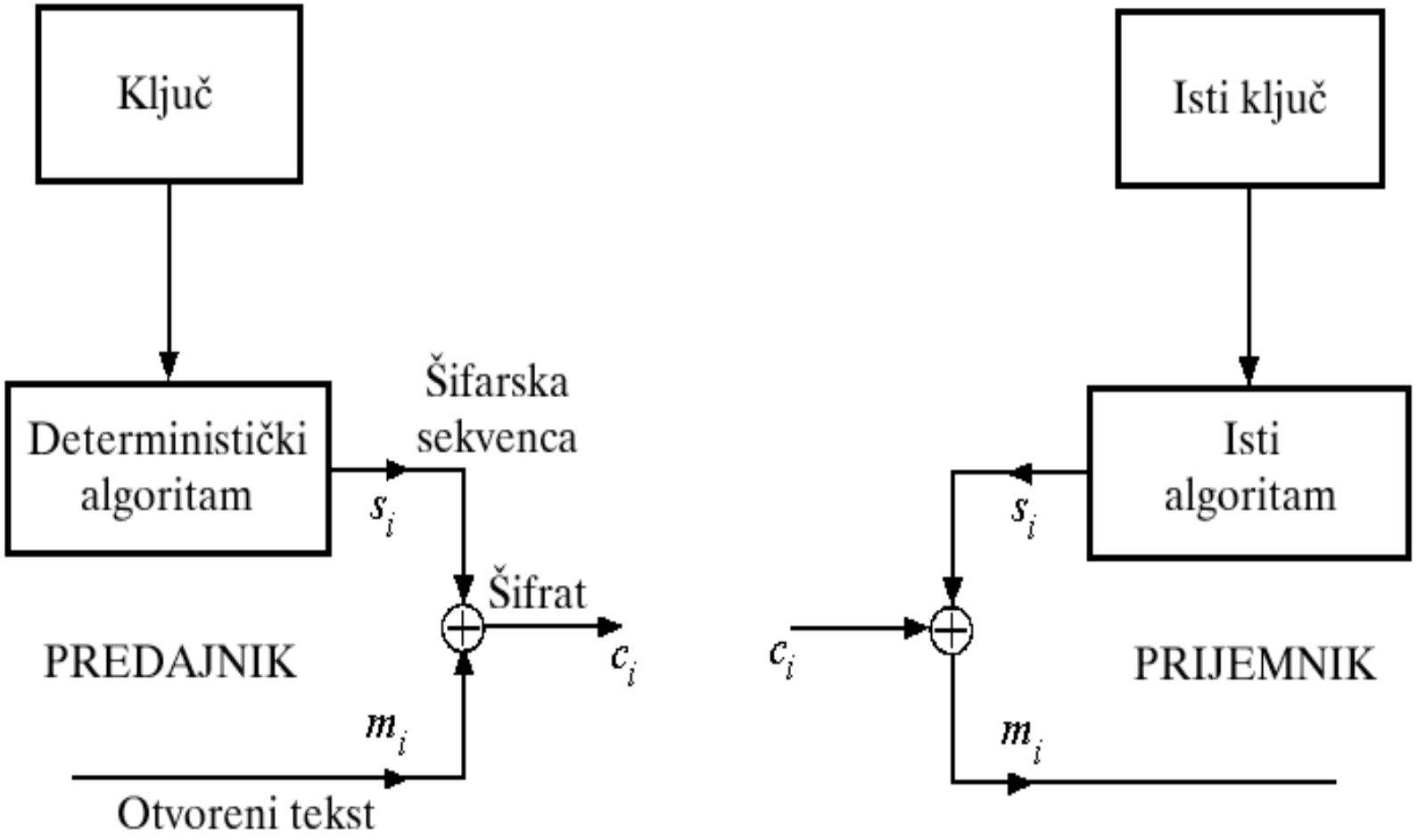
- Slučajni su:
  - Ravnomerno distribuirani (približno jednak broj nula i jedinica)
  - Nezavisni (nijedan podniz ne može da se izvede od ostalih)
- Nepredvidivi su (nemoguće je predvideti sledeći element u nizu na osnovu predhodnih elemenata)
- Postoje generatori pseudoslučajnih brojeva

Sekvencijalni šifarski sistemi

- Generatori pseudoslučajnih brojeva – deterministički algoritmi, ili nizovi simbola koje oni generišu imaju slične osobine kao i slučajni nizovi.
- Koriste kratke ključeve radi započinjanja procesa generisanja.
- Izlazni niz generatora se sabira po modulu 2 sa nizom otvorenog teksta i na taj način se dobija niz šifrata.

- Pseudoslučajni nizovi su periodični u širem smislu (što znači da mogu imati aperiodični početak), ali je poželjno da periodi takvih nizova budu mnogo veći od dužina nizova otvorenog teksta zbog odbrane od napada grubom silom.

Osnovna šema sekvencijalnog šifarskog sistema



Zahtevi koje svaki šifarski niz mora da zadovolji da bi se mogao koristiti u sekvencijalnom šifarskom sistemu:

- **Period** – Period šifarskog niza mora da bude bar jednake dužine kao i dužina niza koji se šifruje. U praksi, generišu se nizovi čiji je period mnogo redova veličine veći od dužine niza koji se šifruje.

Protočne šifre

- Uobičajeno šifruje poruku bajt po bajt, a može i bit po bit
- XOR se vrši nad porukom i izlazom iz generatora pseudoslučajnih bita (niz ključa)
- Pseudoslučajni niz je nepredvidiv ako se ne zna ključ I naizgled je slučajni
- Poželjan je ključ od najmanje 128 bita
- Nije dobro koristiti isti ključ više puta (kod blokovskih šifri to je moguće)

Primer sekvencijalnog algoritma: RC4

- RC4 algoritam koristi tablicu S-box dužine 256 bajtova.
- Za generisanje slučajnog broja K treba uraditi sledeće:

  $i=(i+1) \bmod 256$

  $j=(j+S_i) \bmod 256$

  S_i и S_j zamene mesta

  $t=(S_i+S_j) \bmod 256$

  $K=S_t$
- Dobijeni bajt K se koristi za XOR-ovanje sa otvorenim tekstom za dobijanje šifrata.

Primer sekvencijalnog algoritma: RC4

- Inicijalizacija S-box je veoma jednostavna. Prvo se linearno napuni tako da je: S0=0, ..., S255=255,
- Zatim se generiše niz od 256 bajtova ključa (ponavljanjem)
- Tada se S-box popunjava na sledeći način:

Za i=0 do 255

$j=(j + S_i + K_i) \bmod 256$

S_i i S_j zamene mesta.