

### 3. poglavje

## **Simetrični kriptosistemi**

- Bločne šifre, nekaj zgodovine, DES, AES
- Iterativne šifre, zmenjalno-permutacijske mreže
- Produktna šifra in Fiestelova šifra
- Opis šifer DES in AES
- Načini delovanja (ECB, CBC, CFB, OFB) in MAC
- Napadi in velika števila
- 3-DES, DESX in drugi sistemi

## Bločne šifre

**Bločna šifra** je simetrična šifra, ki razdeli čistopis na bloke fiksne dolžine (npr. 128 bitov), in šifrira vsak blok posamično (kontrast: *tekoča šifra* zašifrira čistopis po znakih – ponavadi celo po bitih).

Najmodernejše bločne šifre so **produktne šifre**, ki smo jih spoznali v prejšnjem poglavju: komponiranje več enostavnih operacij, katere (vsaka posebej) niso dovolj varne, z namenom, da povečamo varnost: *transpozicije, ekskluzivni ali (XOR), tabele, linearne transformacije, aritmetične operacije, modularno množenje, enostavne substitucije.*

Primeri bločnih produktnih šifer: DES, AES, IDEA.

## Nekatere zelene lastnosti bločnih šifer

### Varnost:

- **razpršitev**: vsak bit tajnopisa naj bo odvisen od vseh bitov čistopisa.
- **zmeda**: zveza med ključem ter biti tajnopisa naj bo zapletena,
- **velikost ključev**: mora biti majhna, toda dovolj velika da prepreči požrešno iskanje ključa.

### Učinkovitost

- hitro šifriranje in odšifriranje,
- enostavnost (za lažjo implementacijo in analizo),
- primernost za hardware ali software.

## Kratka zgodovina bločnih šifer DES in AES

Konec 1960-ih: IBM – Feistelova šifra in LUCIFER.

1972: NBS (sedaj NIST) izbira simetrično šifro za zaščito računalniških podatkov.

1974: IBM razvije DES, 1975: NSA ga “popravi”.

1977: DES sprejet kot US Federal Information Processing Standard (FIPS 46).

1981: DES sprejet kot US bančni standard (ANSI X3.92).

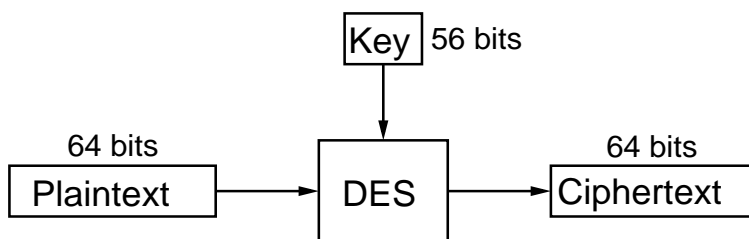
1997: AES (Advanced Encryption Standard) izbor

1999: izbranih 5 finalistov za AES

## National Security Agency (NSA)

- [www.nsa.gov](http://www.nsa.gov)
- ustanovljena leta 1952,
- neznana sredstva in število zaposlenih (čez 100.000?)
- Signals Intelligence (SIGINT):  
pridobiva tuje informacije.
- Information Systems Security (INFOSEC):  
ščiti vse občutljive (classified) informacije,  
ki jih hrani ali pošilja vlada ZDA,
- zelo vplivna pri določanju izvoznih regulacij ZDA za  
kriptografske produkte (še posebej šifriranje).

## Data Encryption Standard (DES)



Ideja za DES je bila zasnovana pri IBM-u v 60-ih letih (uporabili so koncept Claude Shannon-a imenovan *Lucifer*).

NSA je zreducirala dolžino ključev z 128 bitov na 56.

V sredini 70-ih let je postal prvi komercialni algoritem, ki je bil objavljen z vsemi podrobnostmi (FIPS 46-2).

## Advanced Encryption Standard

AES je ime za nov FIPS-ov simetrični (bločni) kriptosistem, ki bo nadomestil DES.

Leta 2000 je zanj *National Institute of Standards and Technology (NIST)* izbral belgijsko bločno šifro **Rijndael**.

Dolžina *ključev* oziroma blokov je 128, 192 ali 256

Uporabljala pa ga bo ameriška vlada, glej

<http://csrc.nist.gov/encryption/aes/round2/r2report.pdf>.

Običajno uporabljamo **iterativne šifre**.

Tipični opis:

- krožna funkcija,
- razpored ključev,
- šifriranje skozi  $N_r$  podobnih krogov.

Naj bo  $K$  naključni binarni ključ določene dolžine.

$K$  uporabimo za konstrukcijo podključev za vsak krog s pomočjo *javno* znanega algoritma.

Imenujemo jih **krožni ključi**:  $K^1, \dots, K^{N_r}$ .

Seznamu krožnih ključev  $(K^1, \dots, K^{N_r})$  pa pravimo **razpored ključev**.



**Krožna funkcija**  $g$  ima dva argumenta:

(i) krožni ključ ( $K^r$ ) in (ii) *tekoče stanje* ( $w^{r-1}$ ).

Naslednje stanje je definirano z  $w^r = g(w^{r-1}, K^r)$ .

Začetno stanje,  $w_0$ , naj bo čistopis  $x$ .

Potem za tajnopis,  $y$ , vzamemo stanje po  $N_r$  krogih:

$$y = g(g(\dots g(g(x, K^1), K^2) \dots, K^{N_r-1})K^{N_r}).$$

Da je odšifriranje možno, mora biti funkcija  $g$  injektivna za vsak fiksni ključ  $K_i$ , tj.  $\exists g^{-1}$ , da je:

$$g^{-1}(g(w, K), K) = w, \quad \text{za vse } w \text{ in } K.$$

Odšifriranje opravljeno po naslednjem postopku:

$$x = g^{-1}(g^{-1}(\dots g^{-1}(g^{-1}(y, K^{N_r}), K^{N_r-1}) \dots, K^2)K^1).$$

## Zamenjalno-permutacijske mreže

(angl. *substitution-permutation network* – (**SPN**)).

Čistopis  $\mathcal{P}$  in tajnopis  $\mathcal{C}$  so binarni vektorji dolžine  $\ell m$ ,  $\ell, m \in \mathbb{N}$  (tj.  $\ell m$  je dolžina bloka).

SPN je zgrajen iz dveh komponent (zamenjave in permutacije):

$$\begin{aligned}\pi_S &: \{0, 1\}^\ell \longrightarrow \{0, 1\}^\ell, \\ \pi_P &: \{0, \dots, \ell m\} \longrightarrow \{0, \dots, \ell m\}.\end{aligned}$$

Permutacijo  $\pi_S$  imenujemo **S-škatla** in z njo zamenjamo  $\ell$  bitov z drugimi  $\ell$  biti.

Permutacija  $\pi_P$  pa permutira  $\ell m$  bitov.

Naj bo  $x = (x_1, \dots, x_{\ell m})$  binarno zaporedje, ki ga lahko smatramo za spoj  $m$   $\ell$ -bitnih podzaporedij označenih z  $x_{(1)}, \dots, x_{(m)}$ .

SPN ima  $N_r$  krogov, v vsakem (razen zadnjem, ki je bistveno drugačen) opravimo  $m$  zamenjav z  $\pi_S$  in nato uporabimo še  $\pi_P$ . Pred vsako zamenjavo vključimo krožni ključ z XOR operacijo.

### **SPN šifra**

$\ell, m, N_r \in \mathbb{N}$ ,  $\pi_S$  in  $\pi_P$  permutaciji,  $\mathcal{P} = \mathcal{C} = \{0, 1\}^{\ell m}$   
in  $\mathcal{K} \subseteq (\{0, 1\}^{\ell m})^{N_r+1}$ , ki se sestoji iz vseh možnih  
razporedov ključev izpeljanih iz ključa  $K$  z uporabo  
algoritma za generiranje razporeda ključev.

Šifriramo z algoritmom SPN.

**Alg.** :  $SPN(x, \pi_S, \pi_P, (K^1, \dots, K^{N_r+1}))$

$w^0 := x$

**for**  $r := 1$  **to**  $N_r - 1$  **do** (*krožno mešanje ključev*)

$u^r := w^{r-1} \oplus K^r$

**for**  $i := 1$  **to**  $m$  **do**  $v_{(i)}^r := \pi_S(u_{(i)}^r)$

$w^r := (v_{\pi_P(1)}^r, \dots, v_{\pi_P(\ell m)}^r)$

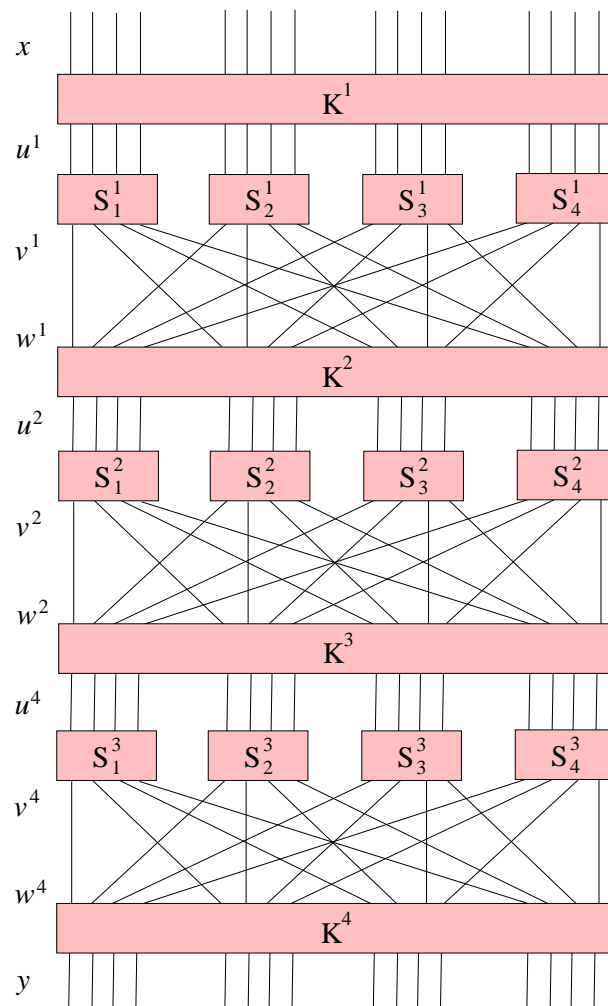
(*zadnji krog*)

$u^{N_r} := w^{N_r-1} \oplus K^{N_r}$

**for**  $i := 1$  **to**  $m$  **do**  $v_{(i)}^{N_r} := \pi_S(u_{(i)}^{N_r+1})$

$y := v^{N_r} \oplus K^{N_r+1}$

**output** ( $y$ )



Primer: naj bo  $\ell = m = N_r = 4$ , permutaciji  $\pi_S$  in  $\pi_P$  pa podani s tabelami:

$z$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

ter

$z$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\pi_P(z)$	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

Naj bo ključ  $K = (k_1, \dots, k_{32}) \in \{0, 1\}^{32}$  definiran z

$$K = 0011\ 1010\ 1001\ 0100\ 1101\ 0110\ 0011\ 1111,$$

sedaj pa izberimo še razpored ključev tako, da je za  $1 \leq r \leq 5$ , krožni ključ  $K^r$  izbran kot 16 zaporednih bitov ključa  $K$  z začetkom pri  $k_{4r-3}$ :

$$K^1 = 0011\ 1010\ 1001\ 0100$$

$$K^2 = 1010\ 1001\ 0100\ 1101$$

$$K^3 = 1001\ 0100\ 1101\ 0110$$

$$K^4 = 0100\ 1101\ 0110\ 0011$$

$$K^5 = 1101\ 0110\ 0011\ 1111$$

Potem šifriranje čistopisa

$$x = 0010\ 0110\ 1011\ 0111$$

poteka v naslednjem vrstnem redu.

$$\begin{array}{ll} w^0 = 0010\ 0110\ 1011\ 0111, & K^1 = 0011\ 1010\ 1001\ 0100 \\ u^1 = 0001\ 1100\ 0010\ 0011, & v^1 = 0100\ 0101\ 1101\ 0001 \\ w^1 = 0010\ 1110\ 0000\ 0111, & K^2 = 1010\ 1001\ 0100\ 1101 \\ u^2 = 1000\ 0111\ 0100\ 1010, & v^2 = 0011\ 1000\ 0010\ 0110 \\ w^2 = 0100\ 0001\ 1011\ 1000, & K^3 = 1001\ 0100\ 1101\ 0110 \\ u^3 = 1101\ 0101\ 0110\ 1110, & v^3 = 1001\ 1111\ 1011\ 0000 \\ w^3 = 1110\ 0100\ 0110\ 1110, & K^4 = 0100\ 1101\ 0110\ 0011 \\ u^4 = 1010\ 1001\ 0000\ 1101, & v^4 = 0110\ 1010\ 1110\ 1001 \\ K^5 = 1101\ 0110\ 0011\ 1111, & y = 1011\ 1100\ 1101\ 0110 \end{array}$$



Možno so številne variacije SPN šifer.

Na primer, namesto ene S-škatle lahko uporabimo različne škatle. To lahko vidimo pri DES-u, ki uporabi 8 različnih škatel.

Zopet druga možnost je uporabiti obrnljive linearne transformacije, kot zamenjavo za permutacije ali pa samo dodatek. Tak primer je AES.

## Feistelova šifra

**Feistelova šifra:**  $r$  krogov (rund)

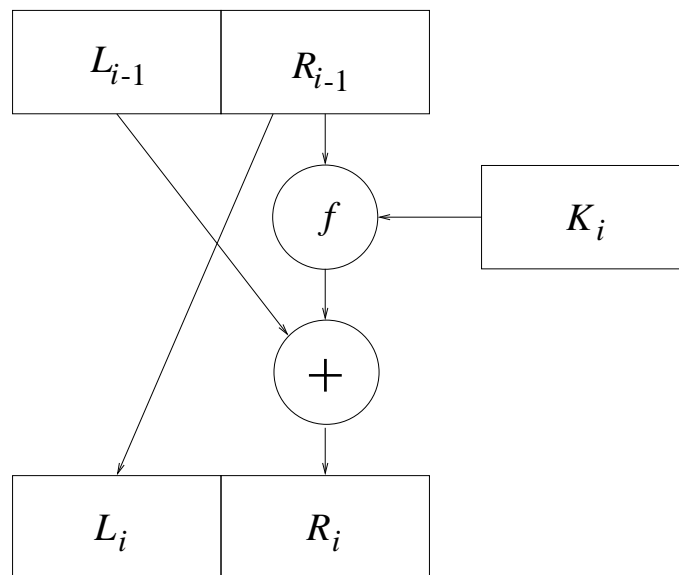
$$(L_{i-1}, R_{i-1}) \xrightarrow{K_i} (L_i, R_i).$$

kjer je  $L_i = R_{i-1}$  in  $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ ,  
in smo podključke  $K_i$  dobili iz osnovnega ključa  $K$ .

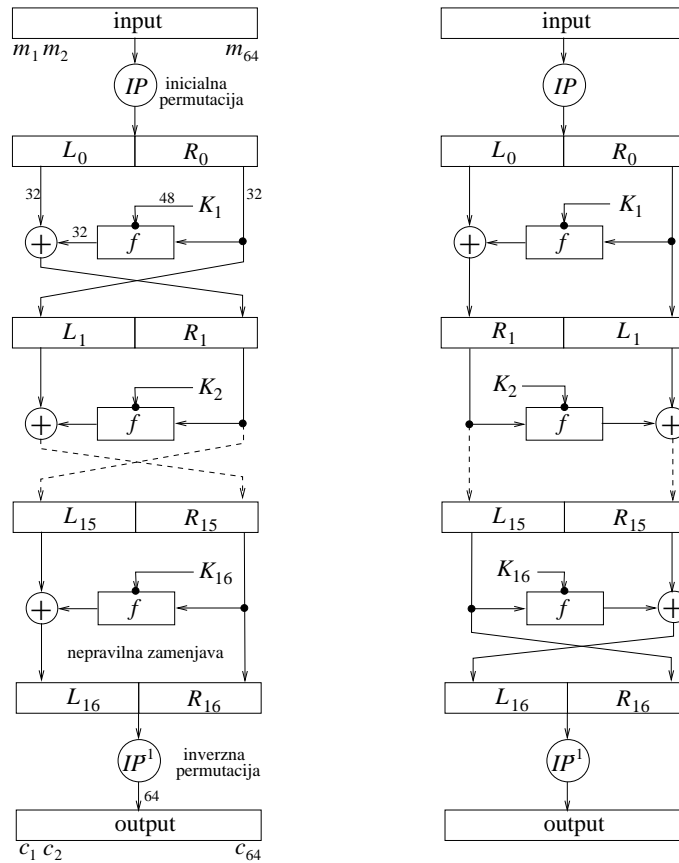
Končamo z  $(R_r, L_r)$  (in ne z  $(L_r, R_r)$ ), zato je šifriranje  
enako odšifriranju, le da ključke uporabimo v obratnem  
vrstnem redu.

Funkcija  $f$  je lahko produktna šifra in ni nujno  
obrnjljiva.

## En krog



## Opis šifre DES



## DES-ove konstante

začetna in končna permutacija:  $IP, IP^{-1}$

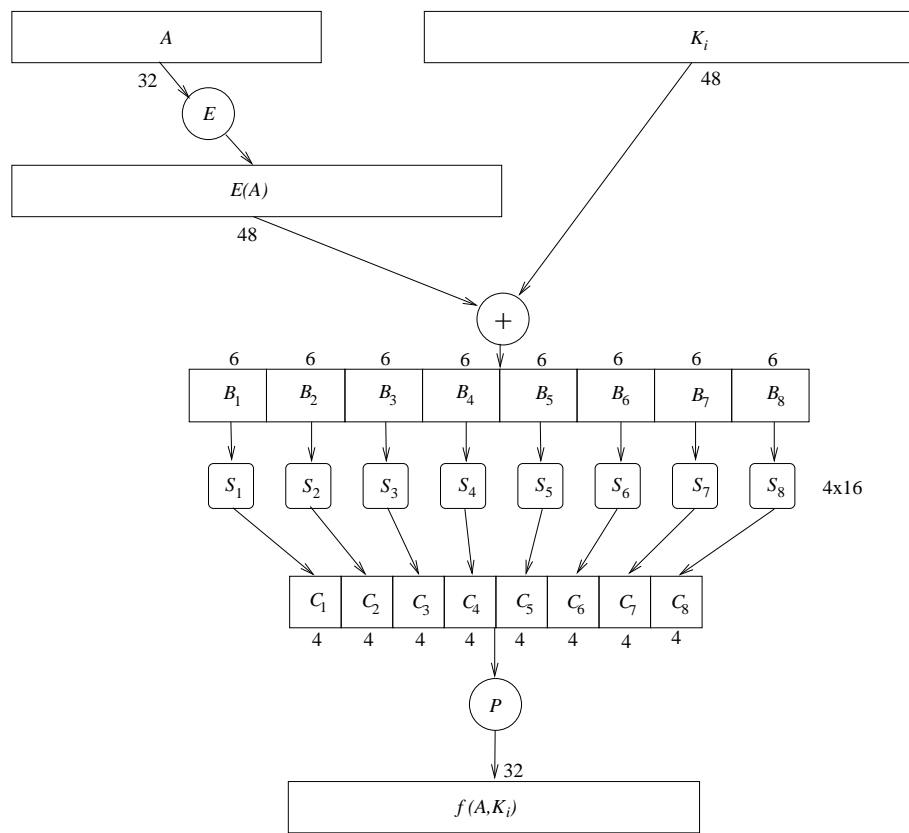
razširitev:  $E$  (nekatero bite ponovimo), permutacija  $P$

$S$ -škatle:  $S_1, S_2, \dots, S_8$

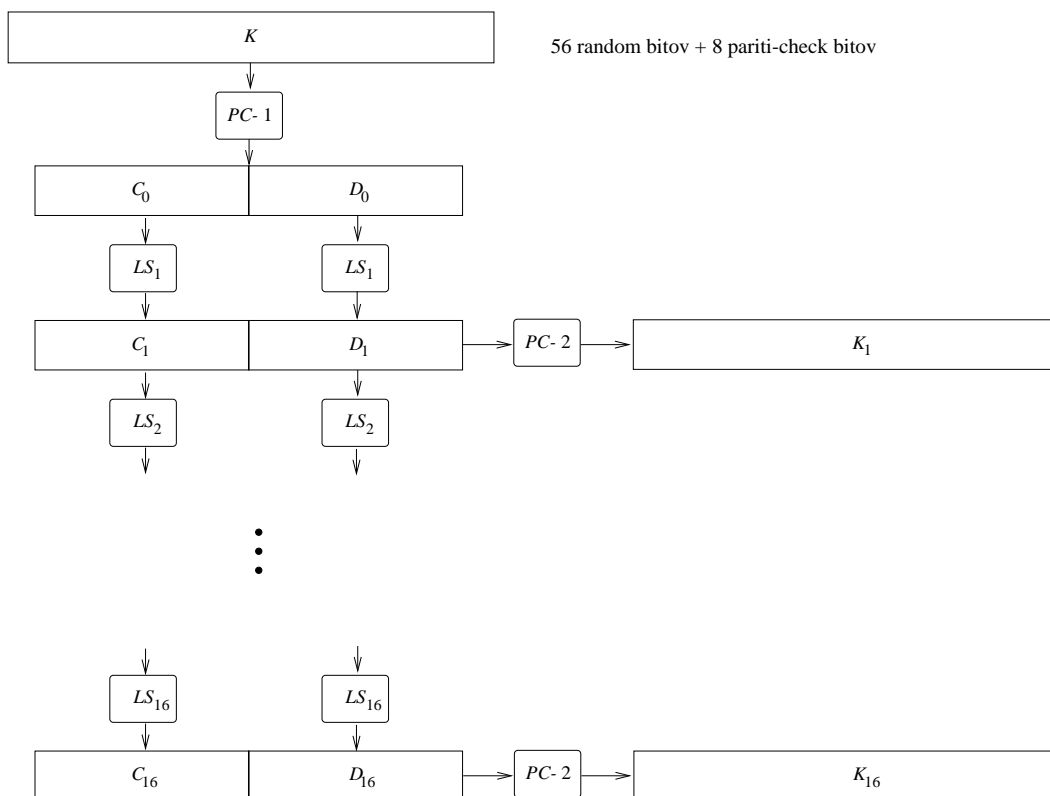
(tabele:  $4 \times 16$ , z elementi  $0 - 15$ )

permutacije za gen. podključev:  $PC - 1, PC - 2$

## DES-ova funkcija



## Računanje DES-ovih ključev



20 let je DES predstavljal delovnega konja kriptografije (bločnih šifer).

- do leta 1991 je NBS sprejel 45 hardwarskih implementacij za DES
- geslo (PIN) za bankomat (ATM)
- ZDA (Dept. of Energy, Justice Dept., Federal Reserve System)