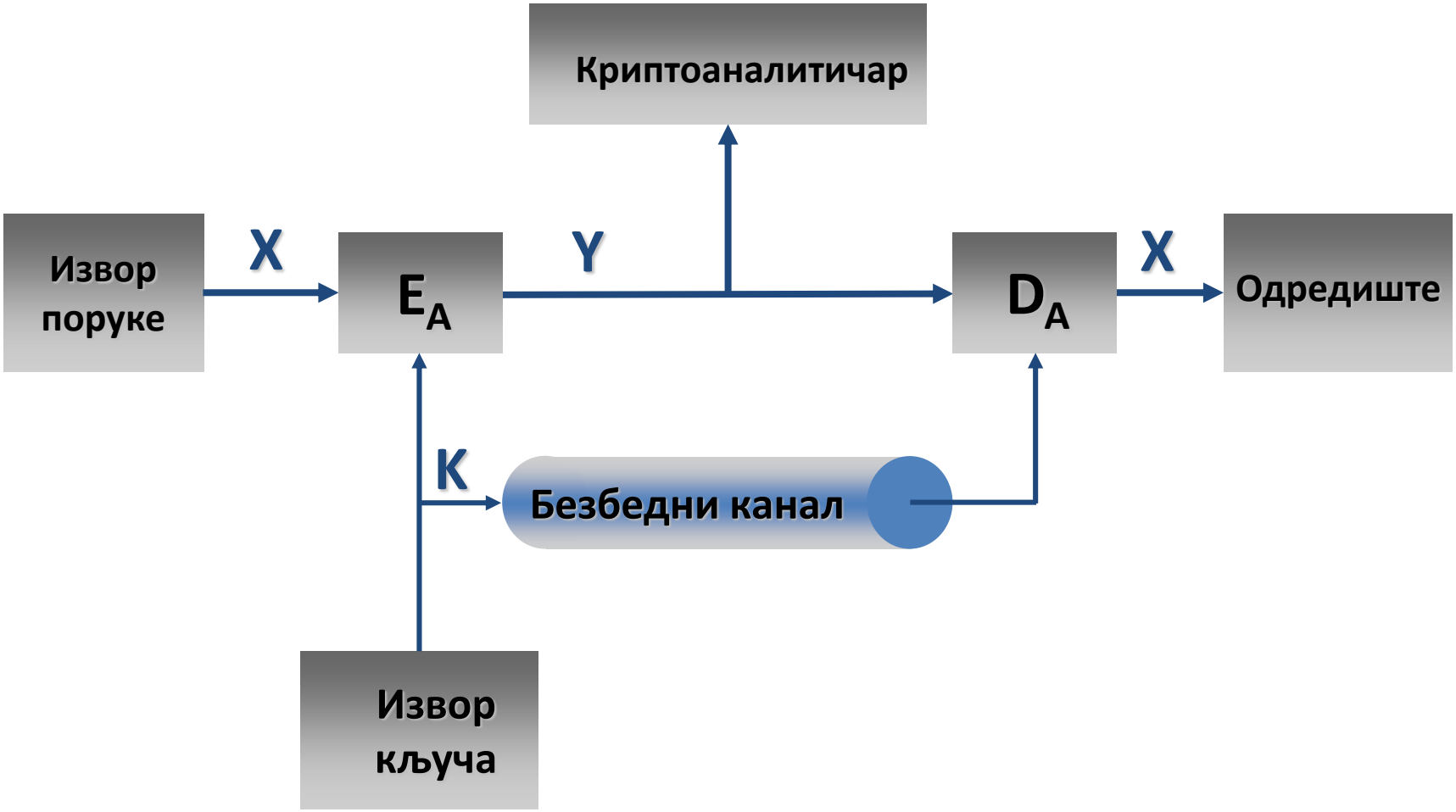
Simetrični kriptosistemi

Kriptografija

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

Princip rada



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

Simetrični blokovski algoritmi šifrovanja

- DES
- 3DES
- AES

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

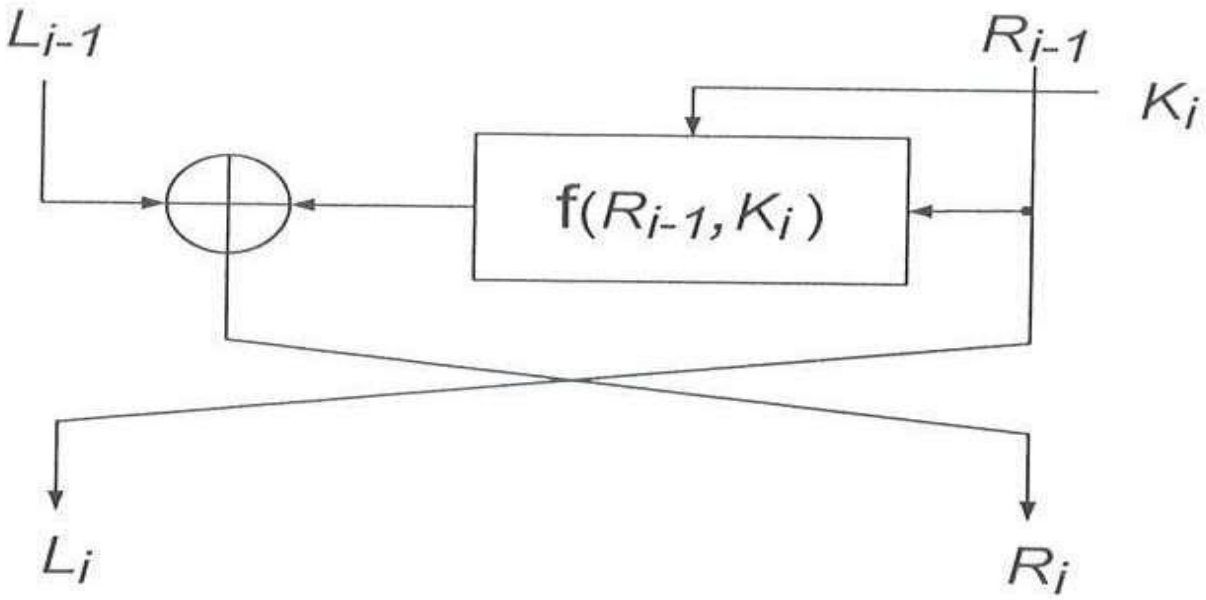
DES – šifrovanje

- Blok običnog teksta X se izloži inicijalnoj permutaciji IP
- 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

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

DES

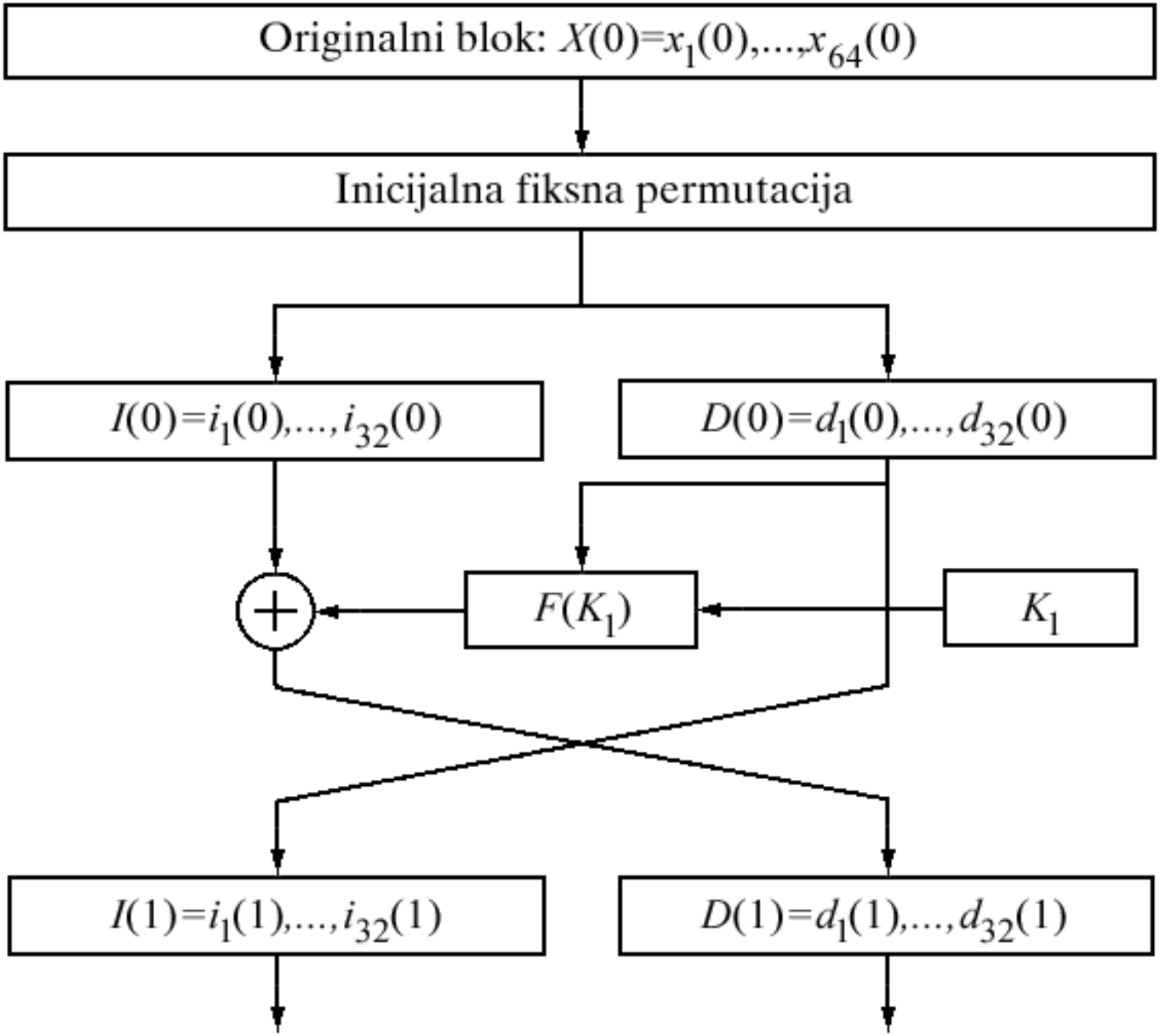
- Блок шифра највише коришћена у пракси је DES (Data Encryption Standard), који је NBS (National Bureau of Standards) увео у САД 1974.
- Дужина блока код ове шифре је 64 бита, а дужина кључа је 56 бита.

Опис рада DES-а

- DES алтернативно шифрује две половине блока.
- Најпре се врши иницијална фиксна пермутација бита у блоку.
- Затим се блок дели на две половине (леви и десни блок).
- После тога се реализује једна модуларна операција која се понавља 16 пута (“рунди").

- Ова операција се састоји од суме по модулу 2 леве половине блока са функцијом $F(K_i)$ десне стране блока, на коју утиче и подкључ $K_i,\ i = 1,\ldots,16$

  где је *i* редни број рунде.
- Затим лева и десна половина мењају места.


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
$I(1)=i_1(1),...,i_{32}(1)$
$D(1)=d_1(1),...,d_{32}(1)$

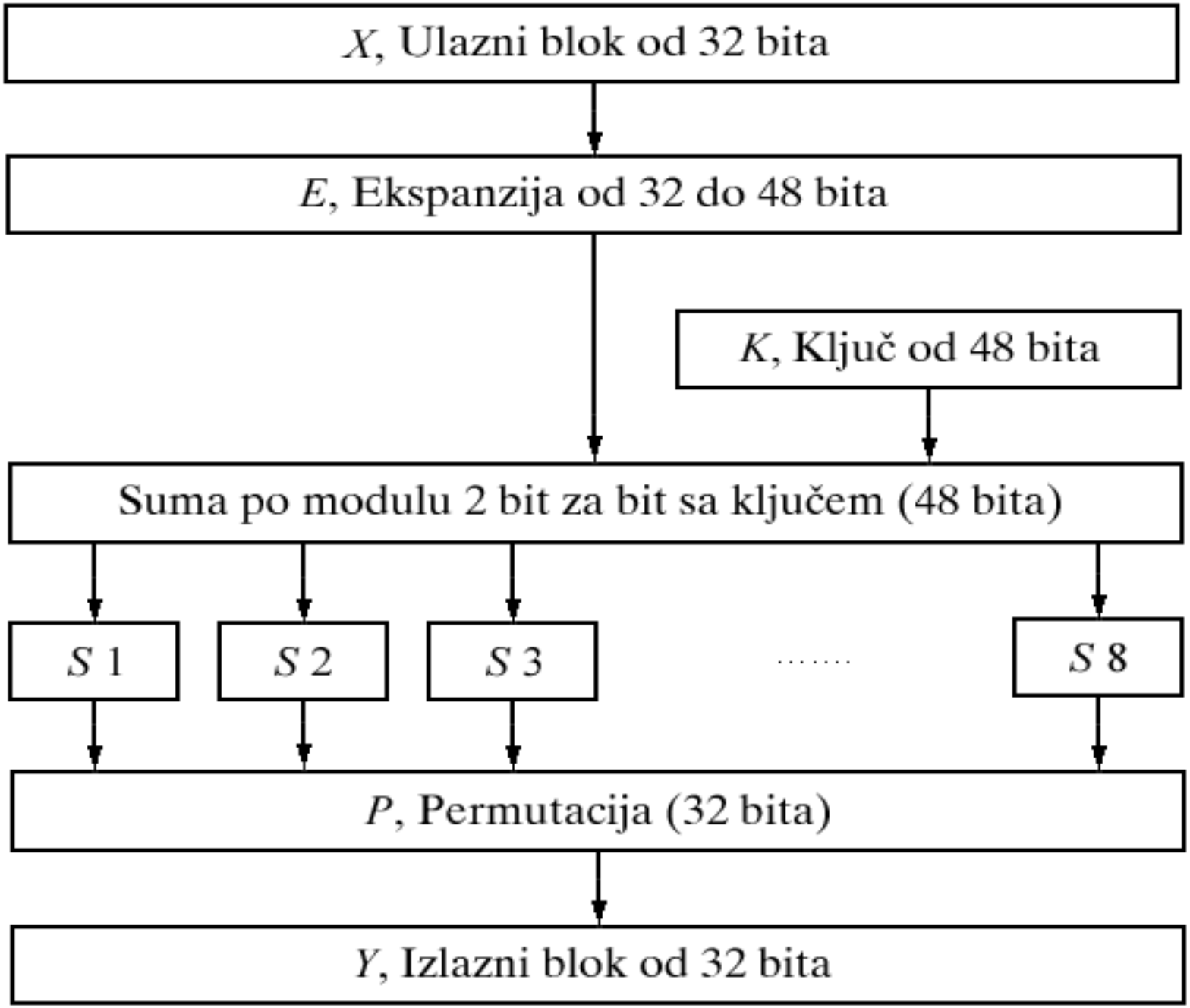
- У 16. Рунди се изоставља размена места леве и десне половине блока, а алгоритам се завршава фиксном пермутацијом бита у блоку која је инверзна иницијалној.
- DES реализује инволутивну трансформацију и зато није потребно инвертовати функцију F у алгоритму за дешифровање. Зато F може да буде једносмерна функција, која садржи нелинеарне операције.

- Иако DES користи кључ од 64 бита, прва операција која се реализује је његова редукција на 56 бита, елиминацијом једног од сваких осам бита.
- Затим се врши преуређење преосталих бита.
- Потом се генерише 16 подкључева потребних у 16 рунди алгоритма. Сваки подкључ се састоји од 48 бита. За време дешифровања они се користе обрнтим редом у односу на онај коришћен током шифровања.

Генерисање подкључева:

- Најпре се кључ од 56 бита подели на две половине од по 28 бита.
- Затим се те половине ротирају улево један или два бита, у зависности од редног броја рунде.
- После ротирања, половине се поново саставе и тако се поново добије 16 група од по 56 бита.
- Од ових бита се изабере по 48 бита из сваке групе, чиме се коначно добија 16 подкључева.

- Овај процес се назива “пермутација са компресијом". Изабрани бити су једнаки за све подкључеве.


X, Ulazni blok od 32 bita
E, Ekspanzija od 32 do 48 bita
K, Ključ od 48 bita
Suma po modulu 2 bit za bit sa ključem (48 bita)
S 1
S 2
S 3
.....
S 8
P, Permutacija (32 bita)
Y, Izlazni blok od 32 bita

- Прва манипулација се састоји од формирања вектора од 48 бита, на основу почетна 32 бита, путем линеарне експанзије.
- Затим се комбинује локални кључ од 48 бита са претходно генерисаним вектором сабирањем по модулу 2, бит за бит, чиме се добија други вектор од 48 бита, који се дели на 8 група по 6 бита.
- Свака од ових група улази у једну од 8 функција које се називају "S-box". Ове таблице су одговорне за нелинеарност DES-а.

- Из сваке таблице излазе 4 бита. Када се промени само један бит на улазу, промене се бар два бита на излазу.
- На крају, информација пролази кроз "P-box", што је једна фиксна пермутација, изабрана на такав начин да дифузија бита буде максимална у блоку од 32 бита.

Основне особине DES-а

- **Међусобна зависност симбола** – Сваки бит шифрата је једна сложена функција свих бита и свих бита отвореног текста.
- **Промена улазних бита** – Промена једног бита поруке проузрокује промену приближно 50% бита блока шифрата.
- **Промена бита кључа** – Промена једног бита кључа проузрокује промену приближно 50% бита блока шифрата.

Недостаци DES-а

- Слаби кључеви – Постоје четири слаба кључа који омогућавају лако декриптовање шифроване поруке, зато што су у случају употребе тих кључева сви подкључеви K_1 do K_{16} међусобно једнаки.
- Постоји 28 “делимично слабих" кључева који омогућавају лако декриптовање шифроване поруке, зато што су у случају употребе тих кључева само два или четири подкључа међусобно различити.
- Грешка при преносу дела шифрата простире се на цео блок у коме је тај део.

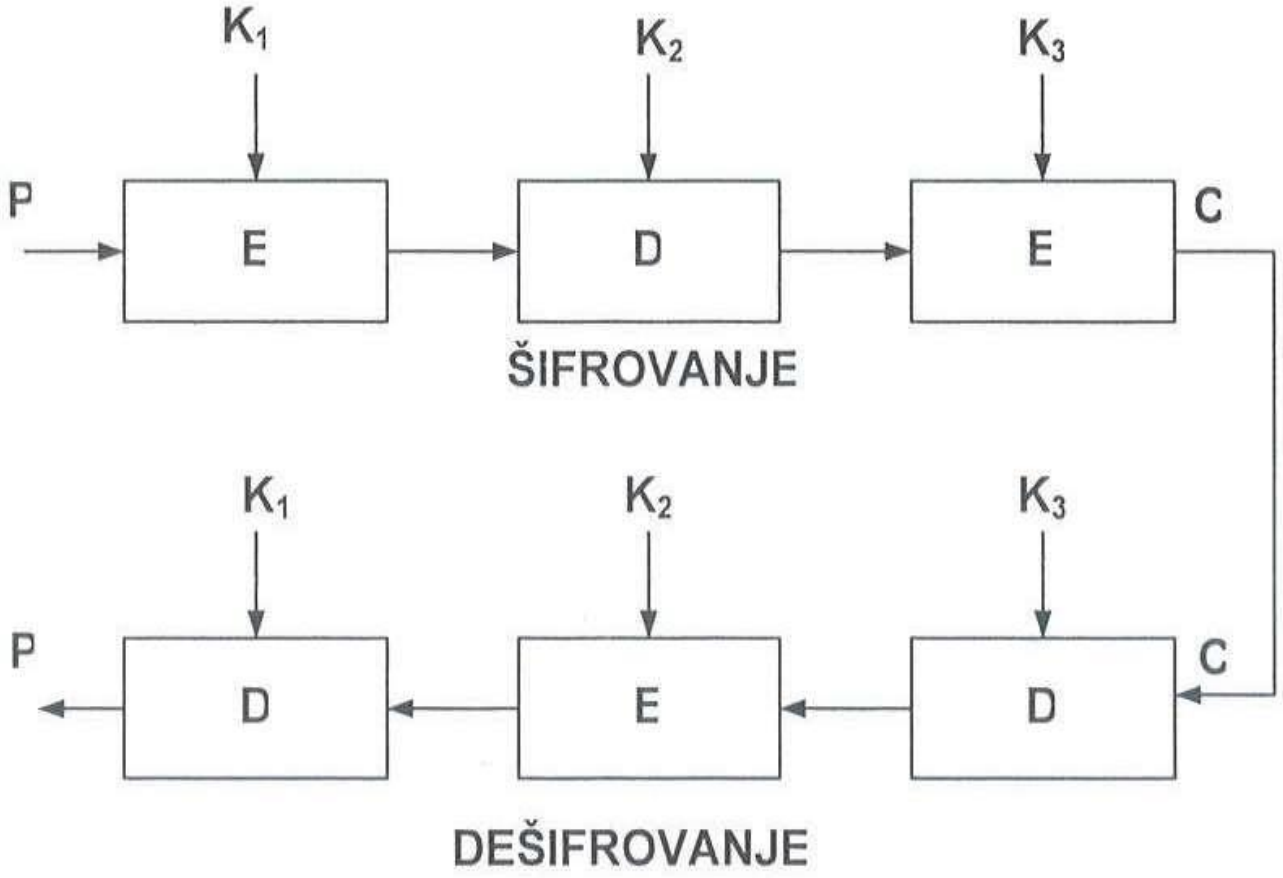
Недостаци DES-а

- Један од проблема при употреби DES-а састоји се у томе што је дужина кључа који ова шифра користи недовољна када се има у виду данашње стање развоја технологије.
- Јасно је да кључ дужине 56 бита не обезбеђује довољан ниво безбедности имајући у виду процесне могућности савремених рачунара и ниво интеграције чипова.
- Такође су објављени и специјални напади на блок шифре, на пример на DES, као што су линеарна и диференцијална криптоанализа.

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

3DES algoritam



Slika 2.4 – 3DES šifrovanje/dešifrovanje

AES (Rijndael)

- Због слабости DES-а, у САД су одлучили да га замене новом блок-шифром, названом AES (Advanced Encryption Standard).
- Коначна верзија алгоритма AES била је изабрана између 5 кандидата. Изабран је алгоритам Rijndael.

- Rijndael је итеративна блок-шифра са променљивом дужином блока, као и са променљивом дужином кључа.
- Ове дужине могу бити 128, 192 и 256 бита.
- Основни елемент ове шифре се назива Стање (State). State је матрица са 4 врсте и *Nb* колона, где је *Nb* једнако дужини блока подељеној са 32.
- Кључ је такође дат матрицом са 4 врсте и *Nk* колона, где је *Nk* једнако дужини кључа подељеној са 32.
- Број рунди *Nr* код ове шифре је такође променљив и зависи од вредности *Nb* и *Nk*. *Nr* узима вредности између 10 и 14.

Трансформација у оквиру једне рунде састоји се од 4 корака

- Нелинеарна супституција бајтова (ByteSub).
- Циклични померај врста матрице State (ShiftRow).
- Множење колона матрице State фиксним полиномом по модулу (MixColumn).
- Сабирање кључа рунде са матрицом State (RoundKey).

- Да би алгоритам дешифровања био што сличнији алгоритму шифровања, последња рунда не садржи корак MixColumn.

- ByteSub је нелинеарна трансформација бајтова, која независно трансформише сваки бајт матрице State.
- Таблица супституције (под именом S-box) је инвертибилна и састоји се од две трансформације:
  - Мултипликативна инверзија у GF(2^8) бајта, у којој се 00 трансформише у самог себе, и
  - Афина трансформација над GF(2), дефинисана још једном матрицом.
- Инверзна трансформација од ByteSub садржи инверзну таблицу од ByteSub. Добија се инверзијом матрице афине трансформације из ByteSub и рачунањем мултипликативне инверзије резултата у GF(2^8).

- Трансформација ShiftRow циклички помера врсте матрице State на различите начине: врста i се помера за C_i позиција, где C_i зависи од дужине блока Nb, i=0,...,3.
- Вредности C_i се налазе између 1 и 4.
- Инверзна трансформација од ShiftRow помера врсту i за $(Nb\text{-}C_i)$ позиција, i=1,...3.

- У трансформацији MixColumn, колоне матрице State се сматрају полиномима над GF(2^8) и множе се фиксним полиномом

$$3X^3 + X^2 + X + 2$$

по модулу $X^4 + 1$

- Инверзна трансформација од MixColumn је слична трансформацији MixColumn: свака колона матрице State се множи фиксним полиномом $11X^3 + 13X^2 + 9X + 14$

по модулу $X^4 + 1$

- У трансформацији RoundKey, кључ рунде се сабира са State по модулу 2, бит за бит.
- Дужина кључа рунде је једнака Nb.
- Овај кључ се добија од шифарског кључа (Cipher key) помоћу посебног алгоритма (Key Shedule Algorithm).
- Трансформација RoundKey је аутоинвертибилна.

- Алгоритам Key Shedule састоји се од две компоненте:
  - Експанзија кључа и
  - Избор кључа рунде.
- Експанзија кључа трансформише шифарски кључ (Cipher Key) у кључ веће дужине, чијих су првих Nk низова од по 4 бајта једнака онима из Cipher Key.
- Постоји разлика између алгоритама експанзије у зависности од тога да ли је $Nk \leq 6$ или $Nk > 6$.
- Алгоритам за избор кључа рунде користи 6 низова од по 4 бајта за сваку рунду, првих 6 за прву рунду, других 6 за другу, итд.

- Слаби, као и делимично слаби кључеви не могу да се појаве код Rijndael-а, пошто алгоритми шифровања и дешифровања користе различите компоненте.
- Ова шифра је такође отпорна на линеарну и диференцијалну криптоанализу, као и на неке друге публиковане нападе на блок-шифре.

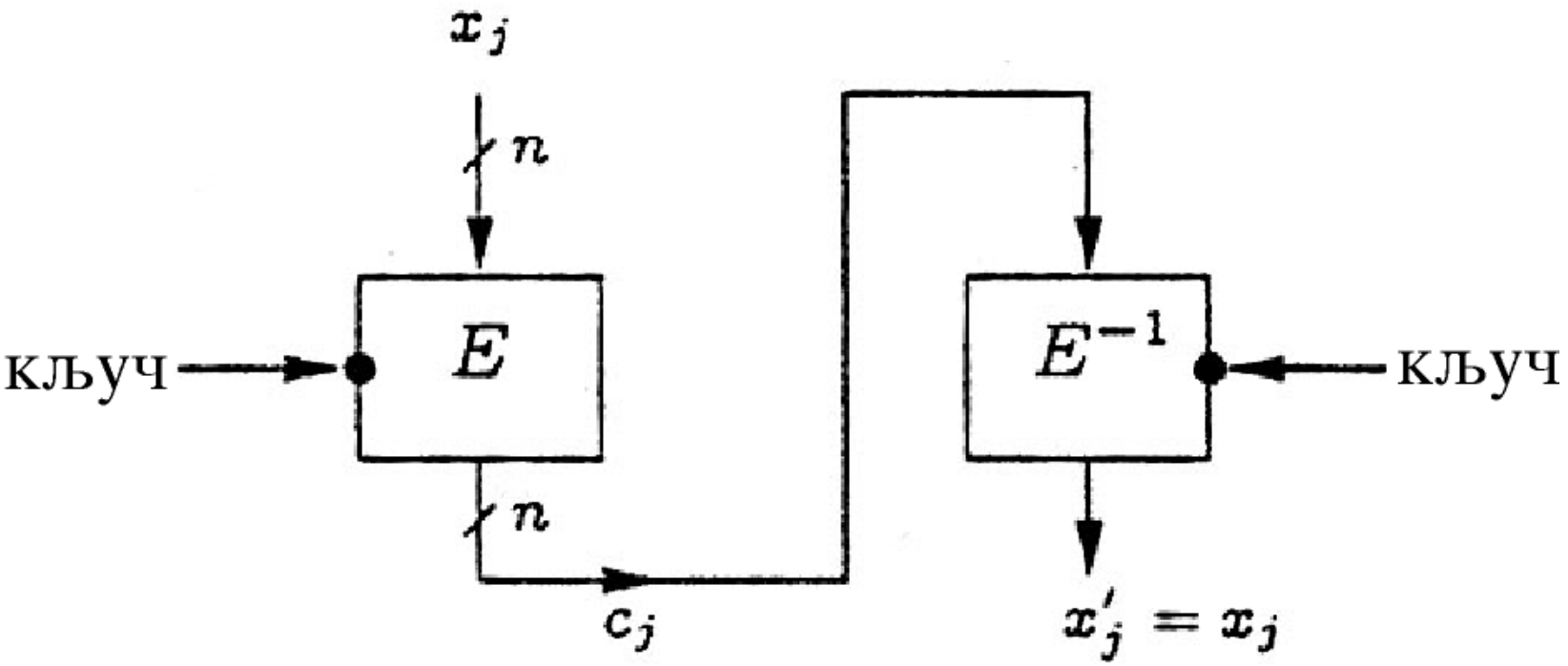
Подручја примене блок шифара

- Блок-шифре су погодне за шифровање кратких порука – кључеви, идентификациони подаци, потписи, лозинке, итд.
- Нису погодне за шифровање великих количина података, као што су форматирани текст, листинзи програма, табеле, и нарочито графичке датотеке пошто се структура таквих докумената лако одређује.

Начини рада блок шифара – криптографски модови рада

- Електронска кодна књига (Electronic Codebook, ECB)
- Уланчавање шифрованих блокова (Cipher Block Chaining, CBC)
- Шифрат у повратној спрези (Cipher Feedback, CFB)
- Излазни низ у повратној спрези (Output Feedback, OFB)

Електронска кодна књига

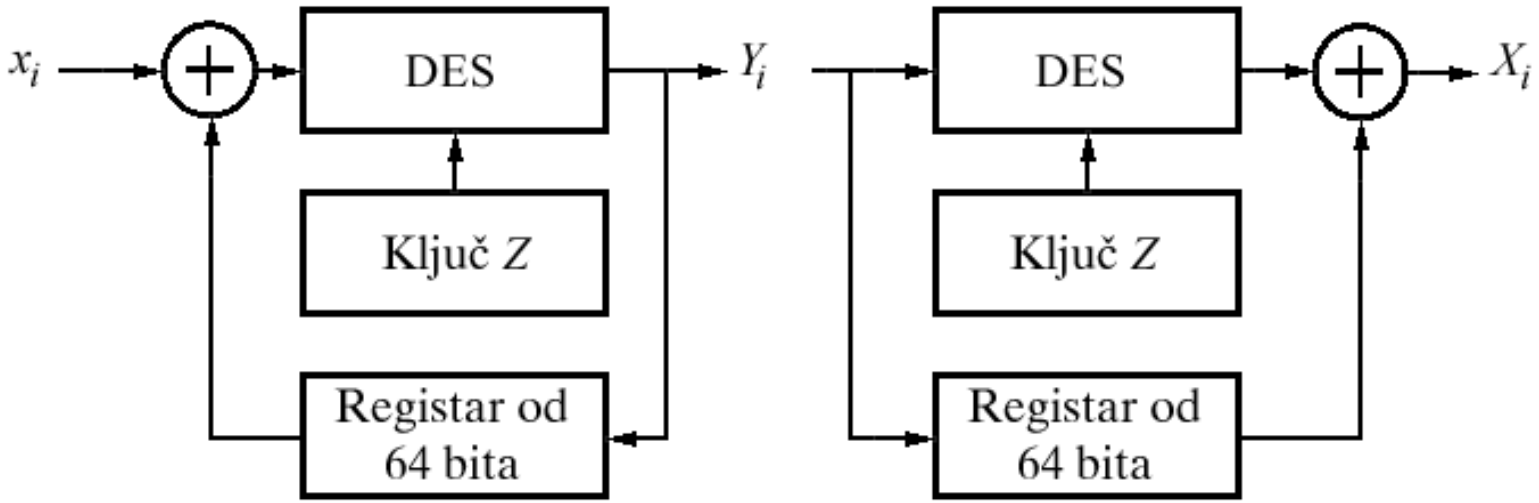


(I) шифровање (II) дешифровање

Електронска кодна књига

- Може се замислити џиновска књига шифара у којој за сваки узорак отвореног текста постоји одговарајући шифрат.
- Исти блок отвореног текста даће увек исти шифрат
- Ако порука садржи блокове који се сукцесивно понављају, то је могуће препознати при криптоанализи

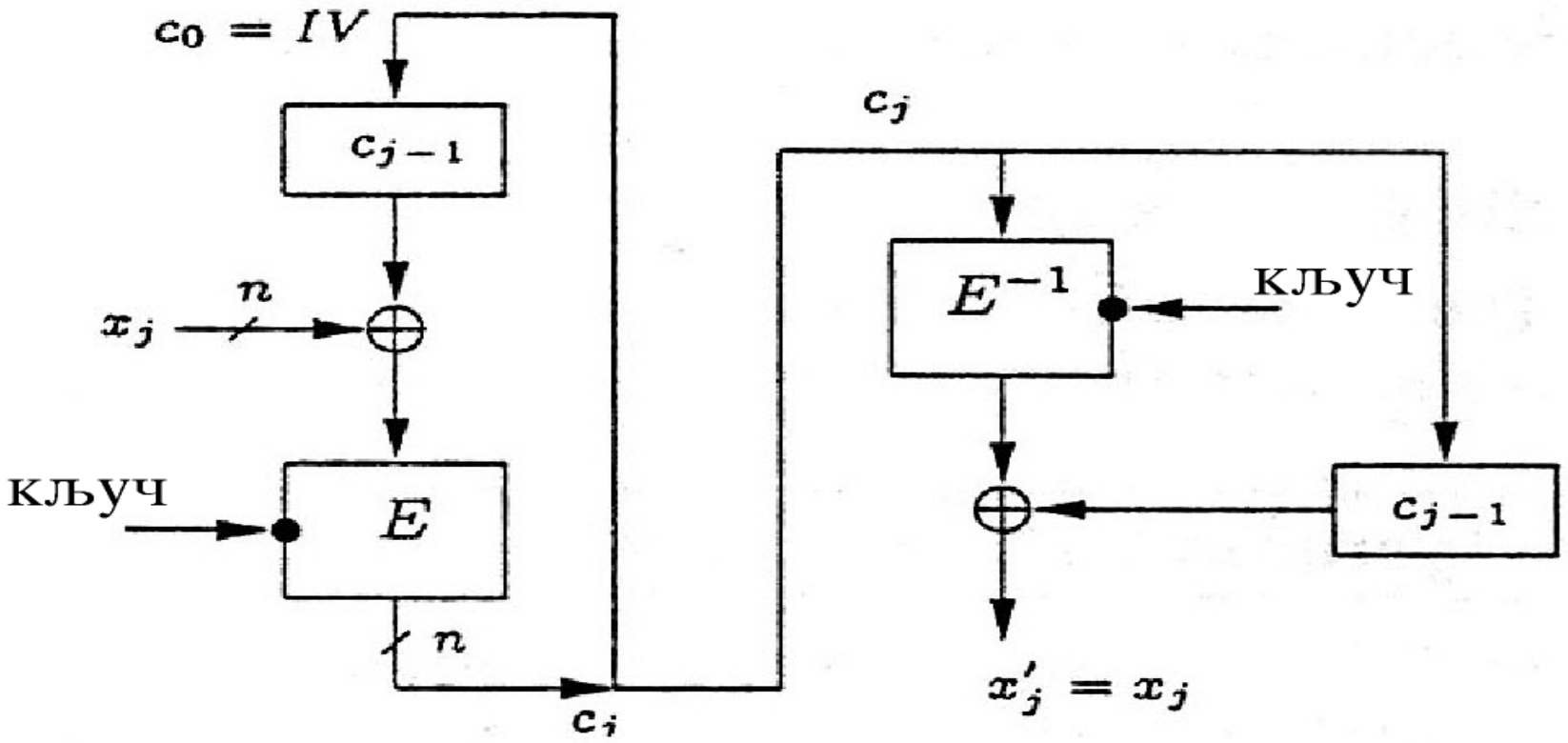
Уланчавање шифрованих блокова



Уланчане блок шифре

- Улаз алгоритам шифровања је резултат операције XOR текућег блока поруке (отвореног текста) и претходног блока шифрата
- За све блокове користи се исти кључ

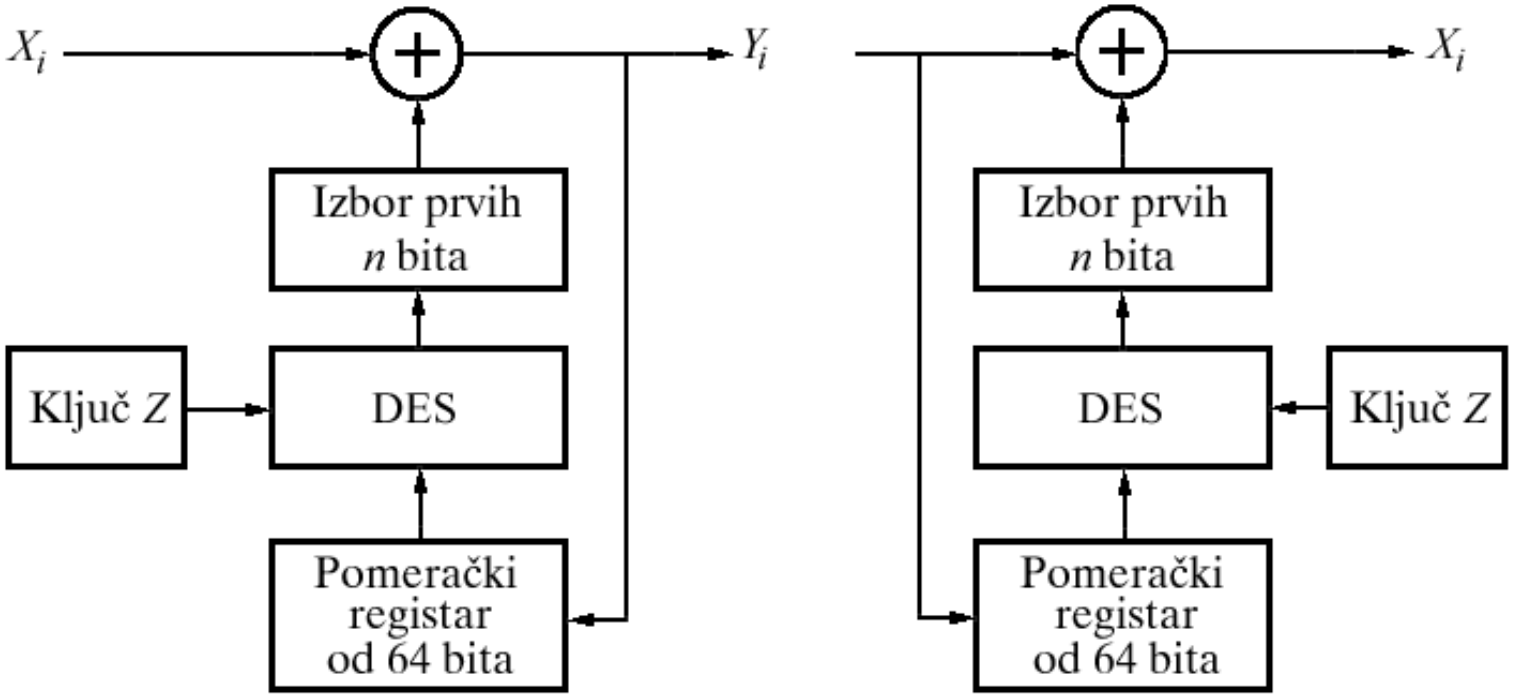
Уланчавање шифрованих блокова



(I) шифровање (II) дешифровање

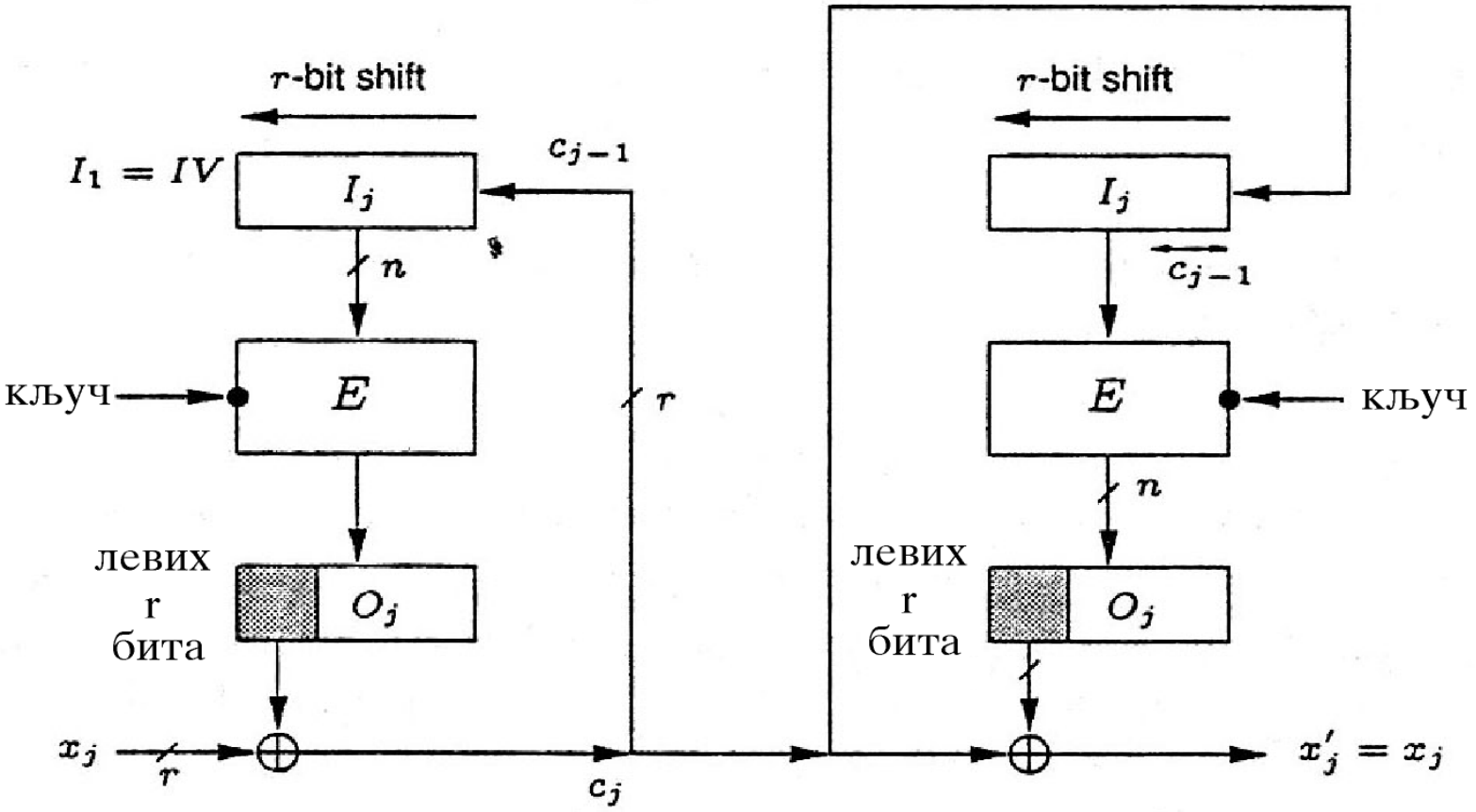
- На почетку се у померачки регистар уводи *n* бита иницијалног вектора (IV), који не мора да се дежи у тајности али је битно да се генерише на случајан начин.
- У овом моду рада, блок-шифра се претвара у секвенцијалну шифру, једнаке поруке се шифрују на различите начине променом IV, пропагација грешака у преносу се ограничава, а простор који разапиње кључ се не мења.

Шифрат у повратној спрези



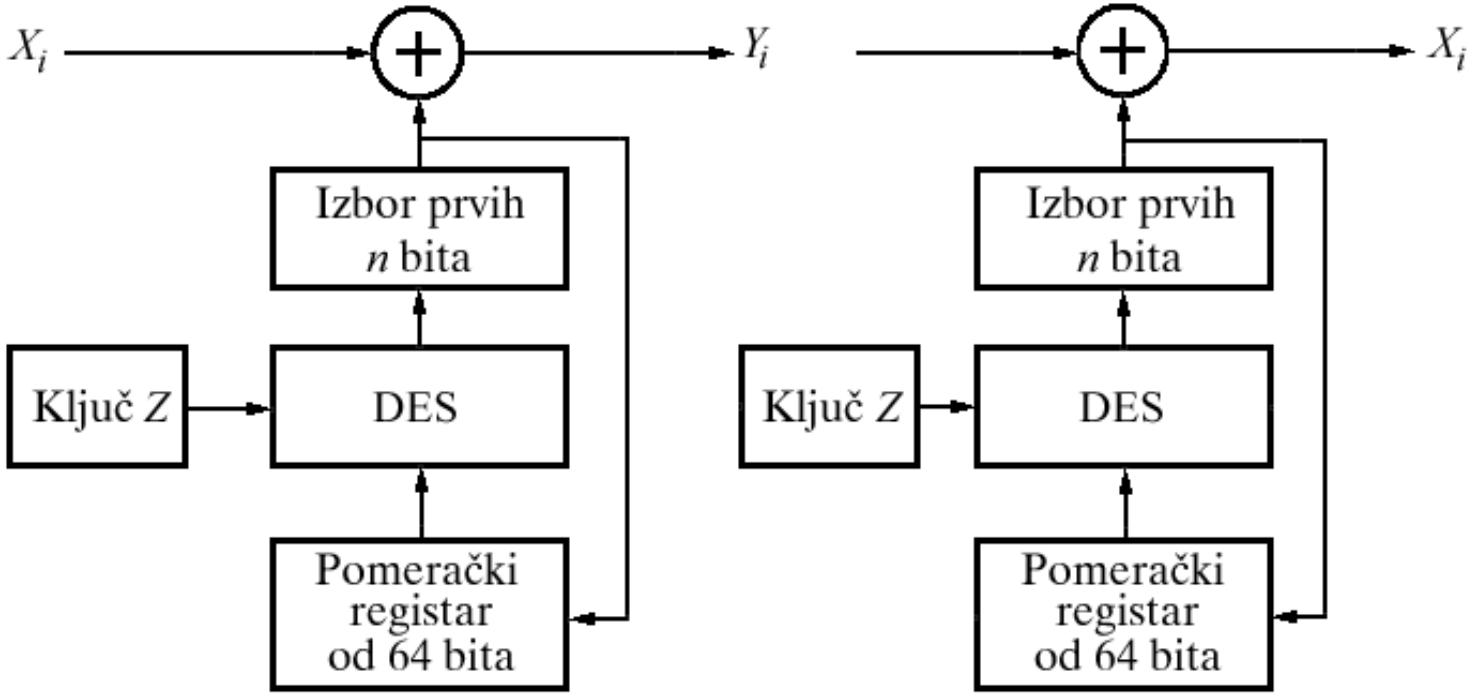
- На почетку се у померачки регистар уводи *n* бита иницијалног вектора (IV) који не мора да се држи у тајности, али је погодно да се генерише на случајан начин.
- Отворени текст се дели на блокове од по *m* бита. Блокови се сабирају по модулу 2, бит за бит, где *m* може да варира између 1 и *n*.
- Померачки регистар дужине *n* бита се помера улево *m* бита после шифровања сваког блока.
- У овом начину рада блок-шифра се претвара у секвенцијалну шифру, једнаке поруке се могу шифровати на различите начине променом вектора IV, ограничава се пропагација грешака у преносу, простор који разапиње кључ не мења се, а шифра је самосинхронишућа.

Шифрат у повратној спрези

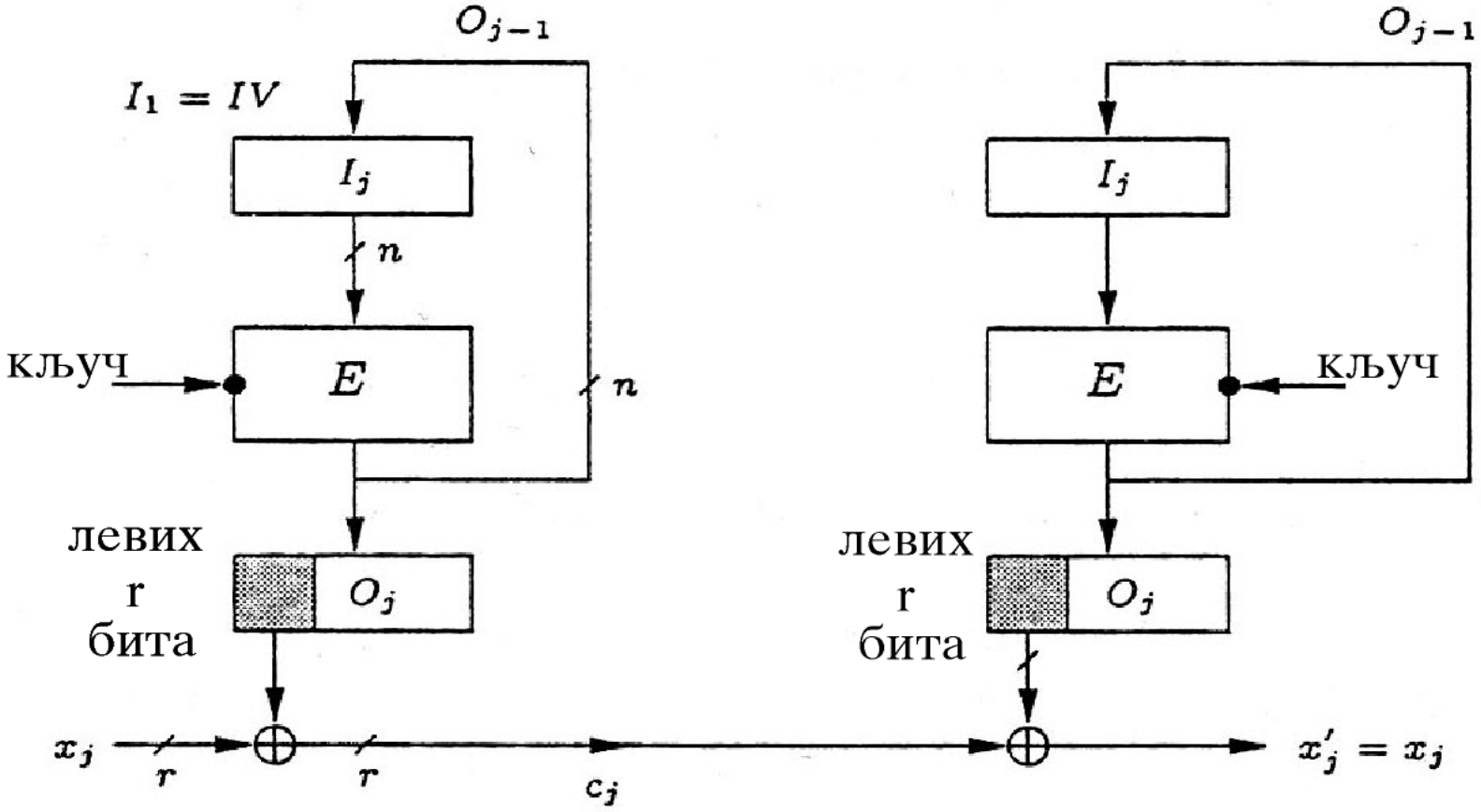


(I) шифровање (II) дешифровање

Излазни низ у повратној спрези



Излазни низ у повратној спрези



(I) шифровање (II) дешифровање

Бројачки режим рада

- Користи се бројач једнак величини блока поруке
- Вредност бројача мора да буде различита за сваки блок поруке
- Нема уланчавања и може се радити паралелно на више блокова
- Садржај бројача се шифрује кључем, па се на шифрован садржај и блок поруке примени XOR

Мултипликација блок шифре

- Једини начин на који се може повећати простор који разапиње кључ блок-шифре је процедура мултипликације шифре.
- Ради се о понављању шифре *n* пута, користећи *n* међусобно независних кључева.

- Очигледно је да се на овакав начин безбедност повећава, али не увек пропорционално дужини кључа. На пример, за DES, ефективна дужина кључа приближно износи

$$l = 56 \cdot \left\lceil \frac{n}{2} \right\rceil$$

бита, уместо 56n. Наиме, ако би n било једнако 3, дужина кључа би била 112 бита.

- Треба имати у виду такође да тако спрегнута шифра не сме да формира алгебарску групу. У том случају би две сукцесивне шифре са два различита кључа биле еквивалентне једној јединој шифри. Може се показати да ни DES ни Rijndael не чине алгебарску групу при мултипликацији.

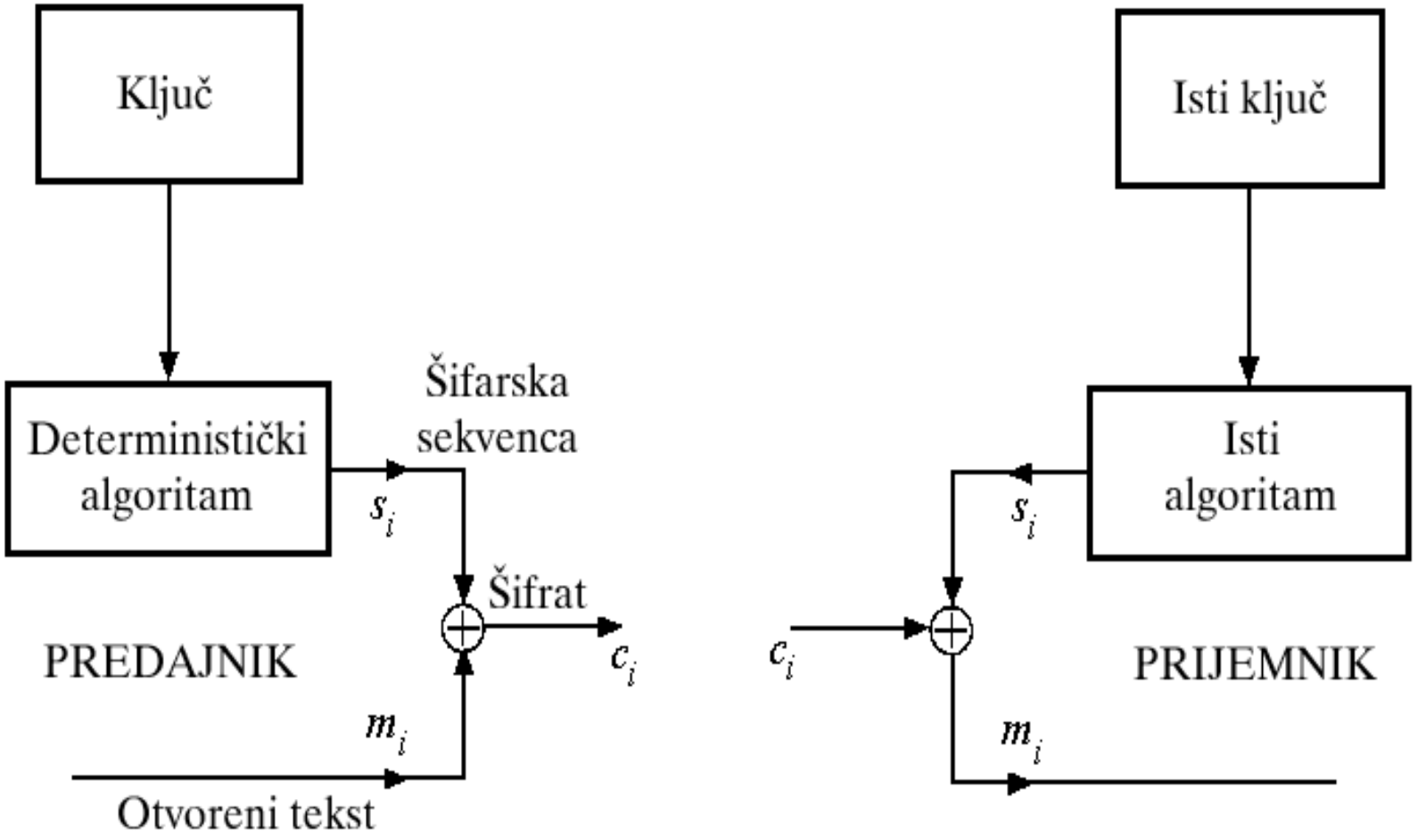
ПРОТОЧНЕ ШИФРЕ

Секвенцијални шифарски системи

- Генератори псеудослучајних бројева – детерминистички алгоритми, или низови симбола које они генеришу имају сличне особине као и случајни низови.
- Користе кратке кључеве ради започињања процеса генерисања.
- Излазни низ генератора се сабира по модулу 2 са низом отвореног текста и на тај начин се добија низ шифрата.

- Псеудослучајни низови су периодични у ширем смислу (што значи да могу имати апериодични почетак), али ако су периоди таквих низова много већи од дужина низова отвореног текста, систем ће се понашати на сличан начин као и Вернамова шифра.

Основна шема секвенцијалног шифарског система



- Захтеви које сваки шифарски низ мора да задовољи да би се могао користити у секвенцијалном шифарском систему:
  - **Период** – Период шифарског низа мора да буде бар једнаке дужине као и дужина низа који се шифрује. У пракси, генеришу се низови чији је период много редова величине већи од дужине низа који се шифрује.

- **Статистичке особине**:

  Ако је дат бинарни низ, серијом дужине *k* се назива низ сукцесивних *k* једнаких бита између различитих бита. На пример, у бинарном низу

  ...0100110100**111**011001**000**110101**000**1...

  Налазе се, између осталог, 2 серије нула (gaps) дужине 3 и једна серија јединица (block) исте дужине.

Проточне шифре

- Уобичајено шифрује поруку бајт по бајт, а може и бит по бит
- XOR се врши над поруком и излазом из генератора псеудослучајних бита (низ кључа)
- Пожељан је кључ од најмање 128 бита
- Није добро користити исти кључ више пута (код блоковских шифри то је могуће)

Пример секвенцијалног алгоритма: RC4

- RC4 алгоритам користи таблицу S-box дужине 256 бајтова.
- За генерисање случајног броја K треба урадити следеће:

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

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

  S_i и S_j замене места

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

  $K=S_t$
- Добијени бајт K се користи за XOR-овање са отвореним текстом за добијање шифрата.

Пример секвенцијалног алгоритма: RC4 (наставак)

- Иницијализација S-box је веома једноставна. Прво се линеарно напуни тако да је: $S_0=0$, ..., $S_{255}=255$,
- Затим се генерише низ од 256 бајтова кључа (понављањем),
- Тада се S-box попуњава на следећи начин:

  За i=0 до 255

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

  S_i и S_j замене места.