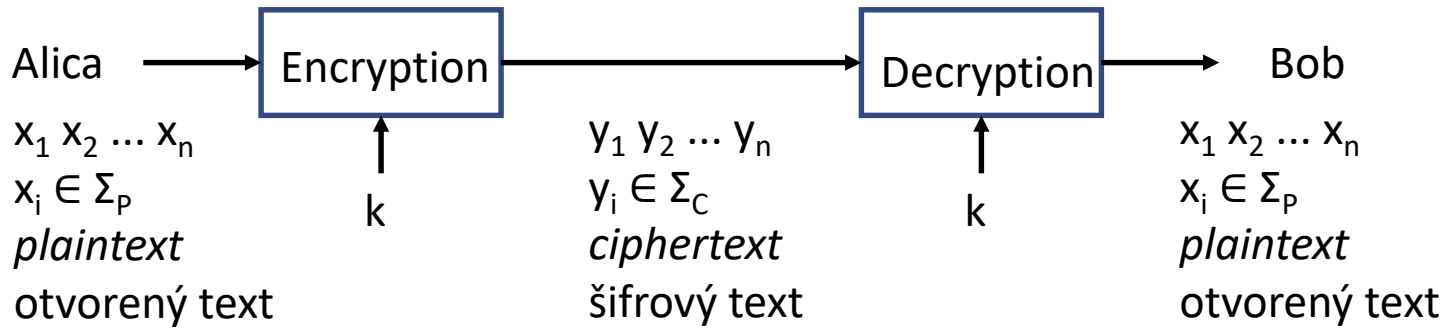
Kryptografické systémy
Blokové šifry

doc. RNDr. Jozef Jirásek, PhD.

ZS 2023

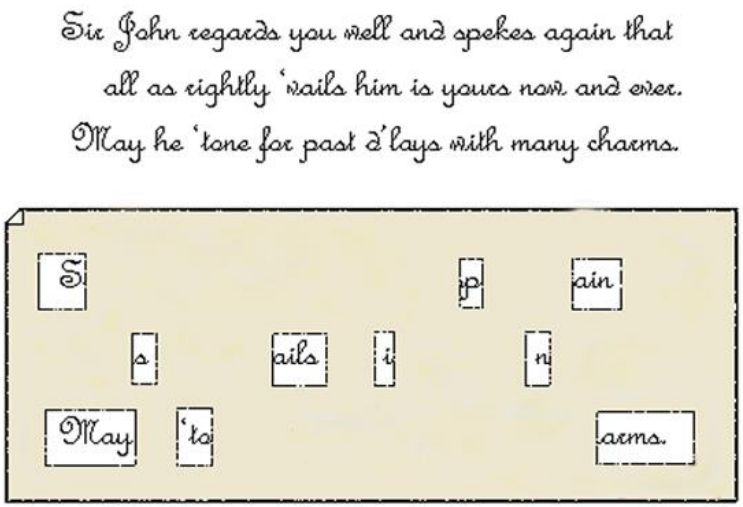
Substitučné šifrovacie systémy



- posuvná šifra
- monoalfabetická substitúcia
- polyalfabetické šifry
- prúdové šifry (substitúcia prekrytím pseudonáhodne generovaným prúdom znakov)
- viacznakové šifry (Playfair, Hill, ...)

Jednoduchá mriežka (Cardan grille)

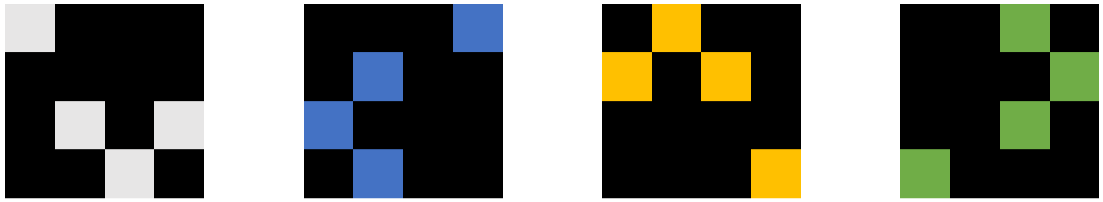
- Cardano (1550)
  znaky textu, ktorý chceme zašifrovať, nájdeme v obyčajnom texte (liste) a ich pozície vyznačíme v mriežke
- dešifrovanie – opäť priložiť mriežku (kľúč)
- skôr steganografia ...



Otáčacia mriežka

Fleissner (1880) – 4 pozície mriežky – všetky miesta obsadené textom

dešifrovanie – použiť mriežku v dohodnutom poradí



K			
	R		Y
		P	

K			T
	O		
G	R		Y
	R	P	

K	A		T
F	O	I	
G	R		Y
	R	P	A

K	A	U	T
F	O	I	P
G	R	J	Y
S	R	P	A

K	A	U	T
F	O	I	P
G	R	J	Y
S	R	P	A

Transpozičné šifry

Šifrový text vznikne permutáciou (niektorých) znakov otvoreného textu (ak je text dlhý, možno ho rozdeliť na bloky podľa veľkosti permutácie)

- zápis otvoreného textu odzadu
- zápis textu do riadkov pevnej dĺžky
  a šifrovanie čítaním po stĺpcoch (scytale)
- stĺpcová transpozícia – pred čítaním stĺpce zamiešame
- permutačné mriežky (jednoduché zapamätanie permutácie – mechanické šifrovanie a dešifrovanie)

expanzná permutácia - zobrazenie znakov otvoreného textu na viacero miest šifrového textu (eliminácia použitia frekvenčnej analýzy a hľadania anagramov)

Šifra ADFGX

- používaná v 1. svetovej vojne v nemeckej armáde
- kombinácia Polybiovho štvorca so stĺpcovou transpozíciou
- znaky šifrového textu – A D F G X – odlišný Morseho kód (redukcia chýb)
- kľúč (napr. „VELMINAHODNE ABEZPECNEHESLO“) zapíšeme do Polybiovho štvorca (ako v Playfair šifre)

	A	D	F	G	X
A	V	E	L	M	I
D	N	A	H	O	D
F	B	Z	P	C	S
G	F	G	K	Q	R
X	T	U	W	X	Y

Šifra ADFGX

	A	D	F	G	X
A	V	E	L	M	I/J
D	N	A	H	O	D
F	B	Z	P	C	S
G	F	G	K	Q	R
X	T	U	W	X	Y

znaky otvoreného textu šifrujeme dvojicou indexu riadku a indexu stĺpca

K R Y P T O G R A F I A

GF GX XX FF XA DG GD GX DX GA AX DD

S	U	P	E	R
G	F	G	X	X
X	F	F	X	A
D	G	G	D	G
X	D	X	G	A
A	X	D	D	

E	P	R	S	U
X	G	X	G	F
X	F	A	X	F
D	G	G	D	G
G	X	A	X	D
D	D		A	X

a pokračujeme stĺpcovou transpozíciou s kľúčom SUPER

šifrový text (po stĺpcoch):

XXDGD GFGXD XAGAX GXDXA FFGDX

Iné možnosti utajenia informácie

Shannon (1945) – zobrazenia, zvyšujúce entropiu :

- konfúzne – zakrývajúce vzťah medzi kľúčom a šifrovým textom, zmena v kľúči spôsobí zmenu CT na viacerých miestach
  - zobrazenie je nelineárne – pre šifrovaciu funkciu nie je možné použiť aproximáciu lineárnymi resp. inými jednoduchými funkciami
- difúzne – zakrývajúce vzťah medzi otvoreným a šifrovým textom tým, že zmena znaku v PT zmení znaky v CT na rôznych miestach (charakteristiky PT sa rozptýlia do celého CT resp. bloku CT)
  - lavínový efekt (the avalanche effect) – zmena bitu v otvorenom texte zmení každý bit výstupu s pravdep. 1/2

Iné možnosti utajenia informácie

Shannon – zobrazenia, zvyšujúce entropiu :

- **konfúzne** – zakrývajúce vzťah medzi kľúčom a šifrovým textom, zmena v kľúči spôsobí zmenu CT na viacerých miestach
- **difúzne** – zakrývajúce vzťah medzi otvoreným a šifrovým textom tým, že zmena znaku v PT zmení znaky v CT na rôznych miestach
- z teórie informácie **neexistujú iné také zobrazenia**
- zloženie konfúzneho a difúzneho zobrazenia nie je komutatívne (záleží na poradí)

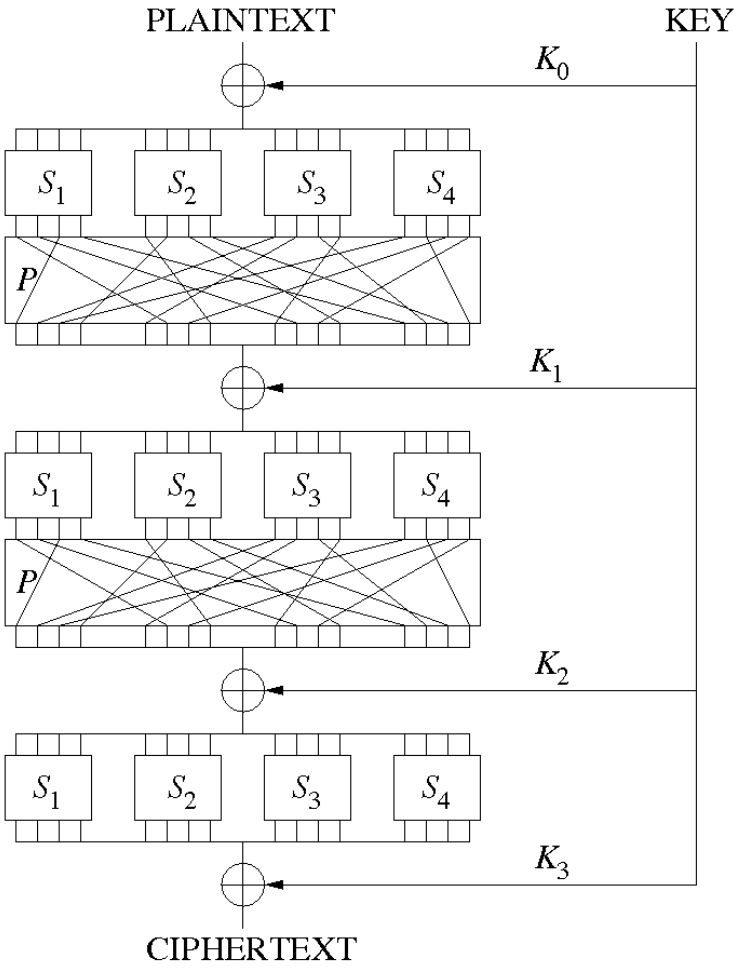
Substitučno – permutačné siete

utajenie zvýši len opakovaná kombinácia konfúzie (substitúcie) a difúzie (transpozície)

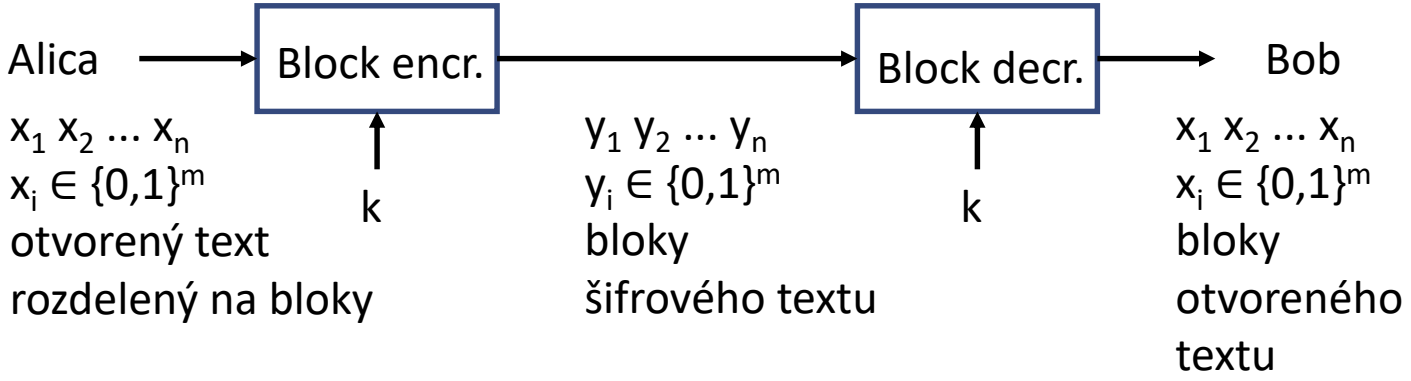
substitučno-permutačné siete opakujú substitúciu (stále s iným kľúčom) a permutáciu v tzv. rundách (*round*)

účinnosť závisí od kvality substitučných blokov (S-boxov) a veľkosti permutácie (P-boxy)

dešifrovanie – obrátený postup (s inverznými S-boxmi)

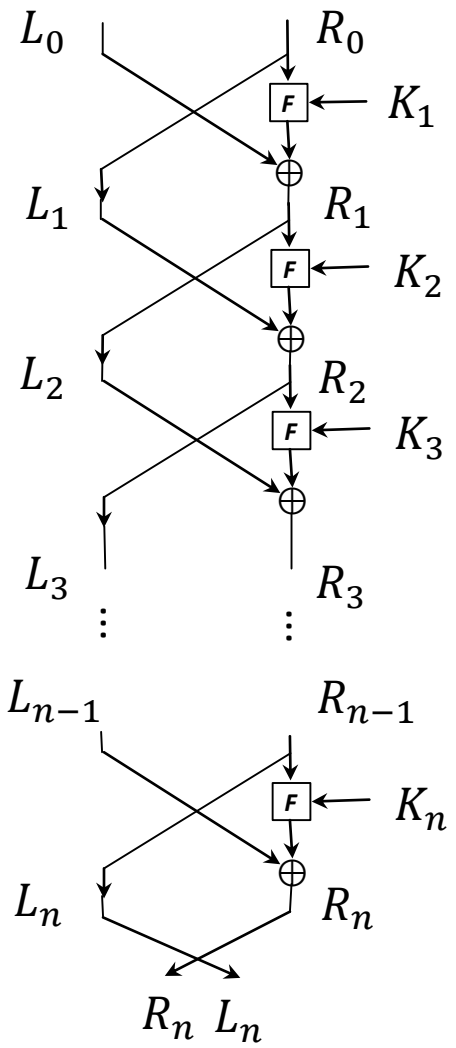


Blokové symetrické šifrovacie systémy



- delenie textu na bloky rovnakej veľkosti (aby sa dali urobiť difúzie)
- šifrovanie rovnakých blokov tým istým kľúčom bude rovnaké – blok musí byť dostatočne veľký, aby sa nedali využiť štatistické metódy resp. kódovacie tabuľky pre každý kľúč
- bloková substitúcia umožňuje $|K| = 2^m !$ kľúčov – prakticky stačí menej, ale treba s nimi správne narábať

Feistelova sieť



Feistel (1973) – SP sieť

(pôvodne pre IBM šifru Lucifer)

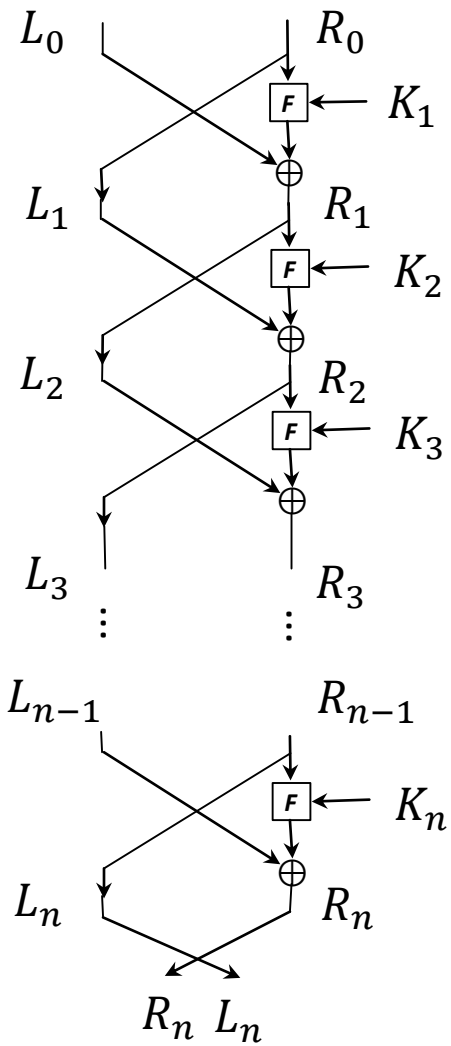
blok rozdelený na polovice L_0 a R_0

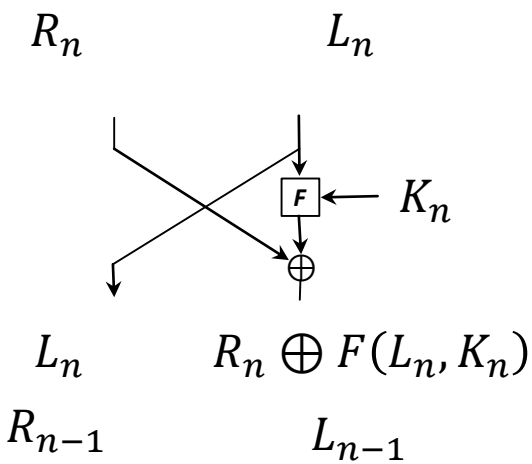
$L_i = R_{i-1} \quad R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

po n rundách je šifrový text $R_n L_n$

- difúzia – zmiešanie s opačnou polovicou bloku
- konfúzia – nelineárna funkcia F ovplyvnená rôznymi kľúčmi

Feistelova sieť - dešifrovanie





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

začiatok $R_n L_n$

po prvej runde bude

$L_n \qquad R_n \oplus F(L_n, K_n)$

a z poslednej rundy šifrovania

$L_n = R_{n-1}$

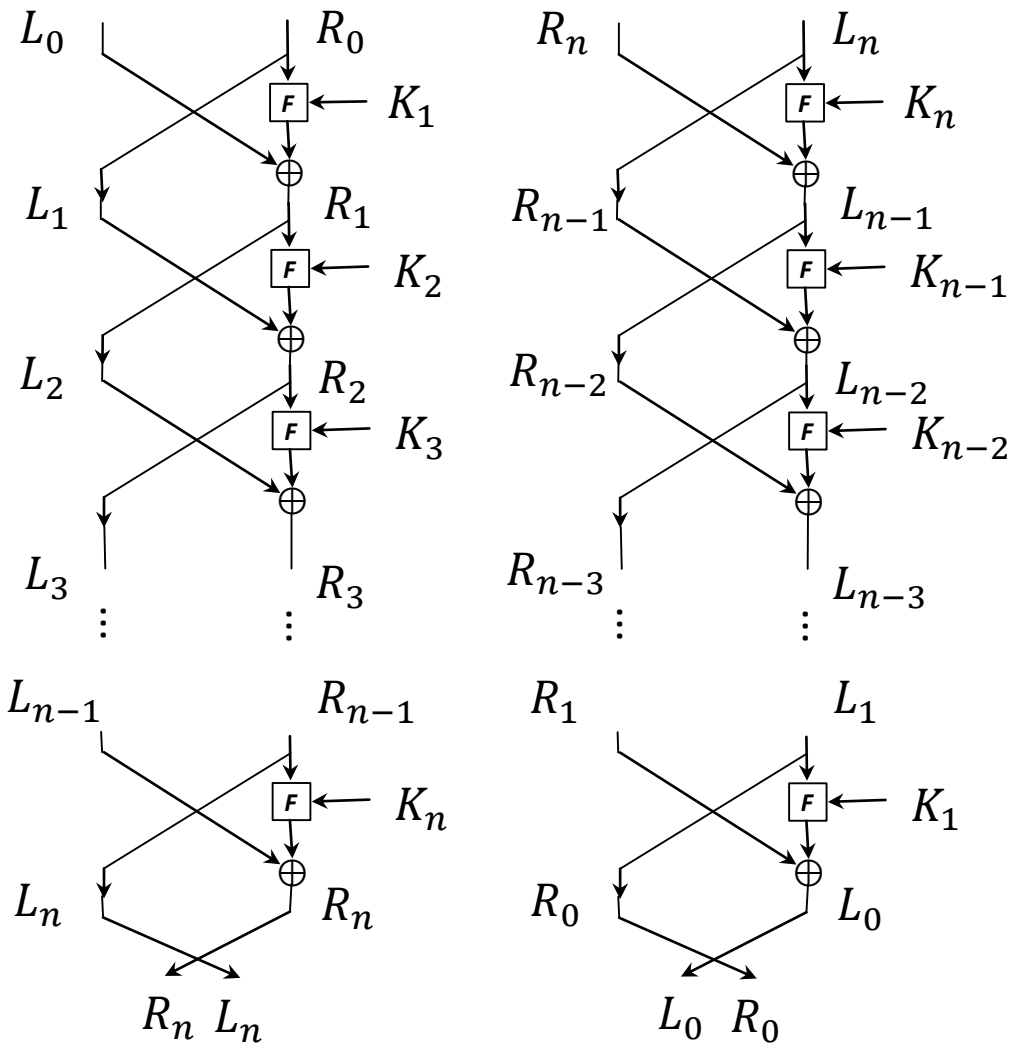
$R_n = L_{n-1} \oplus F(R_{n-1}, K_n)$

dosadením L_n a R_n dostaneme

$R_n \oplus F(L_n, K_n) = L_{n-1} \oplus F(R_{n-1}, K_n) \oplus F(R_{n-1}, K_n) = L_{n-1}$

po prvej runde teda dostaneme $R_{n-1} \quad L_{n-1}$

Feistelova sieť - dešifrovanie



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

začiatok $R_n L_n$

po prvej runde bude

$R_{n-1}\ L_{n-1}$

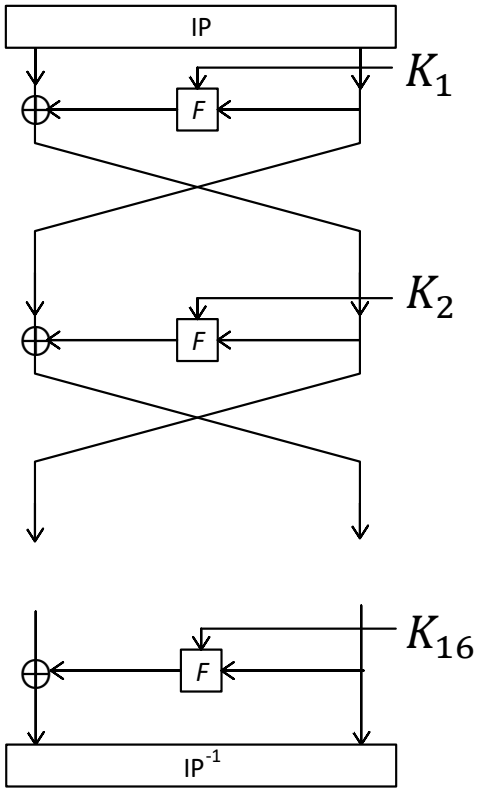
a ďalej podobne až po $R_0 L_0$

dešifrujeme ako $L_0 R_0$
(pridaním výmeny na koniec šifrovania aj dešifrovania)

nie je potrebné poznať inverzné funkcie k F

pri dešifrovaní stačí len zmeniť poradie kľúčov

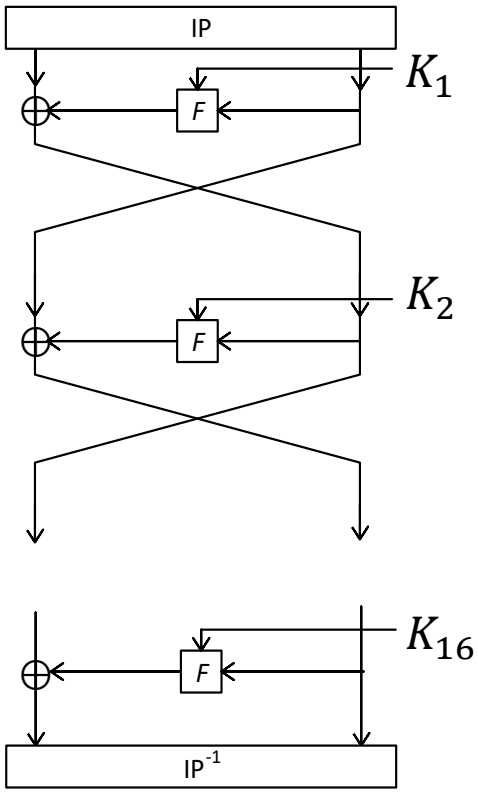
DES – Digital Encryption Standard

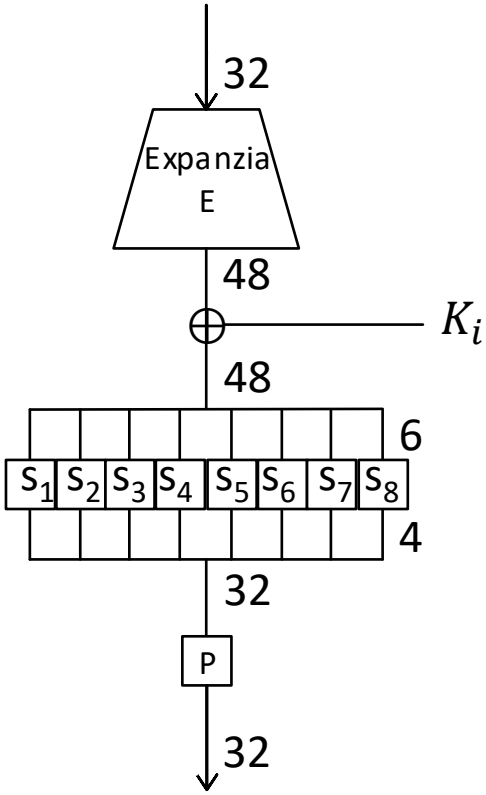


- FIPS (1977-2005) podľa IBM Lucifer
- 64-bitový blok, 16 rúnd
- kľúč 56 bitov –> 16 rundových 48 bitových kľúčov
- inicializačná permutácia (zapojenie vstupov)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

DES – funkcia F





nelineárna funkcia F

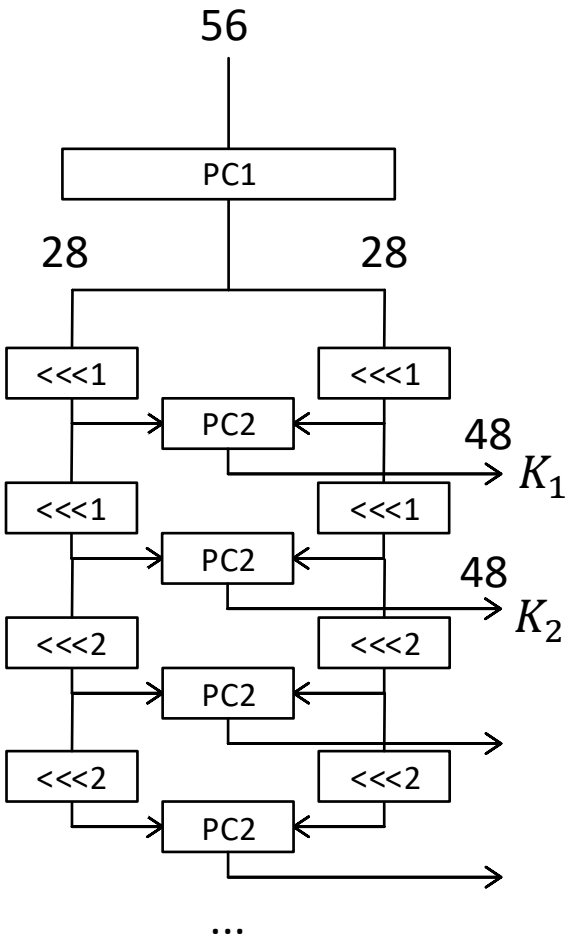
- expanzná permutácia E
- výstupná permutácia P
- 8 substitučných S-boxov

zobrazenia $\{0,1\}^6 \rightarrow \{0,1\}^4$

S-box S_1

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

DES – generovanie kľúčov



odstránenie paritných bitov

začiatočná kľúčová permutácia PC1

kľúč sa rozdelí na 28 bitové polovice C_0 a D_0

for r := 1 to 16 do
  if r ∈ {1,2,9,16} then j := 1 else j := 2 endif;
  $\mathrm{C_r} \leftarrow C_{r-1}$ <<< j
  $\mathrm{D}_r \leftarrow \mathrm{D}_{r-1}$ <<< j
  $K_r \leftarrow \mathrm{PC2}(\mathrm{C_r}, \mathrm{D_r})$
endfor;

PC2 - výstupná výberová permutácia

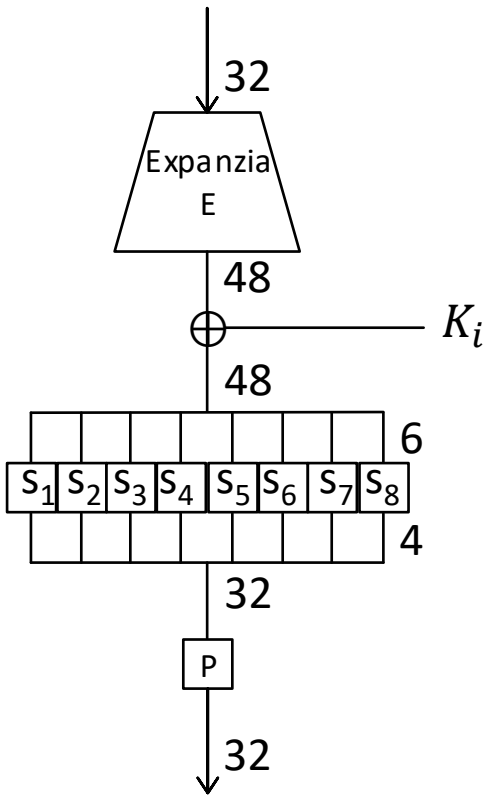
po 28 rotáciách bude $C_{16} = C_0, D_{16} = D_0$

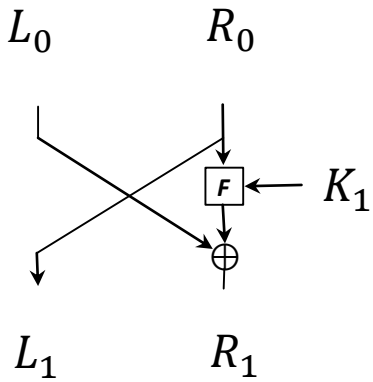
pre dešifrovanie sa použije ten istý postup s opačným smerom posunutia

DES - analýza

- je možné zabezpečiť len výpočtovú bezpečnosť
  (za prelomenie sa považuje útok rýchlejší ako prehľadávanie celej kľúčovej množiny)
- na 56 bitový kľúč je potrebné použiť kvalitný (pseudo)náhodný generátor (nie len 8 znakov ASCII)
- 4 slabé kľúče $E_k\big(E_k(X)\big) = X$ (+12 poloslabých)
- nie je homomorfná šifra $E_{k2}\big(E_{k1}(X)\big) \neq E_{k3}(X)$
- UD (unicity distance) vzdialenosť jednoznačnosti
  $H(K)/H(M) = \log 2^{56} / \log 2^{64} = 0{,}875$
  na úspešný KPA útok stačí jedna dvojica (M,C)

DES – KPA útok na niekoľko rúnd





pre jednu rundu

poznáme L_0, R_0, L_1, R_1

$$L_1 = R_0$$

$$R_1 = L_0 \oplus F(R_0, K_1)$$

$$F(R_0, K_1) = P(S(E(R_0) \oplus K_1))$$

$$K_1 = E(R_0) \oplus \mathrm{S}^{-1}\,(\mathrm{P}^{-1}(\mathrm{L}_0 \oplus R_1))$$

poznáme $E(R_0)$ a $\mathrm{P}^{-1}(\mathrm{L}_0 \oplus R_1)$

na S^{-1} treba vyskúšať $4^8 = 2^{16} = 65536$ možností

pre dve rundy ...

DES – lineárna a diferenciálna kryptoanalýza

- aproximácia S-boxov lineárnymi zobrazeniami
- (Matsui 1994) aspoň 2^{43} párov PT,CT – 10 dní
  - z 2^{43} párov je možné získať 26 bitov, ostatok hrubou silou

- diferenciálna kryptoanalýza - rozdiely medzi vstupmi a výstupmi (čo spôsobí zmena bitu vstupu na výstup)
- pre diferenciálnu kryptoanalýzu DES - 2^{47} choosen PT
  - aproximácia 13 rúnd + hrubá sila
- pomocou známych dvojíc PT/CT je možné dopočítať CT aj pre hľadaný PT (resp. naopak)

TMTO (time memory trade off) útok KPA

pre známu dvojicu (M, C)

- predpočítať tabuľku (k, $DES_k(M)$) pre všetky kľúče a nájsť správny kľúč v konštantnom čase
- náhodne voliť kľúč k a porovnať C a $DES_k(M)$
- (Hellman) dá sa hľadať v čase $O(|K|^{1/2})$ s predpočítanou tabuľkou veľkosti $O(|K|^{1/2})$
- ak veľkosť bloku m sa rovná dĺžke kľúča :

for i = 1 to r { z = rand(x_i); for j = 1 to s {z = $E_z(M)$}; y_i = z }
dostaneme r dvojíc (x_i,y_i) (rainbow table)

vyrobíme maximálne s-prvkový reťazec z_1 = C; {$z_{i+1} = E_{zi}(M)$;},
ak pre nejaké j bude z_i=y_j , potom predchodcom C
v reťazci, začínajúcom x_j musí byť $E_k(M)$

DES – COA analýza

počet možných kľúčov $|K| = 2^{56} \sim 72*10^{15}$
72 057 594 037 927 936 (zo všetkých 2^{64} ! substitúcií)

- 1977 – 10^6 VLSI na testovanie 10^6 k/s – 1 deň – $20 mil.
- 1993 – návrh 5760 VLSI po $10 ~ 1.5 dňa (nerealizované)
- 1997 – DES Challenge (RSA) – 5 mesiacov 25% kľúčov
- 1998 – DES Challenge II-1 - 39 dní 85% kľúčov
- 1998 – EFF – DES Cracker - 1856 ASIC chips - 88 mld k/s
  – DES Challenge II-2 – 56 hodín - $200 tis.
- 1999 – DES Challenge III – DES Cracker + `distributed.net` (100 tis. PC) – 22h15min
- projekt Copacobana (2007) 120 FPGA – 48 mld k/s 9d/$10 tis.
- 2017 dúhové tabuľky (rainbow table) – CPA za 25 s

2DES + KPA útok

2DES $\quad C = DES_r(DES_k(M))$

Meet-in-the-middle útok - ak poznáme dve dvojice (M, C) (M', C')

- $X = DES_k(M)$, $Y = DES_r^{-1}(C)$, $X = Y$ pre správne k a r
- pre všetky k_i nájdeme X_i a uložíme do poľa $K[X_i] = k_i$ (dimenzie 2^{64})
- prechádzame všetky r_j a ak pre $DES_{rj}^{-1}(C) = Y_j$ nájdeme obsadenú pozíciu $K[Y_i]$ v poli K, potom $DES_{K[Yj]}(M) = Y_j = DES_{rj}^{-1}(C)$ teda $(K[Y_i], r_j)$ je vhodná dvojica kľúčov (k,r)
- počet všetkých dvojíc kľúčov je 2^{56}. $2^{56} = 2^{112}$ a počet blokov len 2^{64} teda dostaneme približne $2^{112}/2^{64}$ vhodných riešení (UD $H(K)/H(P) = \log 2^{112}/\log 2^{64} = 1{,}75$)
- potrebujeme aspoň jednu ďalšiu dvojicu (M', C'), na ktorej vyskúšame dvojicu kľúčov $(K[Y_i], r_j)$ – mali by sme dostať približne $(2^{112}/2^{64})(1/2^{64}) = 2^{-16}$ možností, teda ak $DES_{K[Yj]}(M') = DES_{rj}^{-1}(C')$ bude pravdepodobnosť správneho riešenia vysoká
- ak $DES_{K[Yj]}(M') \neq DES_{rj}^{-1}(C')$ musíme pokračovať v prehľadávaní ďalších kľúčov r_j
- počet použití DES je $< 2^{56} + 2^{56} = 2^{57}$
- potrebujeme tiež „vhodne“ uložiť pole veľkosti 2^{64}

TDEA (3DES) a DESx

TDEA (3DES) $\mathrm{C} = \mathrm{DES}_{k_3}(\mathrm{DES}_{k_2}^{-1}(\mathrm{DES}_{k_1}(\mathrm{M})))$

- dešifrovanie M = $\mathrm{DES}_{k_1}^{-1}\left(\mathrm{DES}_{k_2}(\mathrm{DES}_{k_3}^{-1}(C))\right)$
  168 bitový kľúč, ale bezpečnosť len na úrovni 2^{112} (MITM)
- stačí k_1 a k_2 a $\mathrm{C} = \mathrm{DES}_{k_1}(\mathrm{DES}_{k_2}^{-1}(\mathrm{DES}_{k_1}(\mathrm{M})))$ 112 bitový kľúč
- pre $k_3 = k_2 = k_1$, $3\mathrm{DES}_{k_1 k_2 k_3}$ = DES_{k_1} (3DES funguje aj ako DES)

DES-X (Rivest, Killian) $\mathrm{C} = k_3 \oplus \mathrm{DES}_{k_1}(\mathrm{M} \oplus k_2)$

- M = $k_2 \oplus \mathrm{DES}_{k_1}^{-1}(\mathrm{C} \oplus k_3)$
- k_1 56 bitový a k_2, k_3 64 bitové – spolu 184 bitový kľúč
  rýchlejší výpočet, bezpečnosť na úrovni 2^{119}
- key whitening

Odporúčané dĺžky kľúčov

Attacker	Budget	Hardware	Min security
“Hacker”	0	PC	58
	< $400	PC(s)/FPGA	63
	0	”Malware”	77
Small organization	$10k	PC(s)/FPGA	69
Medium organization	$300k	FPGA/ASIC	69
Large organization	$10M	FPGA/ASIC	78
Intelligence agency	$300M	ASIC	84

From “ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012)”

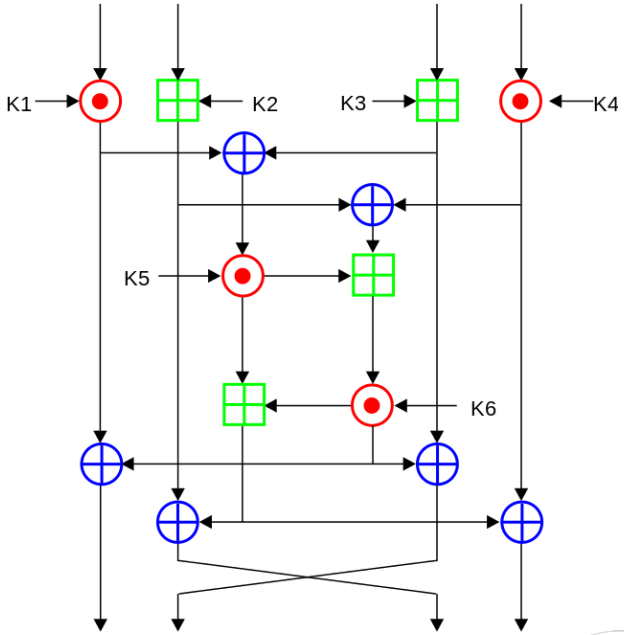
Stupne zabezpečenia

32	Real-time, individuals	Only auth. tag size
64	Very short-term, small org	Not for confidentiality in new systems
72	Short-term, medium org	
	Medium-term, small org	
80	Very short-term, agencies	Smallest general-purpose
	Long-term, small org	< 4 years protection (2-key 3DES, < 240 PT/CT)
96	Legacy standard level	10 years protection (2-key 3DES, < 10^6 PT/CT)
112	Medium-term protection	20 years protection (3-key 3DES) (2023)
128	Long-term protection	30 years Good, generic application-indep. (2030)
256	”Foreseeable future”	

From “ECRYPT II Yearly Report on Algorithms and Keysizes (2012)”

IDEA

- International Data Encryption Algorithm (1991)
- náhrada za DES počas licenčných obmedzení
- pre otvorené riešenia (PGP, ...)
- 64 bitový blok, 128 bitový kľúč
- 8 rúnd jednoduchých operácií (celočíselných 16-bitových)
- Lai-Massey schéma – podobne ako Feistel – dešifruje sa šifrovacou funkciou s opačným poradím kľúčov



Ďakujem za pozornosť.

jozef.jirasek@upjs.sk