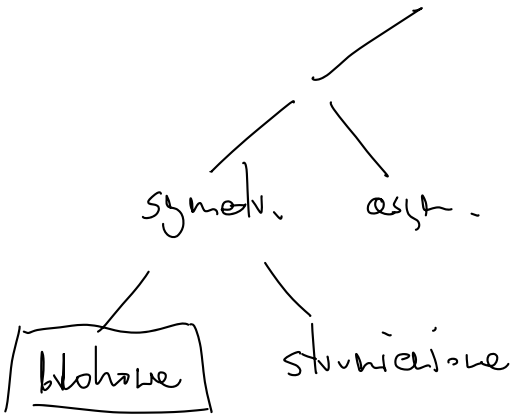
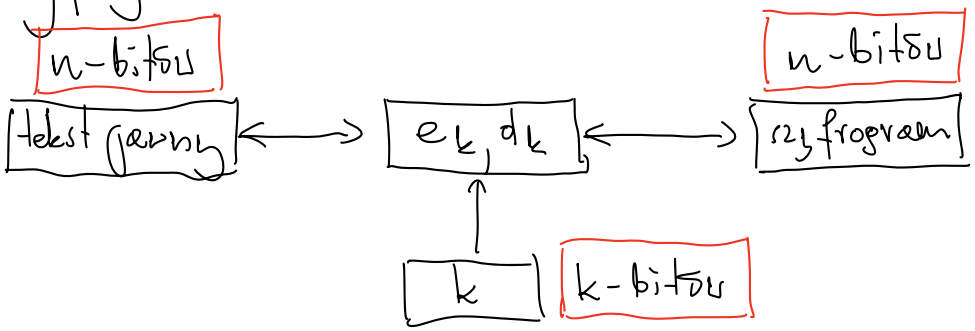
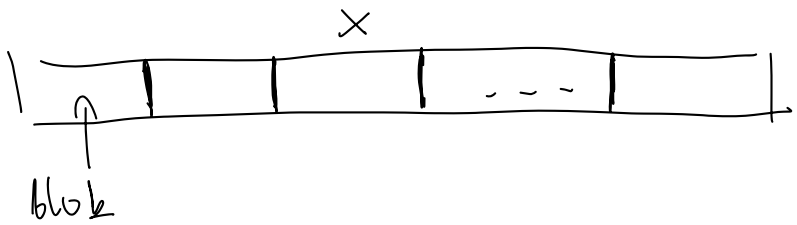


Szyfry blokowe

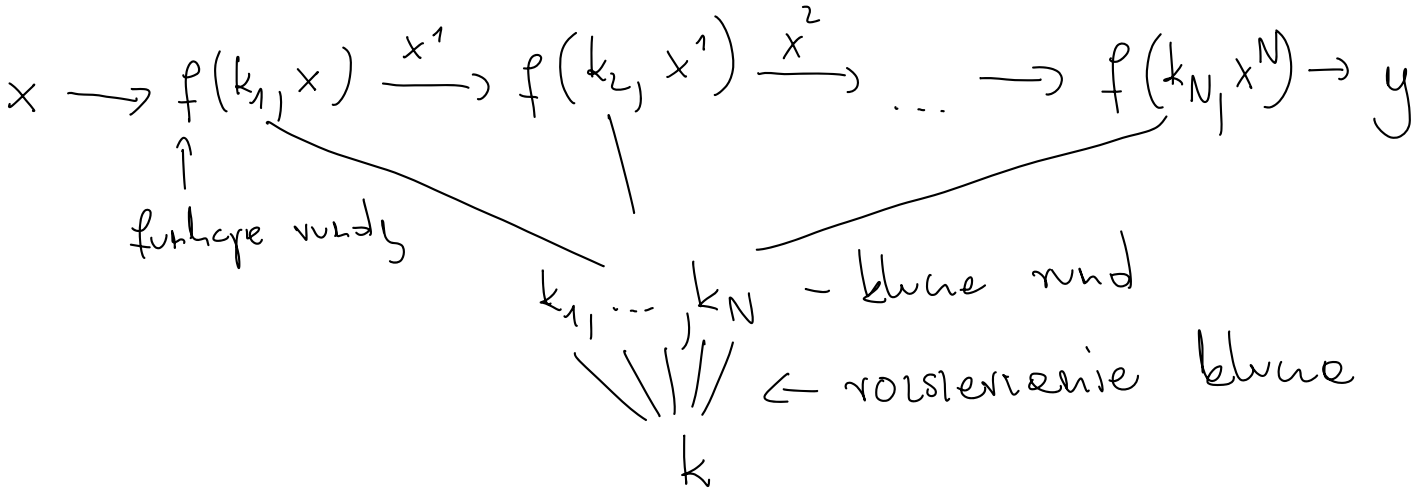




DES ↑
$n = 64$
$k = 56$

3DES ↑
$n = 64$
$k = 168$

AES ↑
$n = 128$
$k = 128, 192, 256$



DES $N = 16$ AES $N = 10$ (k: 128 b)

SPN (Substitution - Permutation Network)

$l, m \in \mathbb{N}$ $\quad n = l \cdot m$

$\pi_S : \{0,1\}^l \to \{0,1\}^l$ ← permutacja $\quad 2^l \to 2^l$

↑ zbiór ciągów 0-1 o dł. l

$\pi_P : \{1,2,\dots,n\} \to \{1,2,\dots,n\}$ ← permutacja

S-box ← konkatenacja

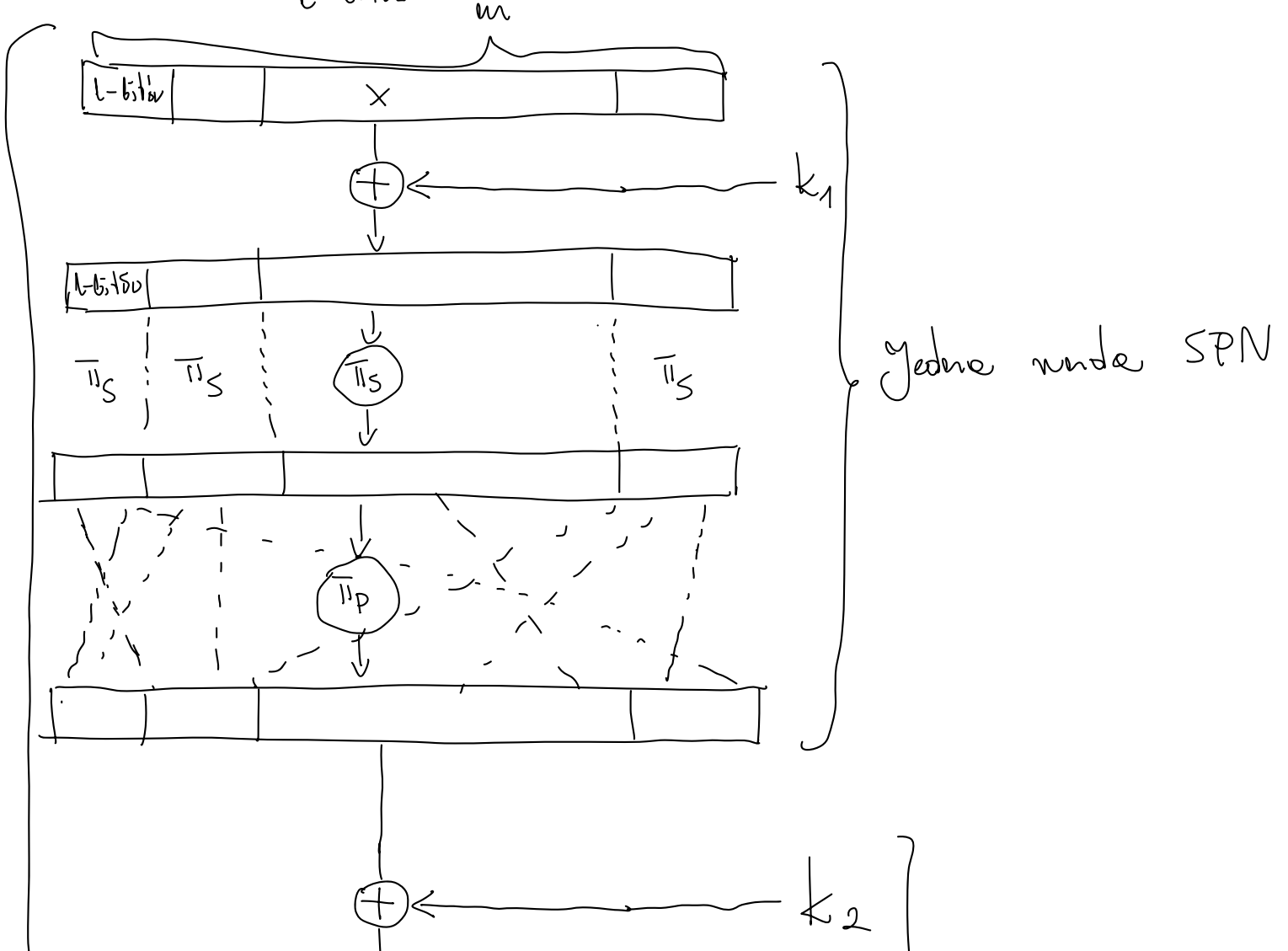
$x = x_1 \| x_2 \| \dots \| x_m$

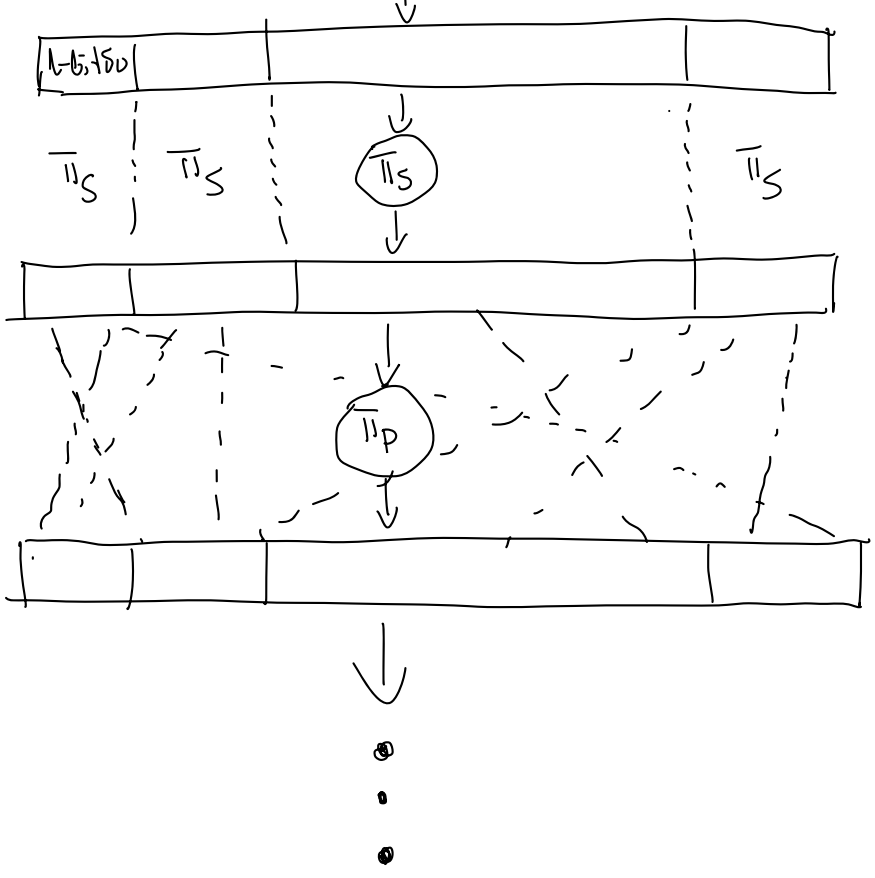
x: n bitów; $x_1, x_2, \dots, x_m$: l-bitów

k - klucz

↳ rozszerzenie $k_1, \dots, k_N$

n bitów





Drugo runda

SPN o N rundach

DES Data Encryption Standard

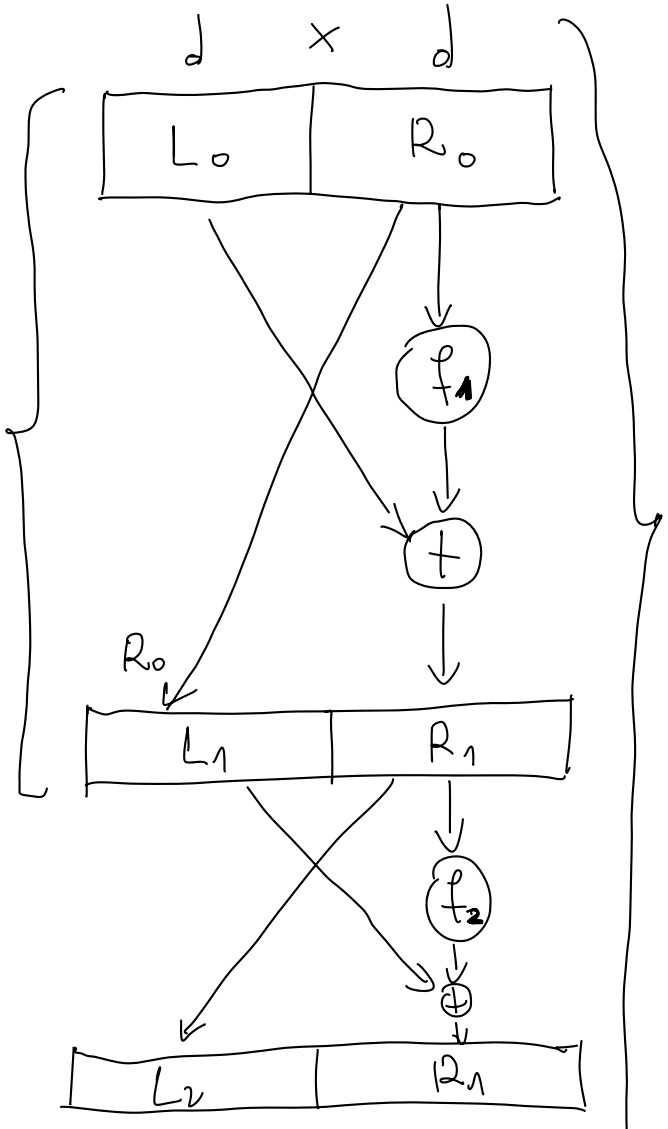
1973 NBS (National Bureau of Standards)

1975 IBM Lucifer ← 1970 Horst Feistel
$n = 128$, $k = 128$

1977 Przyjęty standard DES federalny

Sieć Feistela

$f_1, \dots, f_N : \{0,1\}^d \to \{0,1\}^d$ double funkcja



Sieć Feistela

L_i, R_i

$$\begin{cases} L_{i+1} = R_i \\ R_{i+1} = f_{i+1}(R_i) \oplus L_i \end{cases}$$

$\vdots$

Czy da się odwrócić? $\overset{?}{\exists}$

$$(L_{i+1}, R_{i+1}) \xrightarrow{?} (L_i, R_i)$$

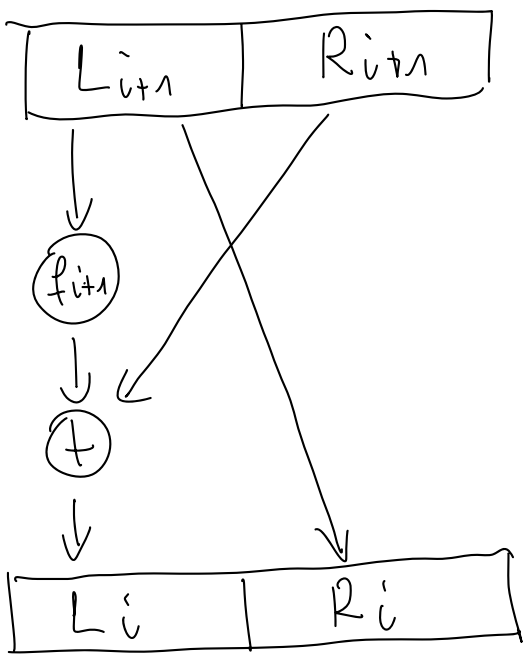
$$\begin{cases} L_{i+1} = R_i \\ R_{i+1} = f_{i+1}(R_i) \oplus L_i \end{cases} \Rightarrow \begin{cases} R_i = L_{i+1} \\ L_i = R_{i+1} \oplus f_{i+1}(L_{i+1}) \end{cases}$$

$$R_{i+1} \oplus f_{i+1}(R_i) = \underbrace{f_{i+1}(R_i) \oplus f_{i+1}(R_i)}_{0} \oplus L_i$$

$R_{i+1} \oplus f_{i+1}(R_i) = L_{i+1}$

$R_{i+1} \oplus f_{i+1}(L_{i+1})$

L_i



DES 16 - rundowa sieć Feistela

$f_1, \dots, f_{16} : \{0,1\}^{32} \to \{0,1\}^{32}$

k - 56 bitów

↓ rozszerzanie

$k_1, \dots, k_{16}$

48 bitów