Teorija kodiranja in kriptografija 2013/2014

Bločne šifre

Arjana Žitnik

Univerza v Ljubljani, Fakulteta za matematiko in fiziko

Ljubljana, 11. 3. 2014

Vsebina

- Splošne bločne šifre
- Sestavljeni kriptosistemi
- Iterativne šifre (SPN omrežja, Feistelove šifre)
- DES

Bločne šifre

Kripotsistem $(\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ je **bločna šifra dolžine** n, če je $\mathcal{B} = \mathcal{C} = \Sigma^n$, kjer je Σ končna abeceda.

Izrek

1. *Pri bločni šifri dolžine n je vsaka kodirna funkcija E_e neka permutacija množice Σ^n.*
2. *Če je d dekodirni ključ, ki pripada e, je $D_d = E_e^{-1}$.*

Zato lahko pri bločnih šifrah vzamemo, da je

$$\mathcal{K} \subseteq S(\Sigma^n),$$
$$E_\pi(x) = \pi(x),$$
$$D_\pi(x) = \pi^{-1}(x).$$

Dokaz izreka.

(1a) Vemo: v vsakem kriptosistemu je vsaka kodirna funkcija injektivna.

(1b) $E_e : \Sigma^n \to \Sigma^n$ je injektivna
Σ^n je končna množica, torej je E_e bijektivna

(2)

$$
\begin{aligned}
& D_d(E_e(b)) = b \quad \text{za vse} \quad b \in \Sigma^n \\
\text{prav tako je} \quad & E_e^{-1}(E_e(b)) = b \quad \text{za vse} \quad b \in \Sigma^n \\
\Longrightarrow \quad & D_d \ \text{in} \ E_e^{-1} \ \text{se ujemata na zalogi vrednosti} \ E_e \\
\Longrightarrow \quad & D_d \ \text{in} \ E_e^{-1} \ \text{se ujemata na} \ \Sigma^n \\
\Longrightarrow \quad & D^d = E_e^{-1}.
\end{aligned}
$$

Zgled: afina bločna šifra

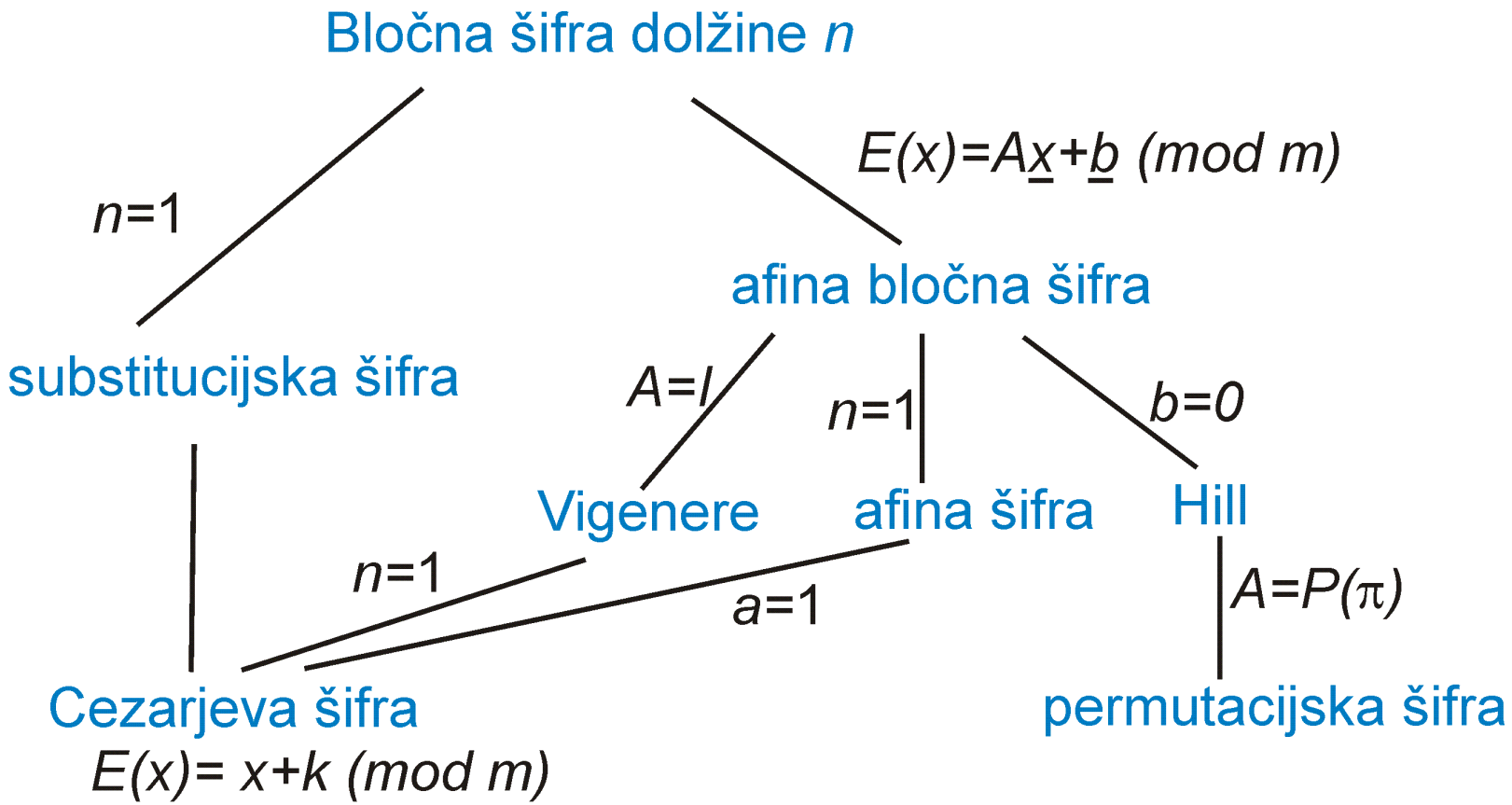
Bločna šifra dolžine n je **afina**, če je

- $\Sigma = \mathbb{Z}_m$,
- $\mathcal{K} = \{(A, b);\ A \in \mathbb{Z}_m^{n \times n},\ \det(A) \in \mathbb{Z}_m^*, b \in \mathbb{Z}_m^n\}$
- $E_{(A,b)}(x) \equiv Ax + b \pmod{m}$
- $D_{(A,b)}(x) \equiv A^{-1}(x - b) \pmod{m}$

Preverimo:

$$\begin{aligned} D_{(A,b)}(E_{(A,b)}(x)) &\equiv A^{-1}((E_{(A,b)}(x) - b) \\ &\equiv A^{-1}(Ax + b - b) \\ &\equiv x \pmod{m} \end{aligned}$$

Klasične šifre so bločne šifre



Produkt kriptosistemov

Naj bosta $\mathcal{S}_1 = (\mathcal{B}_1, \mathcal{C}_1, \mathcal{K}_1, \mathcal{E}', \mathcal{D}')$ in $\mathcal{S}_2 = (\mathcal{B}_2, \mathcal{C}_2, \mathcal{K}_2, \mathcal{E}'', \mathcal{D}'')$, za katera je $\mathcal{C}_1 = \mathcal{B}_2$.

Produkt $\mathcal{S}_1$ in $\mathcal{S}_2$ je kriptosistem

$$\mathcal{S}_1 \times \mathcal{S}_2 = (\mathcal{B}_1, \mathcal{C}_2, \mathcal{K}_1 \times \mathcal{K}_2, \mathcal{E}, \mathcal{D}),$$

kjer je

$$\begin{aligned} E_{(k_1,k_2)}(x) &= E''_{k_2}(E'_{k_1}(x)), \\ D_{(k_1,k_2)}(y) &= D'_{k_1}(D''_{k_2}(y)). \end{aligned}$$

Preverimo zahteve obrnljivosti:

Naj bo $e_i \in \mathcal{K}_i$ in d_i ustrezen dekodirni ključ za $i \in \{1, 2\}$
Potem je

$$\begin{aligned} D_{(d_1,d_2)}(E_{(e_1,e_2)}(b)) &= D'_{d_1}(D''_{d_2}(E''_{e_2}(E'_{e_1}(b)))) \\ &= D'_{d_1}(E'_{e_1}(b)) \\ &= b \end{aligned}$$

V $\mathcal{S}_1 \times \mathcal{S}_2$ torej kodirnemu ključu (e_1, e_2)
ustreza dekodirni ključ (d_1, d_2).

Zgled: $\mathcal{M} \times \mathcal{C} = \mathcal{A}$, afina šifra.

Cezarjeva šifra: $\mathcal{C} = (\mathbb{Z}_{26}, \mathbb{Z}_{26}, \mathbb{Z}_{26}, \mathcal{E}^{\mathcal{C}}, \mathcal{D}^{\mathcal{C}})$.

Multiplikativna šifra: $\mathcal{M} = (\mathbb{Z}_{26}, \mathbb{Z}_{26}, \mathbb{Z}_{26}^*, \mathcal{E}^{\mathcal{M}}, \mathcal{D}^{\mathcal{M}})$, kjer je

$$\begin{aligned} E_a^{\mathcal{M}}(x) &\equiv ax \pmod{26} \\ D_a^{\mathcal{M}}(x) &\equiv a^{-1}y \pmod{26} \end{aligned}$$

$\mathcal{M} \times \mathcal{C} = (\mathbb{Z}_{26}, \mathbb{Z}_{26}, \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}, \mathcal{E}', \mathcal{D}')$ je afina šifra, saj je

$$\begin{aligned} E'_{(a,b)}(x) &= E_b^{\mathcal{C}}(E_a^{\mathcal{M}}(x)) \\ &\equiv E_a^{\mathcal{M}}(x) + b \\ &\equiv ax + b \pmod{26} \\ D'_{(a,b)}(y) &= D_a^{\mathcal{M}}(D_b^{\mathcal{C}}(y)) \\ &\equiv a^{-1} D_b^{\mathcal{C}}(y) \\ &\equiv a^{-1}(y - b) \pmod{26} \end{aligned}$$

Prevedljivost kriptosistemov

Kriptosistem $\mathcal{S} = (\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ je prevedljiv na kriptosistem $\mathcal{S}' = (\mathcal{B}, \mathcal{C}, \mathcal{K}', \mathcal{E}', \mathcal{D}')$, če obstaja $f : \mathcal{K} \to \mathcal{K}'$, da za vse $k \in \mathcal{K}$ velja:

$$E_k = E'_{f(k)}, \quad D_k = D'_{f(k)}.$$

Tedaj pišemo $\mathcal{S} \to \mathcal{S}'$.

Kriptosistema $\mathcal{S}$ in $\mathcal{S}'$ sta ekvivalentna, če velja

$$\mathcal{S} \to \mathcal{S}' \quad in \quad \mathcal{S}' \to \mathcal{S}.$$

Tedaj pišemo $\mathcal{S} \equiv \mathcal{S}'$.

Ekvivalenca $\mathcal{C} \times \mathcal{M}$ in $\mathcal{A}$

Torej: cezarjeva šifra $\mathcal{C}$ in multiplikativna šifra $\mathcal{M}$ v bistvu komutirata.

Idempotentni kriptosistemi

Kriptosistem $\mathcal{S} = (\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ je idempotenten, če je

$$\mathcal{S} \times \mathcal{S} \equiv \mathcal{S}.$$

- Klasični kriptosistemi: Cezarjev, substitucijski, afin, Hillov, permutacijski, Vigenèrjev so vsi idempotentni.
- Če sta simetrična kriptosistema S_1 in S_2 idempotentna in obenem še komutirata, potem je tudi produkt $S_1 \times S_2$ idempotenten.
- Če simetrični kriptosistem ni idempotenten, potem morda z njegovo iteracijo za večkrat povečamo varnost. Na tem so zasnovani **AES** in mnogi drugi simetrični kriptosistemi.

Idempotentnost substitucijske šifre

Sestavine sestavljenih šifer

Najmodernejše bločne šifre so produktne šifre.
Komponiramo več enostavnih operacij, ki (vsaka posebej) niso dovolj varne, z namenom, da povečamo varnost:

- permutacije mest
- substitucije
- XOR (ekskluzivni ali)
- linearne transformacije
- aritmetične operacije
- modularno množenje

Primeri bločnih sestavljenih šifer: DES, AES, IDEA.

Nekatere želene lastnosti bločnih šifer

Varnost:

- **razpršitev** (*angl.* diffusion):
  vsak bit kriptograma naj bo odvisen od vseh bitov besedila.
- **zmeda** (*angl.* confusion):
  zveza med ključem ter biti kriptograma naj bo zapletena,
- **velikost ključev**: mora biti majhna, toda dovolj velika da je izčrpno iskanje ključa ne pride v poštev.

Učinkovitost

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

Iterativne šifre

Običajno uporabljamo **iterativne šifre**, ki jih tipično sestavlja:

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

Razpored ključev

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:** $K^1, \ldots, K^{N_r}$.

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

Krožna funkcija

Krožna funkcija g ima dva argumenta:

(i) krožni ključ (K^r) in

(ii) *tekoče stanje* (w^{r-1}).

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

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

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

Šifriranje

Besedilo x vzamemo za začetno stanje w_0.
Kriptogram y je stanje po N_r krogih:

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

Dešifriramo potem

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

Substitucijsko-permutacijska omrežja (SPN)

Vpeljal jih je Claude Shannon (1949).

Naj bo $\Sigma = \{0, 1\}$, $\ell, m \in \mathbb{N}$.

Substitucijsko-permutacijsko omrežje je iterativna bločna šifra $(\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, kjer je $\mathcal{B} = \mathcal{C} = \Sigma^{\ell m}$.

SPN je zgrajen iz dveh komponent

- substitucije $\pi_s \in S(\Sigma^\ell)$
- permutacije $\pi_p \in S_{\ell m}$

Permutacijo π_s imenujemo *S*-škatla in z njo zamenjamo ℓ bitov z drugimi ℓ biti.

Permutacija π_p pa permutira ℓm bitov.

Oznake

$x = x_1\, x_2\, \ldots x_{\ell m}, \quad |x_i| = 1$ delitev na bite

$x = \underline{x_1}\, \underline{x_2}\, \ldots\, \underline{x_m}, \quad |x_i| = \ell$ delitev na zloge dolžine ℓ

Kodiranje pri SPN

$w^0 = b$

za $r = 1, 2, \ldots N_r - 1$ **ponovi**

$u^r = w^{r-1} \oplus K^r$ (primešamo ključ)

za $i = 1, 2, \ldots m$ **ponovi**

$\underline{v}_i^r := \pi_s(\underline{u}_i^r)$ (substitucija zlogov)

$w^r = v^r_{\pi_p(1)}, \ldots, v^r_{\pi_p(\ell m)}$ (permutacija bitov)

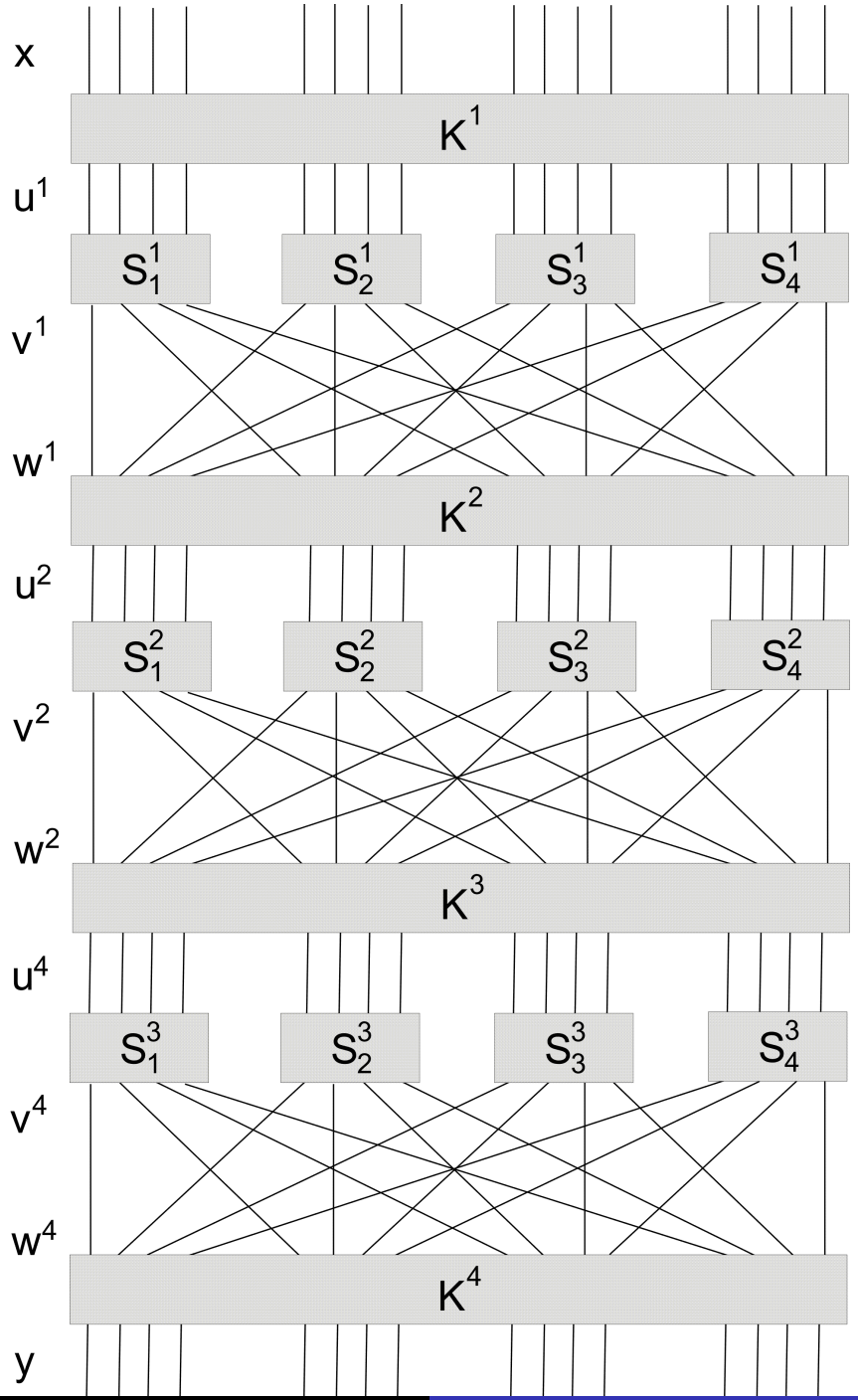
(zadnji krog)

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

za $i = 1, 2, \ldots, m$ **ponovi**

$\underline{v}_i^{N_r} := \pi_s(\underline{u}_i^{N_r})$

vrni $c = v^{N_r} \oplus K^{N_r+1}$ (beljenje)


x
K1
u1
S11
S21
S31
S41
v1
w1
K2
u2
S12
S22
S32
S42
v2
w2
K3
u4
S13
S23
S33
S43
v4
w4
K4
y

Dekodiranje pri SPN

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

za $i = 1, 2, \ldots, m$ **ponovi**

$\quad \underline{u}_i^{N_r} := \pi_s^{-1}(\underline{v}_i^{N_r})$

za $r = N_r - 1, N_r - 2, \ldots, 1$ **ponovi**

$\quad w^r = u^{r+1} \oplus K^{r+1}$

$\quad v^r = (w^r_{\pi_p^{-1}(1)}, \ldots, w^r_{\pi_p^{-1}(\ell m)})$

$\quad$ **za** $i = 1, 2, \ldots m$ **ponovi**

$\quad\quad \underline{u}_i^r := \pi_s^{-1}(\underline{v}_i^r)$

$b = u^1 \oplus K^1$

Feistelova šifra

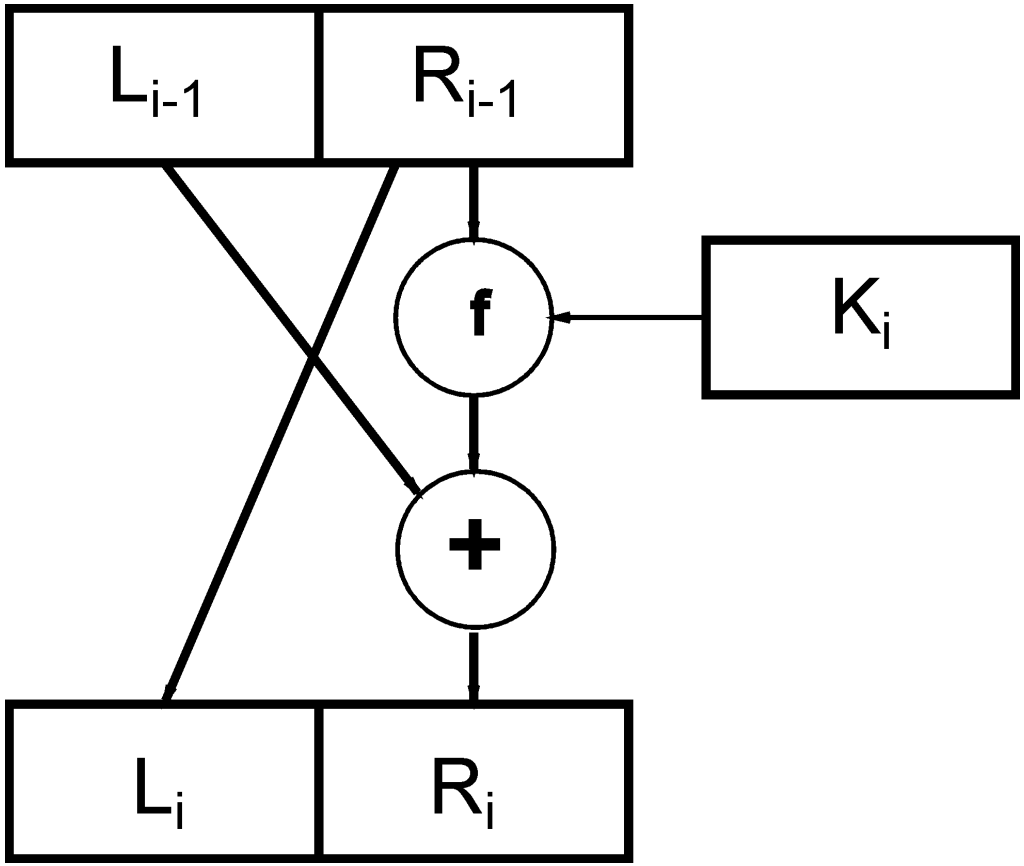
Izumil jo Horst Feistel (IBM T.J. Watson Research Labs) v 1970'.

Feistelova šifra je bločna iterativna šifra dolžine $2t$ nad abecedo $\Sigma = \{0, 1\}$:

N_r je število krogov,
$K^1, K^2, \ldots, K^{N_r}$ razpored ključev, ki ga dobimo iz ključa K
$f_K : \Sigma^t \to \Sigma^t$ za vsak podključ K Feistelova kodirna funkcija (ni nujno obrnljiva)

Kodiranje:
$L_0 =$ leva polovica b
$R_0 =$ desna polovica b
za $i = 1, 2, \ldots, N_r$ **ponovi**
$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus f_{K_i}(R_{i-1})$,
$c = (R_{N_r}, L_{N_r})$

En krog pri Feistelovi šifri



Dekodiranje pri Feistelovi šifri

Ker pri kodiranju končamo z (R_{N_r}, L_{N_r}) (in ne z (L_{N_r}, R_{N_r})), je dekodiranje enako kodiranju, le da ključe uporabimo v obratnem vrstnem redu.

Dekodiranje:
$L_{N_r} =$ leva polovica c
$R_{N_r} =$ desna polovica c
za $i = N_r, N_r - 1, \ldots, 2, 1$ **ponovi**
$L_{i-1} = R_i$
$R_{i-1} = L_i \oplus f_{K_i}(R_i)$,
$b = (R_0, L_0)$

Kratka zgodovina bločne šifre DES

1970': IBM – Feistelova šifra in LUCIFER.

1972: NBS (sedaj NIST) izbira simetrično šifro za zaščito računalniških podatkov, ki bo:

- varna
- javna
- izdelana bo kompletna specifikacija
- enostavna za analizo
- dostopna vsem uporabnikom
- učinkovita v strojni in programski implementaciji
- dovoljeno jo bo izvoziti

1974: IBM razvije DES,

1975: NSA ga "popravi" (dolžino ključev s 128 bitov na 56...)

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

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

1992: Biham and Shamir objavita teoretični napad z diferenčno kriptoanaliza; pregledati je treba manj ključev kot za napad z grobo silo, a zahteva 2^{47} izbranih parov (b, c).

1994: Prva eksperimentalna kriptoanaliza: linearna kriptoanaliza (Matsui, 1994); potrebuje 2^{47} znanih parov (b, c).

1997: V projektu DESCHALL prvič (javno) dekodirajo sporočilo, kodirano z DES (porazdeljena omrežja).

1997: AES (Advanced Encryption Standard) - objava natečaja

1998: Electronic Frontier Foundation (EFF) konstruira posebno napravo (Deep Crack), ki najde ključ za DES v 56 urah.

1999: Hitrejše iskanje ključa: 22 ur, 15 minut (Deep Crack in računalniške mreže).

1999: Des je potrjen za uporabo (že četrtič) kot FIPS 46-3, vendar že priporoča za uporabo 3DES.

2001: Objavljen je standard AES (FIPS 197).

2002: Standard AES stopi v veljavo.

2004: Predlog za umik FIPS 46-3 (in nekaj sorodnih standardov).

2005: NIST umakne standard FIPS 46-3.

Zgradba DES

DES je 64- bitna bločna šifra s Feistelovo strukturo,
56-bitni ključem (v resnici 64 bitov, 8 bitov je kontrolnih),
in 16 krogi, ki uporabljajo podključe dolžine 48 bitov.

Feistelova funkcija $F_k : \Sigma^{32} \to \Sigma^{32}$ uporabi pomožne funkcije:
ekspanzijska funkcija $E : \Sigma^{32} \to \Sigma^{48}$
substitucije (S-box) $S_i : \Sigma^6 \to \Sigma^4$, $i = 1, 2, \ldots, 8$
permutacija mest $P \in S_{32}$

$$F_k(x) = P(S_1(w^1)S_2(w^2)\ldots S_8(w^8),$$

kjer je $w^1 w^2 \ldots w^8 = E(x) \oplus k$.

Razpored podključev

$\mathcal{K} = \Sigma^{56}$ množica DES-ovih ključev
$\mathcal{P} = \Sigma^{48}$ množica DES-ovih podključev

Pomožne funkcije:
$PC1 : \Sigma^{56} \to \Sigma^{56}$ permutacija bitov.
$PC2 : \Sigma^{56} \to \Sigma^{48}$ izbor in permutacija bitov.
$v : \{1, 2, \ldots, 16\} \to \{1, 2\}$,
$v(i) = 1$, če $i \in \{1, 2, 9, 16\}$ in 2 sicer.

Generiranje razporeda podključev

Podatek: $k \in \Sigma^{56}$

Postopek:
$C^0 D^0 = PC1(k)$
za $i = 1, 2, \ldots 16$ **ponovi**
$C^i =$ krožni pomik C^{i-1} za $v(i)$ v levo
$D^i =$ krožni pomik D^{i-1} za $v(i)$ v levo
$k^i = PC2(C^i D^i)$

Rezultat: $k^1, k^2, \ldots, k^{16} \in \Sigma^{48}$

Celotni DES

Podatek: besedilo b.
Izhod: kriptogram c.

- Na b uporabimo začetno permutacijo IP:$\Sigma^{64} \to \Sigma^{64}$.
- Na IP(b) uporabimo Feistelovo šifro.
- Na rezultatu IP^{-1}.

Vse podrobnosti najdemo v standardu FIPS 46-3.

Trojni DES, DESX

Zakaj dvojni DES ne zadošča? (vaje)
(uporabimo lahko napad s srečanjem v sredini (*angl.* Meet-in-the-middle attack); časovna zahtevnost se samo podvoji v primerjavi z napadom na DES, poveča se prostorska zahtevnost.)

Trojni DES, TDEA: $k = (k_1, k_2, k_3)$

$$TDEA_k(b) = DES_{k_3}(DES_{k_2}(DES_{k_1}(b)))$$

DESX (Rivest, 1984): $k = (k_1, k_2, k_3)$

$$DESx_k(b) = k_3 \oplus DES_{k_1}(b \oplus k_2)))$$

Ključ ima dolžino 56+64+64, vendar je pri napadu z grobo silo ekvivalenten le ključu dolžine $56 + 64$.
Veliko hitrejše računanje kot pri TDEA!.