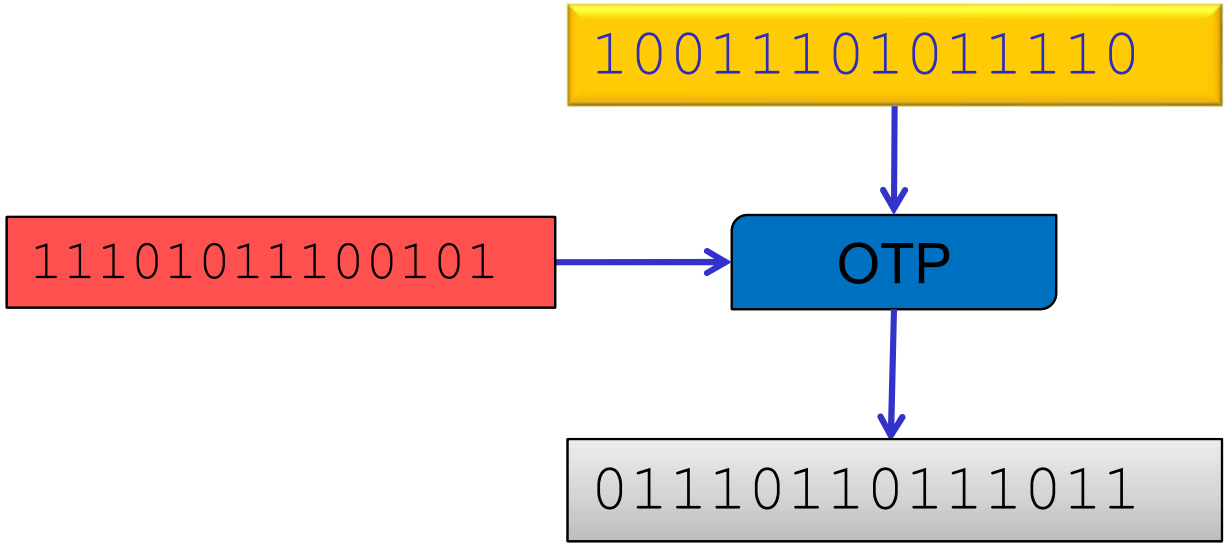
Simetrična enkripcija – definicija

- Neka su K, M i C konačni skupovi:
  - K - prostor ključeva,
  - M - prostor jasnih tekstova i
  - C - prostor skrivenih tekstova.
- Simetrična enkripcija je par algoritama E i D ($E: M \times K \to C$, $D: C \times K \to M$) gdje za svaki $k \in K$ i $m \in M$ vrijedi

$$D(E(m,k),k) = m.$$

Primjer: jednokratna bilježnica

- $M = K = C = \{0,1\}^n$
- $E(m,k) = m \oplus k$
- $D(c,k) = c \oplus k$



Sigurnost

- Neformalno:
  Simetrična enkripcija je sigurna ako je napadaču *jako teško* na temelju skrivenog teksta
  $$c = E(m, k)$$
  odrediti *bilo što* o jasnom tekstu M.

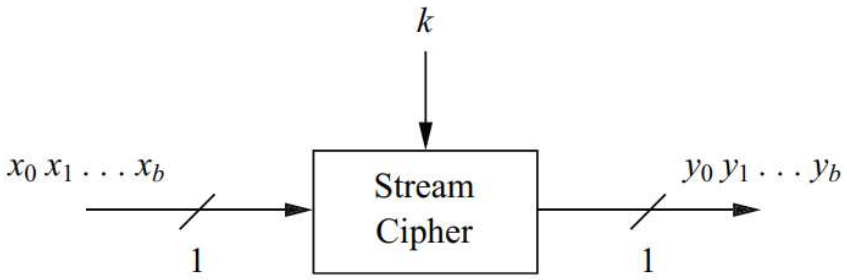
Različite vrste sigurnosti

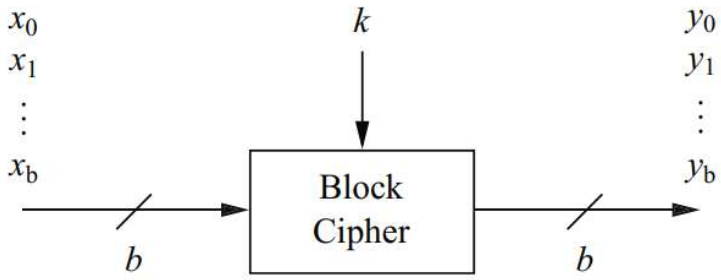
prema tome što napadač ima na raspolaganju:

- samo jedan skriveni tekst
- jedan par (m_i, c_i)
- puno parova (m_i, c_i) gdje je $c_i = E(m_i, k)$
  - Napad poznatim izvornim tekstom / *known plaintext attack*
- mogućnost da dobije $c_i = E(m_i, k)$ za m_i po izboru
  - Napad odabranim izvornim tekstom / *chosen plaintext attack*
- mogućnost da dobije $m_i = D(c_i, k)$ za c_i po izboru
  - Napad odabranim skrivenim tekstom / *chosen ciphertext attack*
- ...

Vrste simetrične enkripcije

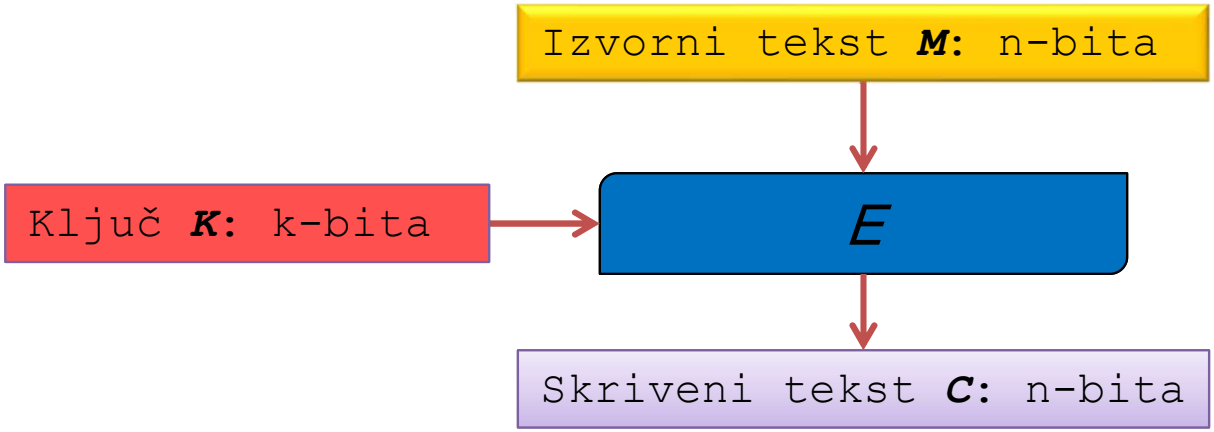
- Protočna enkripcija (*eng. stream cipher*) ili kriptiranje toka podataka
  - kriptira se jedan po jedan bit
- Sustavi kriptiranja bloka podataka (*eng. block cipher*)
  - kriptiraju se blokovi fiksne duljine





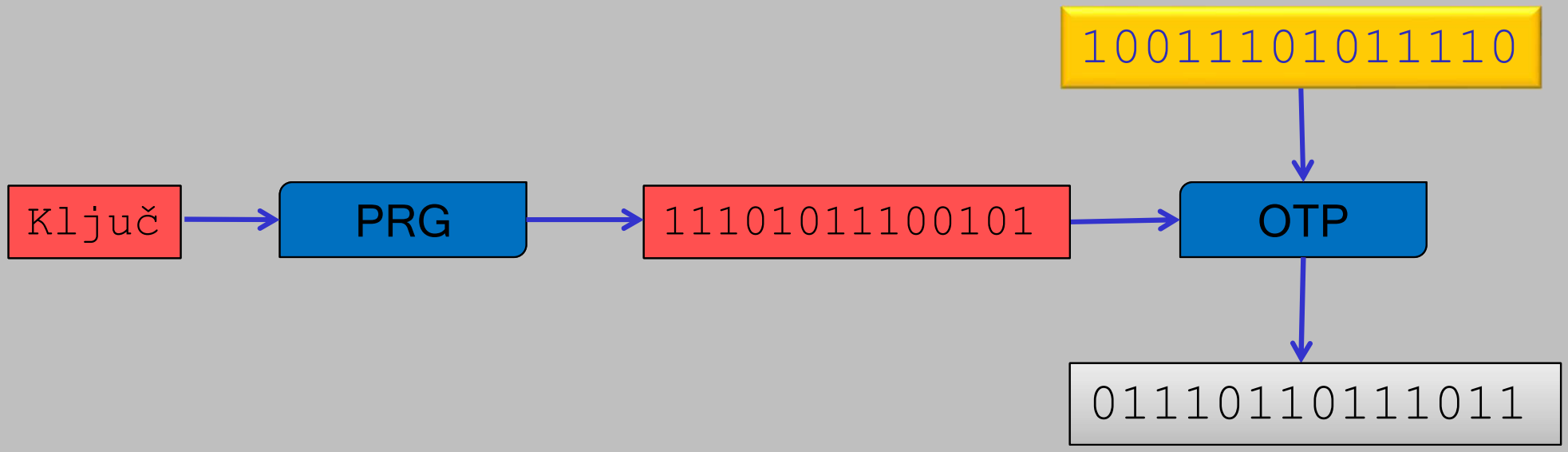
Sustav kriptiranja bloka

- $M = C = \{0,1\}^n$
- $K = \{0,1\}^k$
- E i D su deterministički algoritmi.



Sustav kriptiranja toka podataka

- Ideja: umjesto slučajnog ključa koristimo *pseudoslučajni ključ*.
- Generator pseudoslučajnih brojeva na temelju ključa generira niz bitova koji se XOR-a s izvornim tekstom.



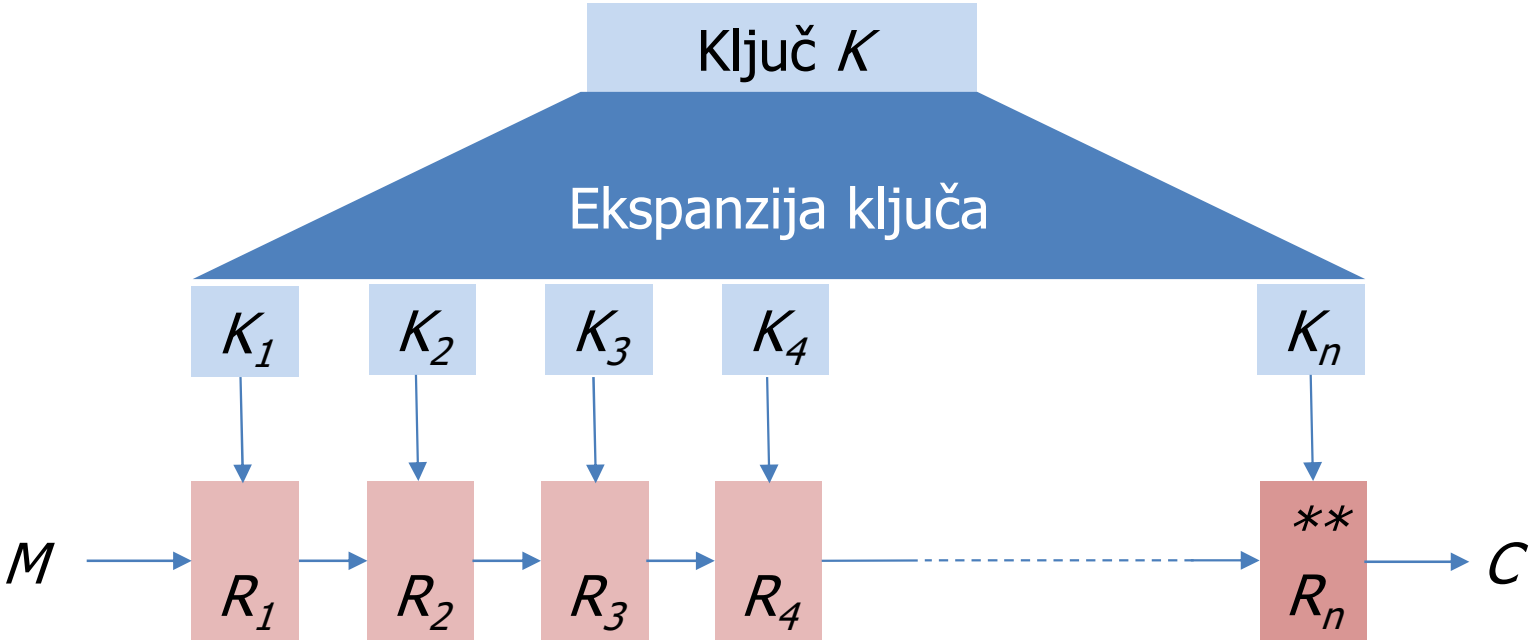
Primjeri sustava kriptiranja bloka

- DES (1970-te)
  - **n=64, k=56**, danas potpuno nesiguran zbog malog ključa
  - dugogodišnji standard, još uvijek se široko koristi
- 3DES, trostruki DES (1970-te)
  - **n=64, k=112 ili 168**
  - veća sigurnost s istim algoritmom kriptiranja
- IDEA (1991)
  - **n=64, k=128**
- Blowfish (1993)
  - **n=64, k=32–448**
- AES (1999)
  - **n=128 k=128, 192, 256**
  - standard od 2002., vrlo se široko koristi

Kako izgraditi sustav kriptiranja bloka?

- Upozorenje:
  - U ovom predmetu (kroz predavanja i vježbe) objašnjavamo kako iznutra rade ovakvi sustavi.
  - Osmišljavanje novih kriptografskih sustava nije jedan od predviđenih ishoda znanja!
  - Ispravna i sigurna implementacija kriptografskih sustava nije jedan od predviđenih ishoda znanja!
  - U praksi uvijek koristite dobro poznate sustave definirane standardima i implementirane u provjerenim bibliotekama!

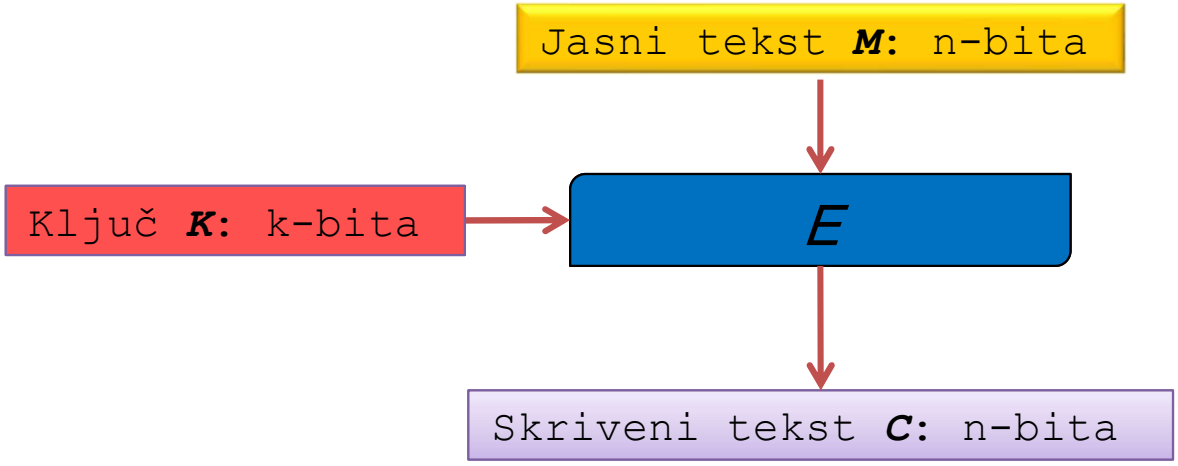
Koraci* algoritma kriptiranja bloka



* iteracije ili *runde*
** zadnji korak je kod nekih algoritama drugačiji

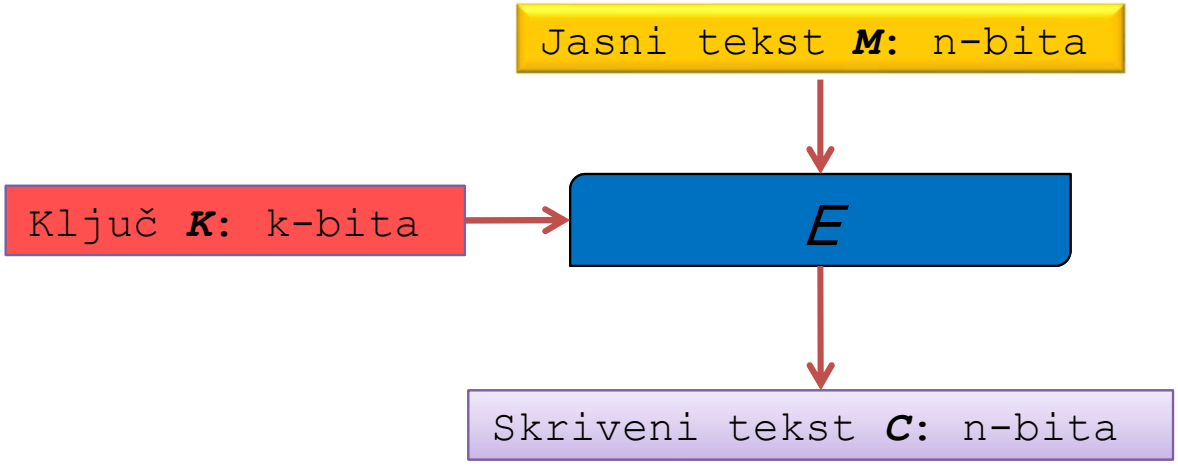
Shannonova načela

- **Difuzija**
  - svaki bit jasnog teksta kao i svaki bit tajnog ključa treba utjecati na mnogo bitova kriptiranog teksta
  - promjena samo jednog bita jasnog teksta mora uzrokovati promjenu (statistički) polovicu bitova kriptiranog teksta
  - ostvaruje se primjerice permutacijom i u više koraka algoritma



Shannonova načela

- **Konfuzija**
  - međuzavisnost kriptiranog i jasnog teksta je previše složena da bi se mogla iskoristiti za razbijanje kriptosustava
  - svaki bit kriptiranog teksta treba ovisiti o više bitova ključa ali tako da se pritom prikrije veza između njih
  - ostvaruje se primjerice supstitucijom, tj. supstitucijskim tablicama



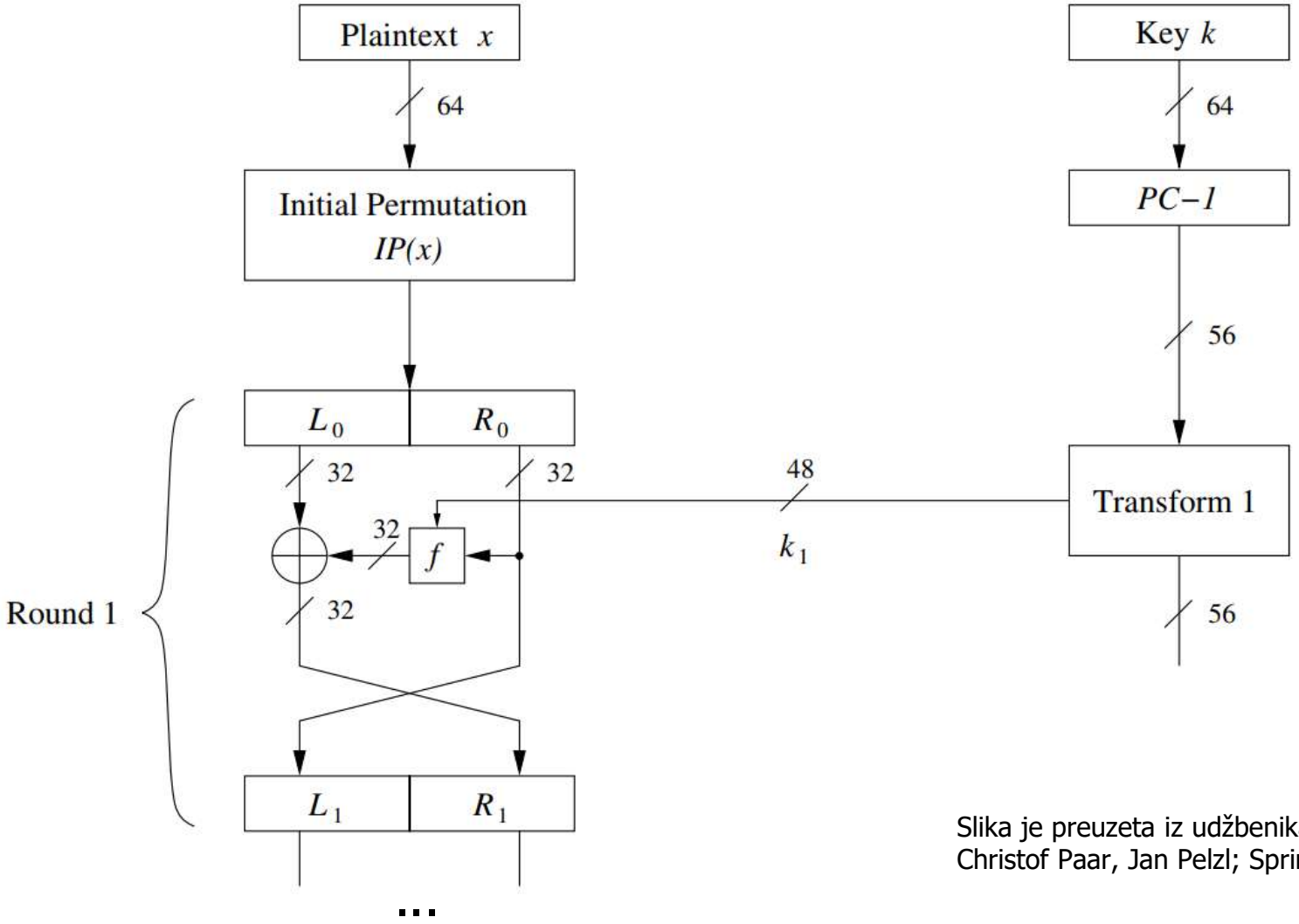
DES (Data Encryption Standard)

- veličina bloka: 64 bita
- veličina ključa: 56 bita
- struktura: Feistelova mreža
- razvijen u IBM-u, povijest:
  - Kasne **1960-te**: IBM razvija Lucifer
  - **1972**: US National Bureau of Standards (NBS) započinje proces standardizacije simetrične enkripcije
  - **1975**, **1976**: National Security Agency (NSA) predlaže određene promjene NBS-u, IBM-u
  - **1977**: NBS objavljuje Data Encryption Standard (FIPS PUB 46)
  - **1990**: Diferencijalna kriptoanaliza DES-a (neuspješna)
  - **1994**: Linearna kriptoanaliza DES-a (donekle uspješna)
  - **1990-te**: DES Challenges – napadi grubom silom na DES
  - **2002**: NIST (preimenovani NBS) objavljuje novi standard (AES)

DES (Data Encryption Standard)

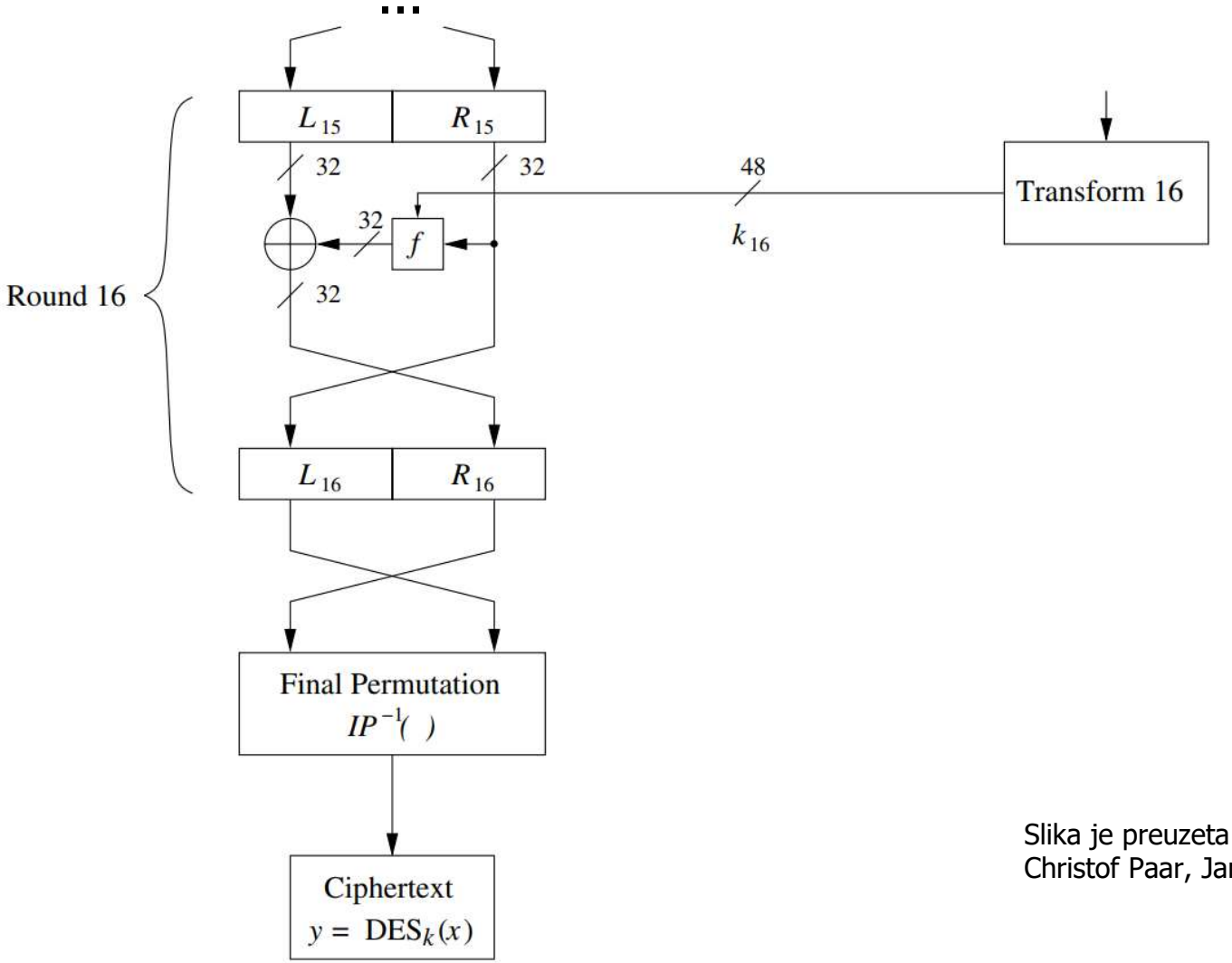
- nesiguran
  - 1998: "DES Challenge II" ostvareno računalo za $250.000 koje za manje od 3 dana razbija DES poruku (nagrada je bila $10.000)
- mala veličina ključa od 56 bita je najveći nedostatak koji se otklanja višestrukim kriptiranjem
  - utrostručeni (*triple*) DES (3DES) s ključem veličine
    - 112 (2x56) ili
    - 168 (3x56) bita
- unatoč svojoj *nesigurnosti* još uvijek se široko koristi

DES – Feistelova mreža



Slika je preuzeta iz udžbenika: ***Understanding Cryptography***, Christof Paar, Jan Pelzl; Springer-Verlag Berlin Heidelberg, 2009.

DES – Feistelova mreža



Slika je preuzeta iz udžbenika: ***Understanding Cryptography***, Christof Paar, Jan Pelzl; Springer-Verlag Berlin Heidelberg, 2009.

DES – postupak kriptiranja

- kriptiraju se blokove duljine 64 bita (8 bajtova)
- iz ključa *K* veličine 56 bita određuje se 16 podključeva *Ki* duljine 48 bita
- Postupak kriptiranja poruke *M* duljine 8 bajtova:
  - *L0 R0* = IP (*M*).
  - 16 koraka: $Li = Ri\text{-}1$

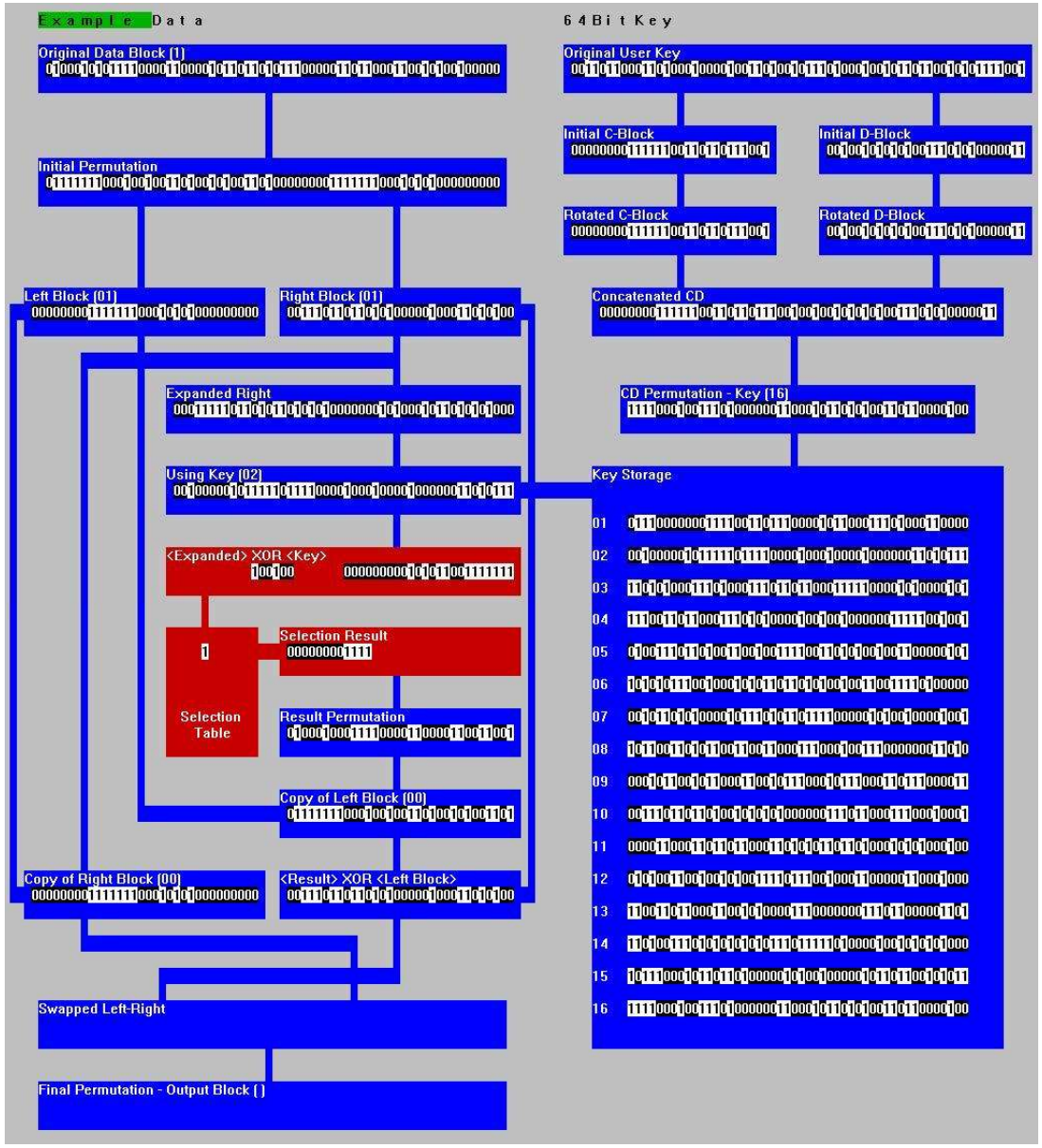
    $Ri = Li\text{-}1 \oplus f\,(\,Ri\text{-}1, Ki\,),$
- *f(Ri-1, Ki)* obavlja "preslagivanje" bitova u *Ri-1* ovisno o parametru *Ki*
- na kraju se obavlja inverzna permutacija od IP

  $C = IP^{-1}\,(\,R16\ L16\,).$

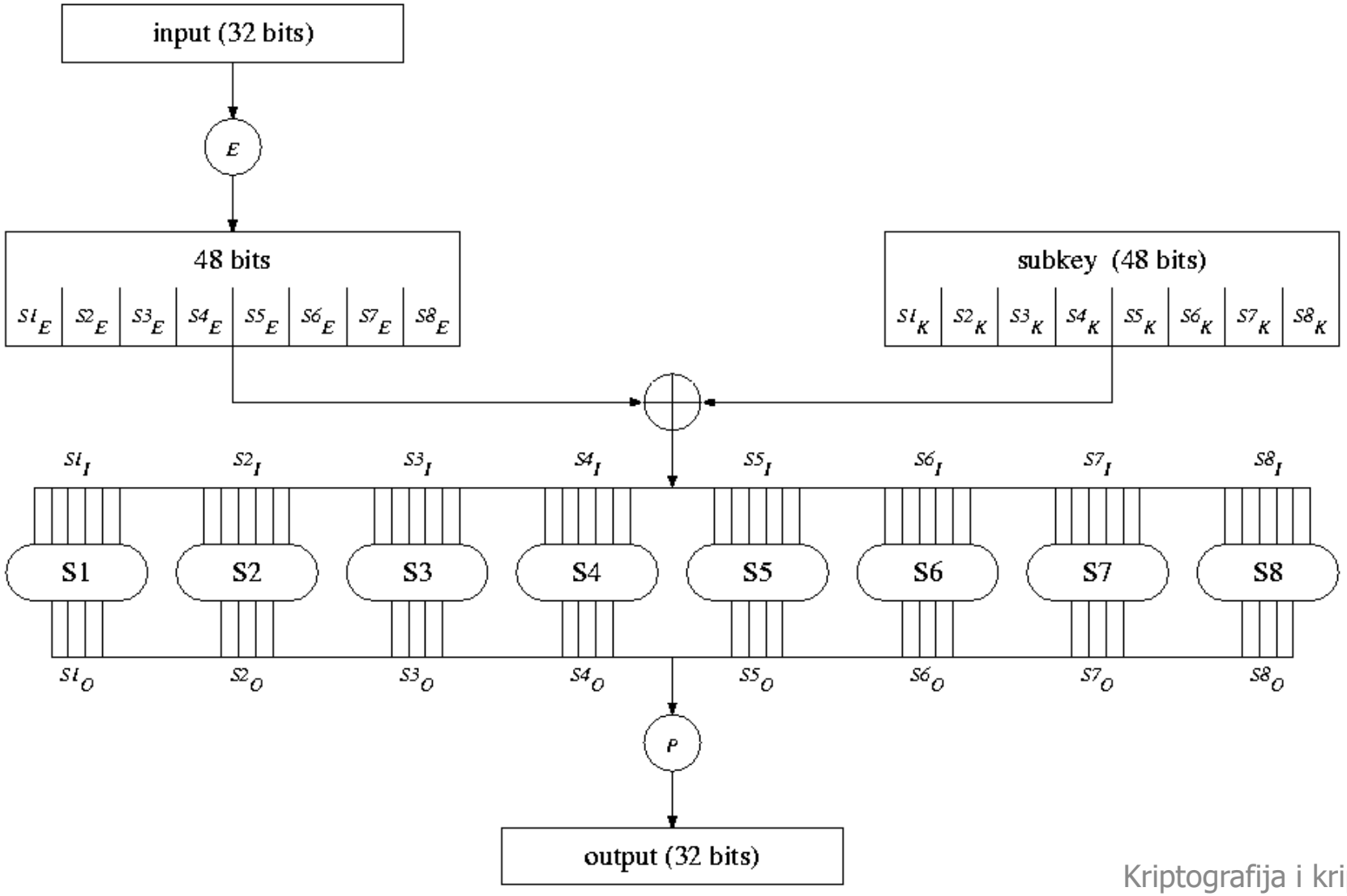
DES – detalji koji nisu jako bitni

- Permutacija IP nema utjecanja na sigurnost, nepoznato je zašto se koristi u DES-u.
- Ekspanzija ključa je jednostavna i nema velikog utjecaja na sigurnost.
  - Svaki podključ sadrži nekih 48 bitova ključa u nekom redoslijedu.
  - Svaki bit ključa se koristi u skoro svim rundama.

Simulacija kriptosustava DES



funkcija *f*


input (32 bits)
E
48 bits
S1E S2E S3E S4E S5E S6E S7E S8E
subkey (48 bits)
S1K S2K S3K S4K S5K S6K S7K S8K
S1I S2I S3I S4I S5I S6I S7I S8I
S1
S2
S3
S4
S5
S6
S7
S8
S1O S2O S3O S4O S5O S6O S7O S8O
P
output (32 bits)

Funkcija f

- Funkcija E proširi ulaz tako da ponovi neke bitove dva puta.
  - Ne igra bitnu ulogu u sigurnosti.
- Supstitucijske tablice zamijenjuju 6-bitne blokove 4-bitnim blokovima.
  - Kritična uloga u sigurnosti, treba ih pažljivo odabrati.
- Funkcija P permutira bitove.
  - Bitna za difuziju.

Supstitucijske tablice

- ulaz u S tablicu je veličine 6 bita, a izlaz 4 bita
- supstitucijska tablica S1:

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

- prvi i zadnji bit svakog dijela ulaza predstavlja adresu retka
- srednja četiri bita određuju adresu stupca u tablici selekcije
- nakon primjene 8 supstitucijskih tablica od ulaznih 48 bita dobivamo 32 bita nakon supstitucije

Važne činjenice o supstitucijskim tablicama

- Kritične za sigurnost DES-a!
- Jedini nelinearni dio sustava.
- Kada bi supstitucijske tablice bile nasumično odabrane, sustav bi bio potpuno nesiguran.

Dizajn supstitucijskih tablica za DES

(S-1) Each S-box has six bits of input and four bits of output. (This was the largest size that we could accommodate and still fit all of DES onto a single chip in 1974 technology.)

(S-2) No output bit of an S-box should be too close to a linear function of the input bits. (That is, if we select any output bit position and any subset of the six input bit positions, the fraction of inputs for which this output bit equals the XOR of these input bits should not be close to 0 or 1, but rather should be near 1/2.)

(S-3) If we fix the leftmost and rightmost input bits of the S-box and vary the four middle bits, each possible 4-bit output is attained exactly once as the middle four input bits range over their 16 possibilities.

(S-4) If two inputs to an S-box differ in exactly one bit, the outputs must differ in at least two bits. (That is, if $|\Delta I_{i,j}| = 1$, then $|\Delta O_{i,j}| \geq 2$, where $|x|$ is the number of 1-bits in the quantity x.)

(S-5) If two inputs to an S-box differ in the two middle bits exactly, the outputs must differ in at least two bits. (If $\Delta I_{i,j} = \mathbf{001100}$, then $|\Delta O_{i,j}| \geq 2$.)

(S-6) If two inputs to an S-box differ in their first two bits and are identical in their last two bits, the two outputs must not be the same. (If $\Delta I_{i,j} = \mathbf{11xy00}$, where **x** and **y** are arbitrary bits, then $\Delta O_{i,j} \neq 0$.)

(S-7) For any nonzero 6-bit difference between inputs, $\Delta I_{i,j}$, no more than eight of the 32 pairs of inputs exhibiting $\Delta I_{i,j}$ may result in the same output difference $\Delta O_{i,j}$.

(S-8) Similar to (S-7), but with stronger restrictions in the case $\Delta O_{i,j} = 0$, for the case of three active S-boxes on round i. See the discussion below.

Izvor: D. Coppersmith, Data Encryption Standard (DES) and its strength against attacks, 1994

Svojstva Feistelove mreže

- Kako dekriptirati?

- Kriptiranje je invertibilno bez obzira na svojstva funkcije f.
- Isti sklop se može koristiti za kriptiranje i za dekriptiranje.
- Sigurnost ovisi o funkciji f, sve ostalo su XOR operacija i permutacije bitova.

DES: kriptiranje i dekriptiranje

```
generiraj_podključeve ( ključ, K [16] )
za svaki blok čini
   p = perm_IP ( blok [j] )
   L1 = p [1:32]      // lijevih 32 bita bloka
   R1 = p [33:64]     // desnih 32 bita bloka
   za i = 1 do 16 čini
        Li+1 = Ri
        Ri+1 = Li ⊕ f ( Ri, Ki ) // kriptiranje
        Ri+1 = Li ⊕ f ( Ri, K16-i+1 ) // dekriptiranje
   q [1:32] = R16
   q [33:64] = L16
   kriptirani_blok = perm_IP-1 ( q )
kraj
```

Zadatak: DES-bez-S

- Sustav DES-bez-S je identičan DES-u osim što nema S-tablice.
- Zadano je nekoliko stotina parova M_i, $C_i = DES\text{–bez–S}(M_i, K)$, odredite ključ K.

Utrostručeni DES, 3DES

$3DES(M, K1, K2, K3) = DES(DES^{-1}(DES(M, K1), K2), K3)$

$3DES^{-1}(C, K1, K2, K3) = DES^{-1}(DES(DES^{-1}(C, K3), K2), K1)$

- veličine ključeva:
  - varijanta ključa 1: tri nezavisna ključa K1, K2 i K3 $\Rightarrow$ 3x56=168 bitova
  - varijanta ključa 2: dva nezavisna ključa K1=K3 i K2 $\Rightarrow$ 2x56=112 bitova
- nedozvoljene varijante ključa:
  - varijanta ključa 3: K1=K2=K3 (to je zapravo DES)
  - K1=K2 (i to je zapravo DES jer se koristi samo jedan ključ K3)
  - K2=K3 (i to je zapravo DES jer se koristi samo jedan ključ K1)

Zašto se ne koristi 2DES?

Zbog napada *susret u sredini* (*eng. Meet-in-the-middle attack*).

$$C = 2DES\,(M, K1, K2) = DES\,(DES\,(M, K1), K2)$$

Složenost napada grubom silom za poznati par (M,C)

2^{56} mogućnosti: $C' = DES\,(M, K1i)$, $i=1,2, \ldots 2^{56}$

2^{56} mogućnosti: $M' = DES^{-1}\,(C, K2i)$, $i=1,2, \ldots 2^{56}$

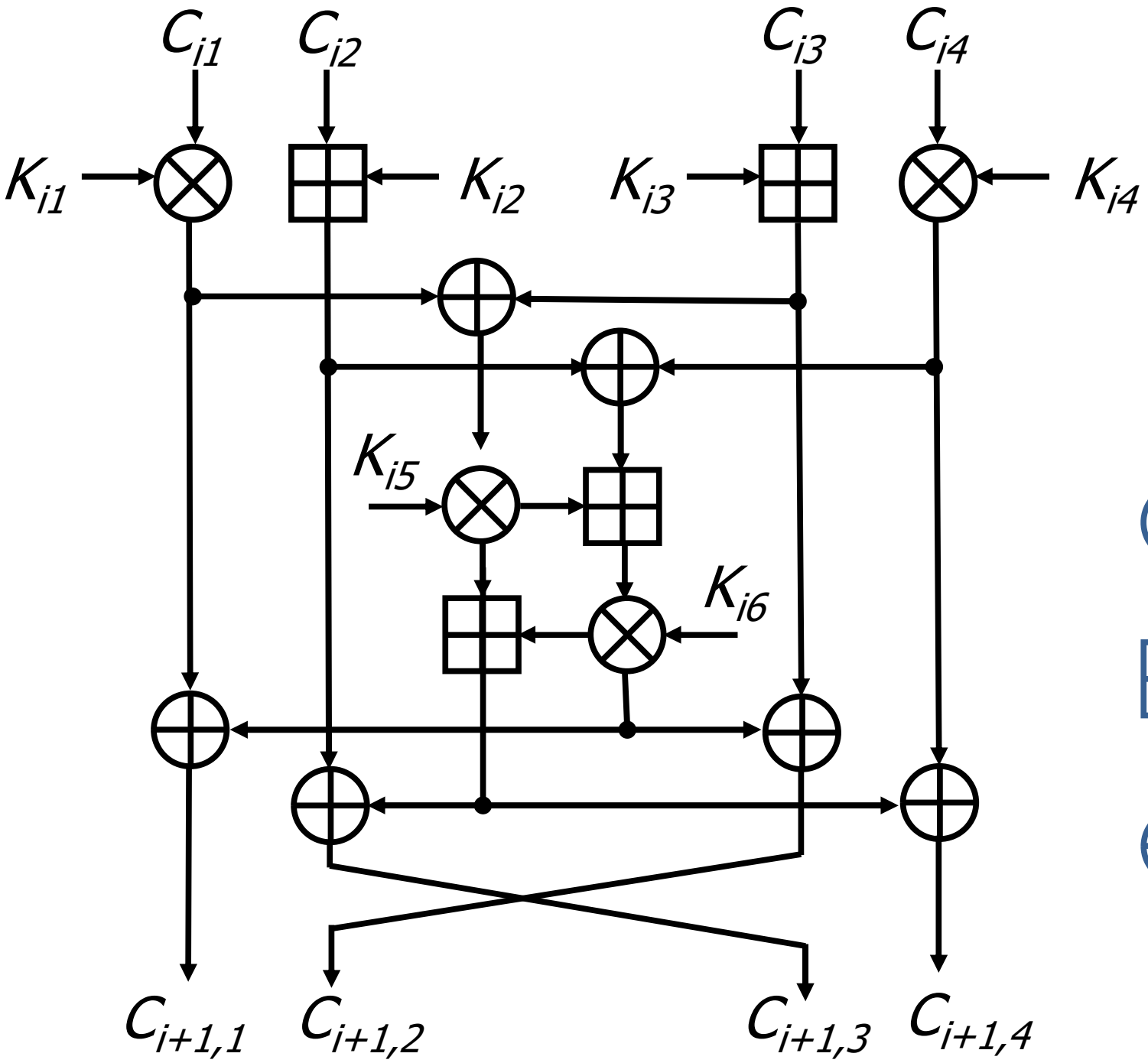
Ako je $M' = C'$ tada smo pronašli par ključeva *K1* i *K2*

$\Rightarrow$ složenost $2 \cdot 2^{56} = 2^{57}$, a ne 2^{112}!

IDEA (*Internatonal Data Encription Algorithm*)

- dovršen 1992., siguran
- ključ je duljine 128 bita
- blokovi duljine 64 bita dijele se na 4 podbloka (16 b)
- postupak kriptiranja se provodi u 9 koraka
  - u svakom od prvih 8 koraka sudjeluju:
    4 podbloka i 6 podključeva duljine 16 bita
  - u devetom koraku se koriste 4 podključa
- dakle, iz ključa K je potrebno generirati 8x6+4=52 podključeva

Prvih osam koraka algoritma IDEA

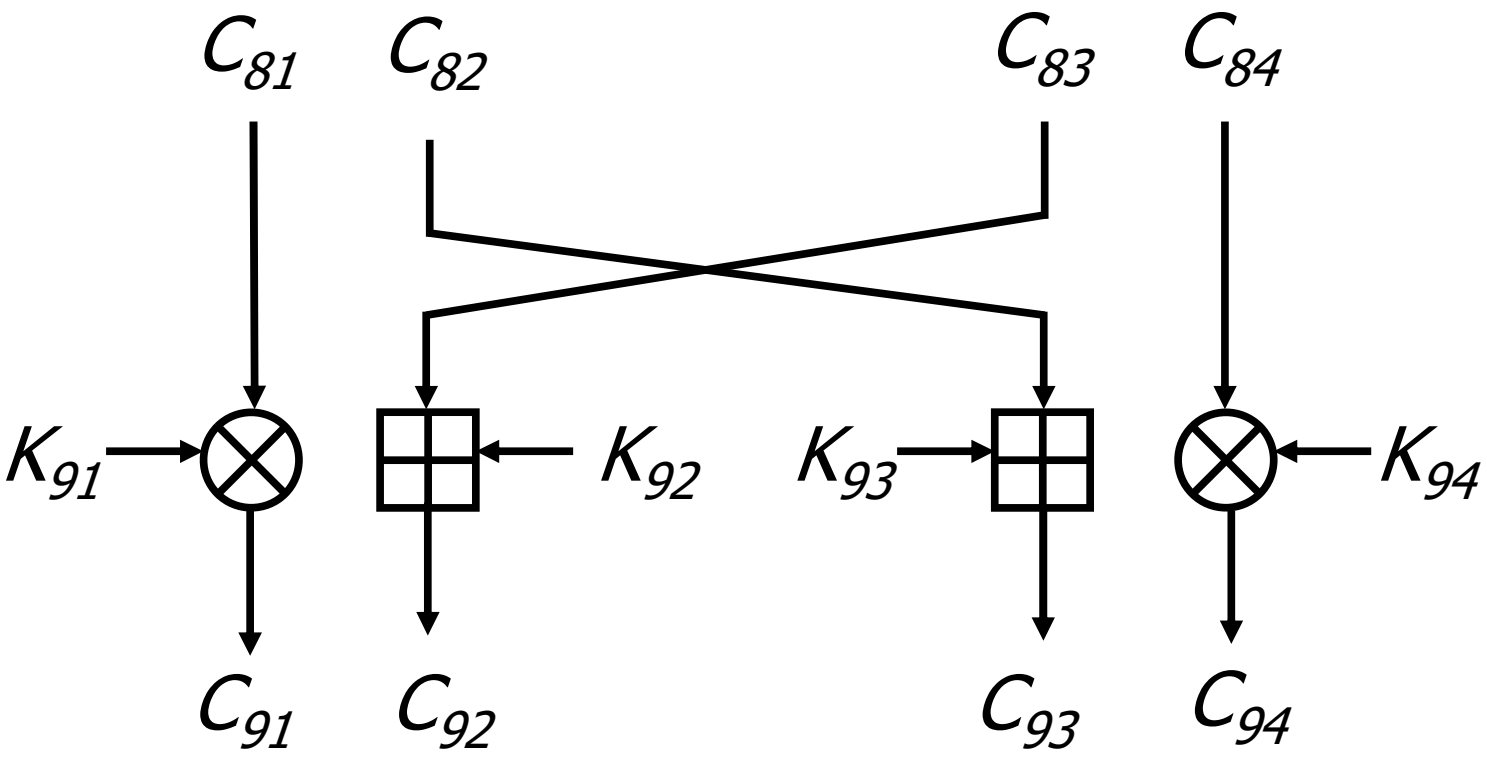


množenje po modulu $2^{16}+1$

zbrajanje po modulu 2^{16}

XOR bit po bit

Deveti korak algoritma IDEA



množenje po modulu $2^{16}+1$

zbrajanje po modulu 2^{16}