Paskaita 17

DES (Data Encryption Standard)

Algoritmas patvirtintas standartu 1974
Galiojo iki 2000 metų.

Jo pagrindas - Feistel algoritmas (šifras)

1. Pasirenkame blokinį šifrą:
   a) $\Sigma = \{0, 1\}$ alfabetas
   b) t duomenų (plain teksto) bloko ilgis
   c) K_i - raktas ~~aibė~~ iš aibės K
   d) f_{K_i} - šifravimo funkcija, kai naudojame raktą $K_i \in K$.

2. Feistelio šifras
   a) $\Sigma = \{0, 1\}$ alfabetas
   b) $2t$ - bloko ilgis
   c) $r > 1$ { iteracijų arba raundų (roundo) skaičius

d) $\mathcal{L}$ - raktų aibė.

Pasirinkus $k \in \mathcal{L}$, generuojame r raktų $K_1, \dots, K_r \in K$ skirtų pagrindinio blokinio šifravimo algoritmo realizavimui.

e) E_k, $k \in \mathcal{K}$ yra Feistelio šifravimo funkcija, ji apibrėžiama taip:

1. p yra nešifruoto teksto (plain) blokas, kurio ilgis $2t$. Jį skaidome į dvi t ilgio blokus $p = (L_0, R_0)$ (left, right).

2. Konstruojame seką

$$(L_i, R_i) = (R_{i-1}, L_{i-1} \oplus f_{K_i}(R_{i-1})), \quad i = 1, \dots, r$$

Ap.
$$\boxed{E_k(L_0, R_0) = (R_r, L_r)} = c$$

c - šifruoto teksto blokas

Dešifravimo algoritmas

$$(R_{i-1}, L_{i-1}) = (L_i, R_i \oplus f_{K_i}(L_i))$$

$$i = r, \dots, 1$$

$$p = (L_0, R_0)$$

Teisingumo patikrinimas

$$R_i = L_{i-1} \oplus f_{K_i}(R_{i-1})$$ (iš šifravimo algoritmo)

$$(R_{i-1} = L_i) = L_{i-1} \oplus f_{K_i}(L_i)$$

$$R_i \oplus f_{K_i}(L_i) = L_{i-1} \oplus f_{K_i}(L_i) \oplus f_{K_i}(L_i)$$

$$= L_{i-1}.$$

Taigi Feistelio algoritme šifravimo ir dešifravimo žingsniai yra tokie patys, tik kriptografo raktų panaudojimo eiliškumas

DES algoritmas

Blokai dvejetainių: $t = 32$, $2t = 64$

$p_i \in \mathcal{P}$, $c \in C$

$\mathcal{P}, C \in \{0,1\}^{64}$

DES raktas $k \in \mathcal{K} = \{(b_1, b_2, \dots, b_{64}) \in \{0,1\}^{64}\}$

$$k = \begin{bmatrix} b_1 & b_2 & b_3 & \dots & b_8 \\ b_9 & b_{10} & b_{11} & \dots & b_{16} \\ \dots & \dots & \dots & \dots & \dots \\ b_{57} & b_{58} & b_{59} & \dots & b_{64} \end{bmatrix}$$

Normavimo sąlyga $\sum_{i=1}^{8} b_{8\ell+i} \equiv 1 \pmod 2$,

t. y. kiekviena eilutės (baito) bitų suma yra nelyginis skaičius (t. y. laisvai parenkame septynis pirmuosius bitus, o aštuntį jau randame iš normavimo sąlygos!

Taigi $|\mathcal{K}| = 2^{56} \sim 7.2 \cdot 10^{16}$ raktų.

Užd. 1. Patikrinkite, kad HEX skaičius

13345779 9BBCDFF1 yra keistinas raktas.

$1 \rightarrow 0001$

$F \rightarrow 1111$

$D \rightarrow 1101$

$C \rightarrow 1100$

$3 \rightarrow 0011$

$$k = \begin{bmatrix} \overbrace{0001}^{1}\,\overbrace{0011}^{3} \\ 0011\,0100 \\ 1101\,1111 \\ \underbrace{1111}_{F}\,\underbrace{0001}_{1} \end{bmatrix}$$

Normalaus ilgio yra išpildytos

1. Pradinė perstata bloko p (IP-initial permutation)

Ši perstata nepriklauso nuo rakto k.

$$p = p_1 p_2 \cdots p_{64} \Rightarrow IP(p) = p_{58} p_{50} p_{42} \cdots p_{15} p_7$$

$$IP(p) = p'$$

Feistelio šifras pritaikomas p' blokui.

Šifruotas tekstas c' dar veikiamas perstatos (operatoriumi) IP^{-1}

$$c = IP^{-1}(c').$$

Dabar apibrėžkime blokinės algoritmo šifravimo funkciją f_{K_j}. Alfabetas $\{0,1\}$, $t=32$ bloko ilgis

Raktų ~~čia~~ arba (endvė) yra $\{0,1\}^{48}$:

$$f_{K_j}: \{0,1\}^{32} \longrightarrow \{0,1\}^{32}, \quad K_j \in \{0,1\}^{48}.$$

- $R \in \{0,1\}^{32}$ yra išplečiamas naudojant išplėtimo funkciją E:

$$E: \{0,1\}^{32} \longrightarrow \{0,1\}^{48}$$

$$E(R) = \underbrace{R_{32} R_1 R_2 R_3 \cdots R_{31} R_{32} R_1}_{48}$$

- suskaičiuojame $E(R) \oplus K_j$ ir gautąjį bloką dalinome į 8 blokus, kurių ilgis 6.

$$E(R) \oplus K_j = B_1 B_2 B_3 \cdots B_8, \quad B_\ell \in \{0,1\}^6$$

Raktai.
Iš 56 bitų rakto $k \in \mathcal{K}$ generuojame 16 raktų $K_1, K_2, \ldots, K_{16}$, kurių ilgiai yra 48.

- naudojame f-jas $S_i : \{0,1\}^6 \to \{0,1\}^4$,

$i = 1, 2, \dots, 8$ (jos neprikl. nuo k).

$$C_i = S_i(B_i), \quad i = 1, 2, \dots, 8.$$

Tada apibrėžiame blokinio šifro vaizdą

$$C = C_1 C_2 \dots C_8 \in \{0,1\}^{32}.$$

Funkcijos $f_K(R)$ vaizdas gaunamas

C pavidalu perstatos (operatoriaus) P

$$f_K(R) = P(C).$$

Dešifravimo algoritme vėl naudojame tą patį šifravimo algoritmą tik su pakeista (priešinga) raktų tvarka.

vanagas.vgtu.lt

1 min — $6.5 \cdot 10^6$ variantų (raktų k)

$\Rightarrow$ 24h $60 \times 24 \times 6.5 \times 10^6 = \boxed{9.36 \cdot 10^9}$ raktų