Bezpečnost v informačních technologiích (KIV/BIT)

3. Moderní symetrická kryptografie

Ing. Pavel Král, Ph.D.

Katedra informatiky a výpočetní techniky
Západočeská Univerzita

2. března 2016

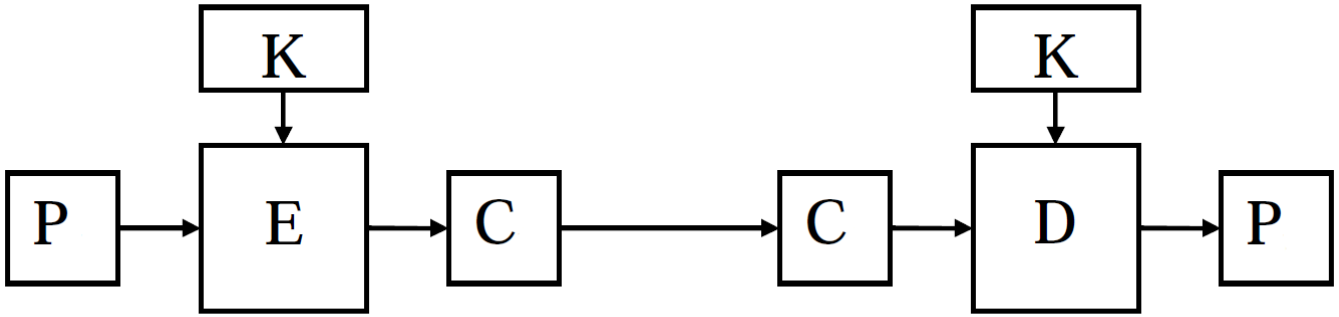
Obsah

Moderní kryptografie

- **historie:** jednoduchost, závislost bezpečnosti na utajení šifrovacího algoritmu, později na délce klíče
- **dnes:** složitá šifrovací funkce (složena z jednodušších) $\rightarrow$ neprolomení při znalosti libovolného množství zvoleného plaintextu (= odolnost na *chosen plaintext attack*)
- použití u tzv. **Produkčních šifer**
- kombinace několika transformací $\rightarrow$ větší bezpečnost

- použité operace:
  - transpozice
  - substituce
  - aritmetické operace (např. součet nebo násobení modulo)

Symetrické šifry



- E šifrovací fce.
- D dešifrovací fce.
- K šifrovací (= dešifrovací) klíč
- P plaintext (znak, blok)
- C šifrový text

Šifrování

- $C = E_K(P)$

Dešifrování

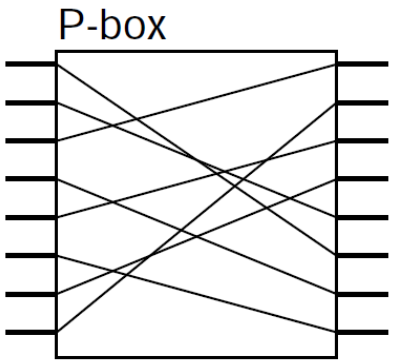
- $P = D_K(C)$

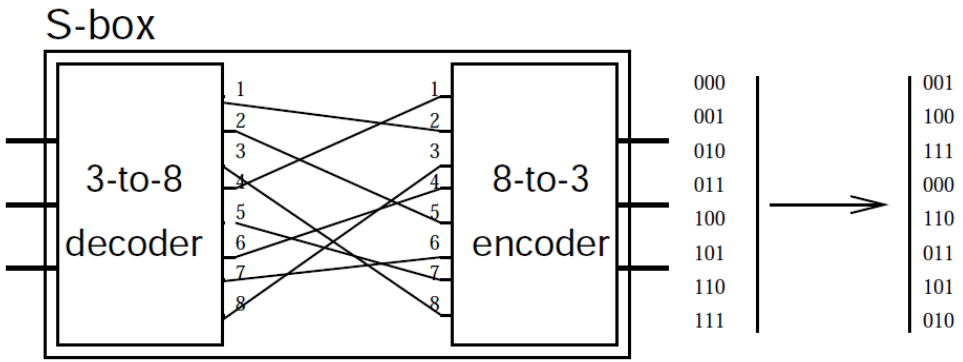
- problém distribuce klíče $\leftarrow$ utajení

S-P síť

= substitučně permutační síť

- základ produkční šifry
- složení: **S**ubstituce + **P**ermutace
- P-box (permutace) - transpozice vstupu
- S-box - substituce
- Př:



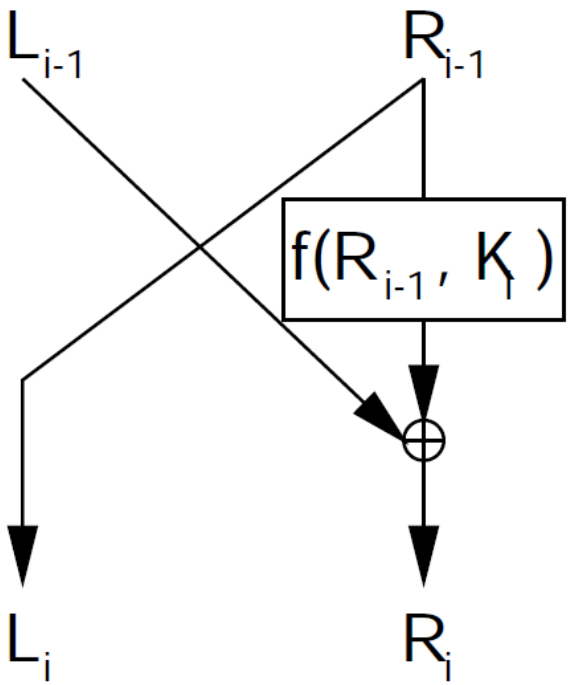


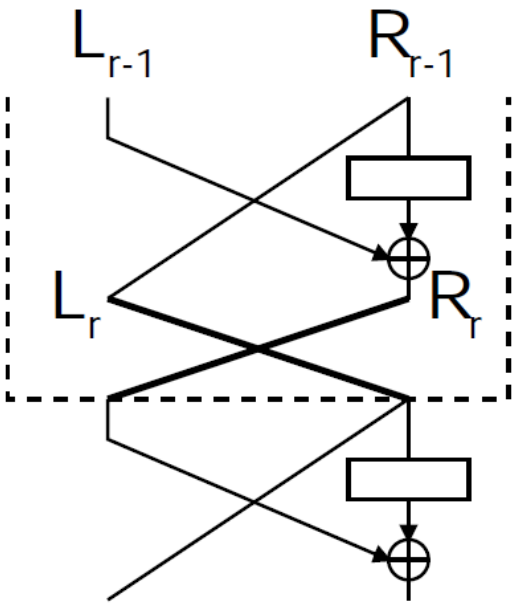
Feistelova síť

- 1973 Feistel
- základ většiny moderních blokových šifer
- několikanásobné opakování jednoduchých operací *XOR*
- $P = (L_0, R_0)$ **blok** ot. textu P rozdělení na poloviny, každá délku d
- klíč K rozdělen na n podklíčů $k_1, k_2, .., k_n$; n představuje počet iterací algoritmu
- každý podklíč k_i definuje funkci f_i
- každá iterace: $L_i = R_{i-1}$, $R_i = L_{i-1} \otimes f(R_{i-1}, k_i)$
- po poslední iteraci záměna L_n a R_n

Feistelova síť

- dešifrování je možno, i když funkce $f()$ není invertovatelná
- klíče jsou použity v opačném pořadí





- nutnost použití jiného klíče v každé iteraci, pokud ne $\rightarrow$ slabá šifra

Feistelova síť - příklad

- $n = 2$, délka bloku $= 4$
- k_1: $00 \rightarrow 10 \quad 01 \rightarrow 00 \quad 10 \rightarrow 11 \quad 11 \rightarrow 01$
- k_2: $00 \rightarrow 00 \quad 01 \rightarrow 11 \quad 10 \rightarrow 10 \quad 11 \rightarrow 01$
- $P = 0011$

Feistelova síť - příklad - řešení

- $n = 2$, délka bloku $= 4$
- k_1: $00 \rightarrow 10$ $01 \rightarrow 00$ $10 \rightarrow 11$ $11 \rightarrow 01$
- k_2: $00 \rightarrow 00$ $01 \rightarrow 11$ $10 \rightarrow 10$ $11 \rightarrow 01$
- $P = 0011$

Šifrování

- $iter.1$: $0011 \rightarrow 1101$ (aplikace k_1)
- $iter.2$: $1101 \rightarrow 0100$ (aplikace k_2)
- $C = 0001$ (záměna L_2 a R_2)

Dešifrování

- $iter.1$: $0001 \rightarrow 0111$ (aplikace k_2)
- $iter.2$: $0111 \rightarrow 1100$ (aplikace k_1)
- $P = 0011$ (záměna L_2 a R_2)

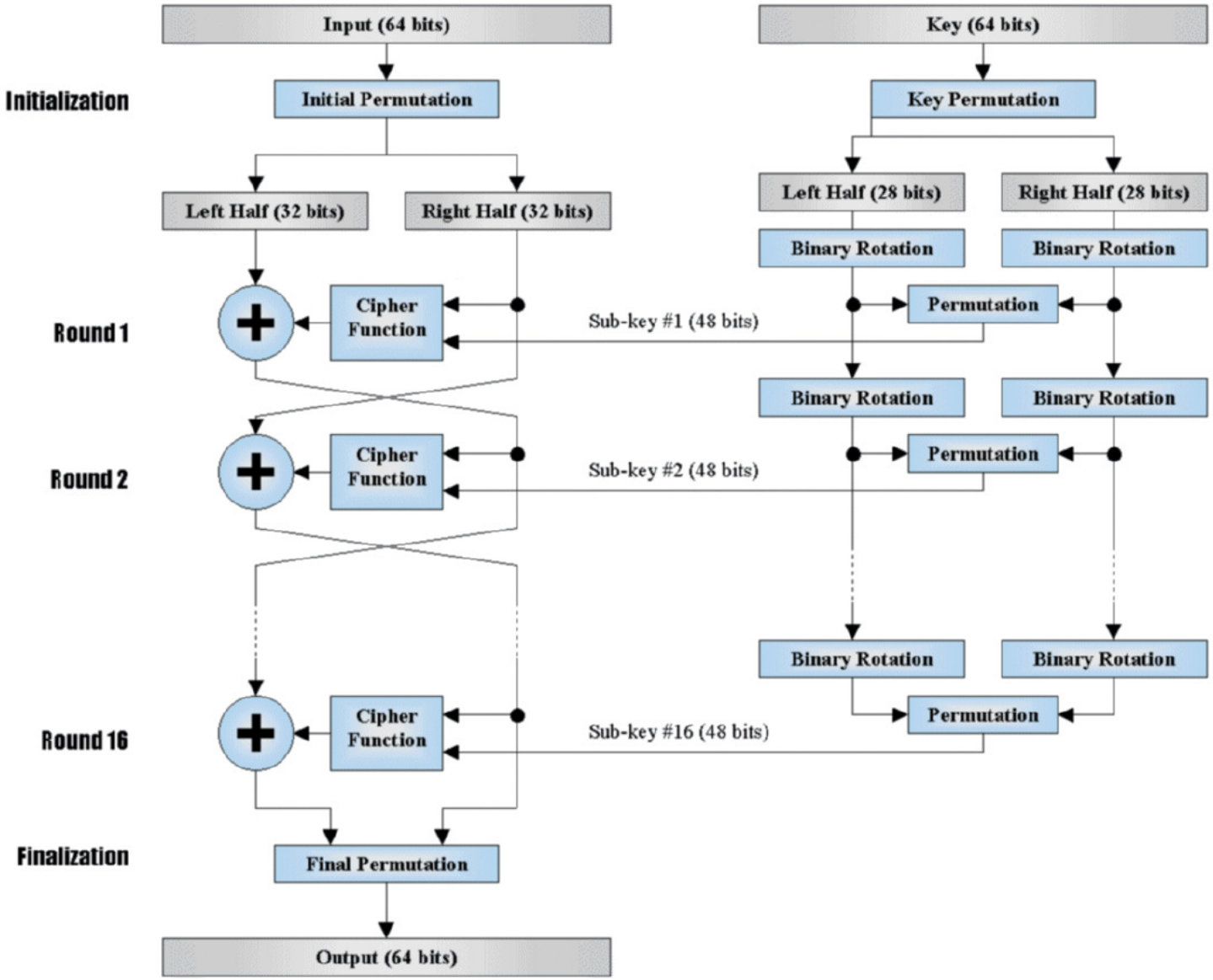
DES

- potřeba standardního šifrovacího algoritmu pro veřejnost
- $\rightarrow$ návrh algoritmu Data Encryption Standard (DES) - výzkumníci z IBM
- předáno National Bureau of Standards (NBS)
- r. 1977 - schválení (po modifikacích) jako vládní standard pro šifrování v USA

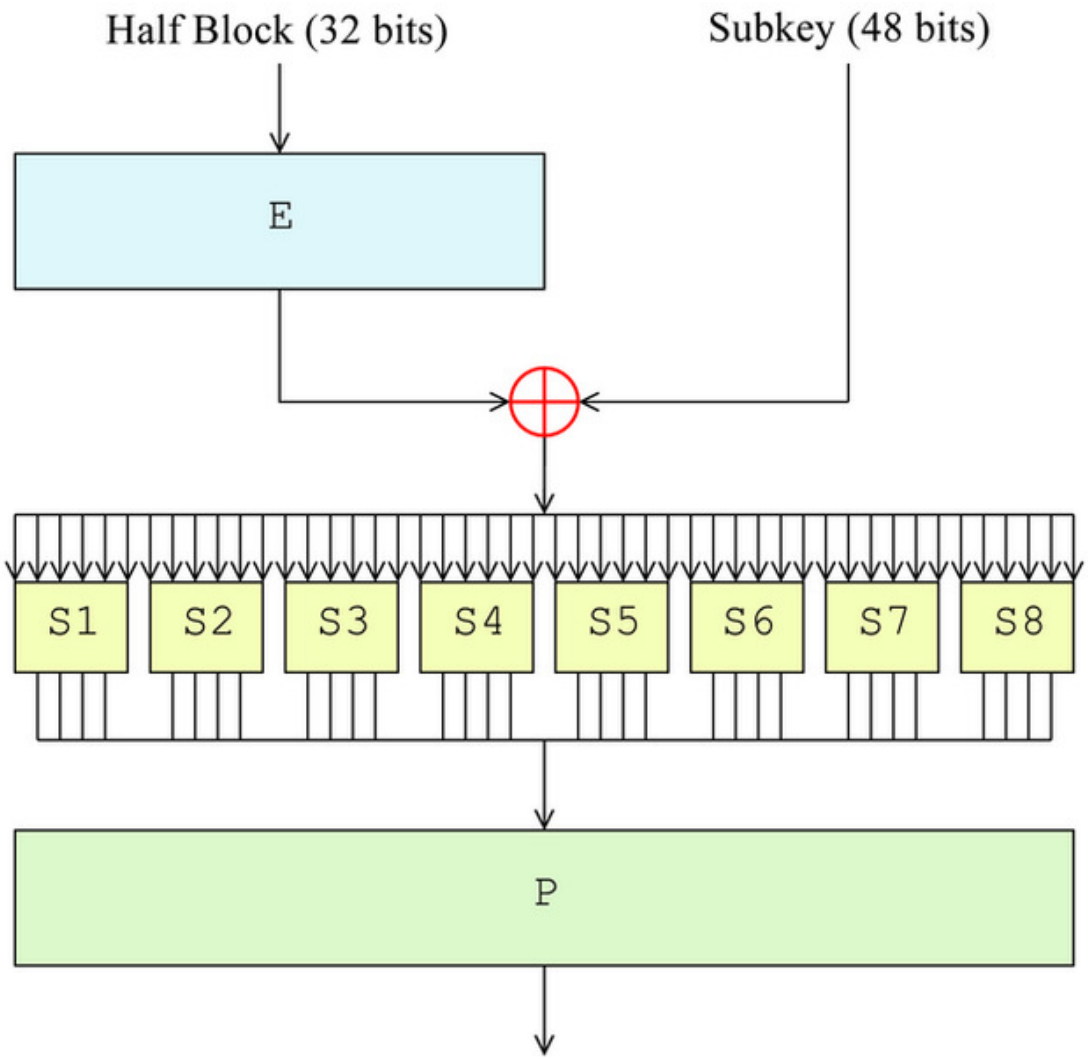
- feistelova síť, 16 iterací, každá iterace podklíč 48 bitů
- délka bloku = 64 bitů, klíč 64 bitů (56 efektivních, 8 kontrolních), symetrická šifra

- dnes považována za nespolehlivou $\leftarrow$ efektivní klíč pouze délky 56 bitů
- $\rightarrow$ prolomení útokem hrubou silou za méně než 24 hodin
- nahrazen variantou Triple DES (trojnásobný DES $\rightarrow$ pomalé), dnes spíše metodou Advanced Encryption Standard (AES)

DES - blokové schéma



DES - šifrovací funkce



DES - počáteční (a konečná) permutace

IP							
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

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

- číst zleva doprava, shora dolů
- = bit otevřeného textu na pozici 58 $\rightarrow$ pozice 1, bit na pozici 50 $\rightarrow$ pozice 2, ...

DES - šifrovací funkce

Expanzní a P-box permutace

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

- E = expanzní permutace z 32 na 48 bitů (bit na pozici 1 $\rightarrow$ pozice 2 a zároveň 48)
- P = permutace na 32 bitech

DES - šifrovací funkce

Substituce (S-box S1)

Row / Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Př:

- vstup 1. S-boxu (tj. bity 1-6) = 110011
  - prvý a poslední bity = 11 $\rightarrow$ 3-tí řádek
  - prostřední bity = 1001 $\rightarrow$ sloupec 9
- číslo 110011 $\rightarrow$ 1011 (des. číslo 11)

DES - dešifrování

- Feistelova síť $\rightarrow$
  - použití shodného algoritmu pro šifrování i dešifrování
  - klíče v opačném pořadí
  - tj.
    - Šifrování: $k_1, k_2, .., k_{16} \rightarrow$ Dešifrování: $k_{16}, k_{15}, .., k_1$
    - algoritmus generování klíčů je shodný jako pro šifrování $\times$ posun bitů **doprava**

DES - způsoby (módy) provozu

- možnost zpracování bloků různým způsobem
- projeví se, když má otevřený text více než jeden blok
- nejjednodušší způsob = elektronická kódová kniha (Electronic Code Book (ECB))
  - postupné zpracování ot. textu blok po bloku

Problémy:

- stejné bloky otevřeného textu vždy zašifrovány stejně
- nalezení několika stejných bloků šifrového textu $\rightarrow$ v některých případech možnost určení plaintextu
- **možnost libovolného vkládání, zaměňování** nebo **mazání bloků**
- $\rightarrow$ není zajištěna integrita otevřeného textu

DES - ECB útok

Př:

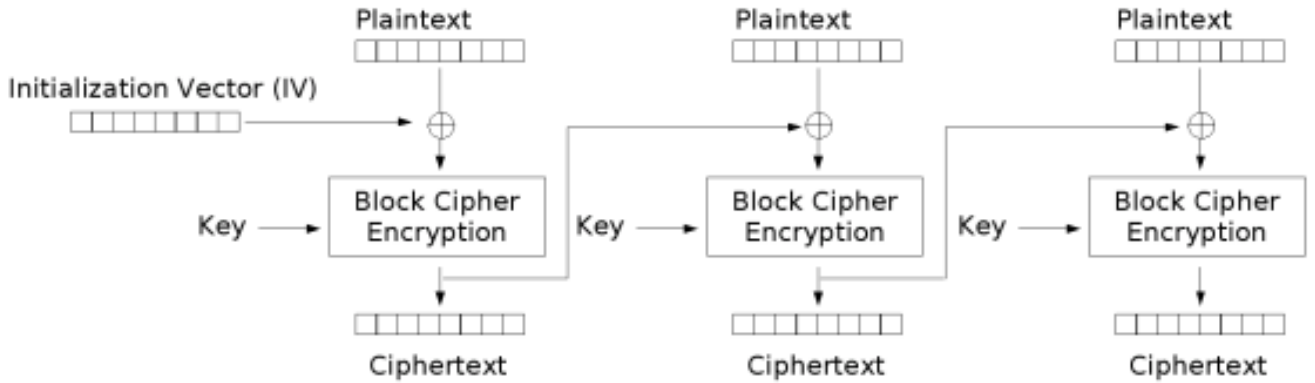
- zaslání zašifrovaného souboru s výplatami zaměstnanců
- rozdělení po 64 bitových blocích + zašifrování

Jiří Vot	ava	plat: 20	500,- Kč
Josef Bo	hatý	plat: 50	100,- Kč
Bohouš P	odvodník	plat: 10	500,- Kč

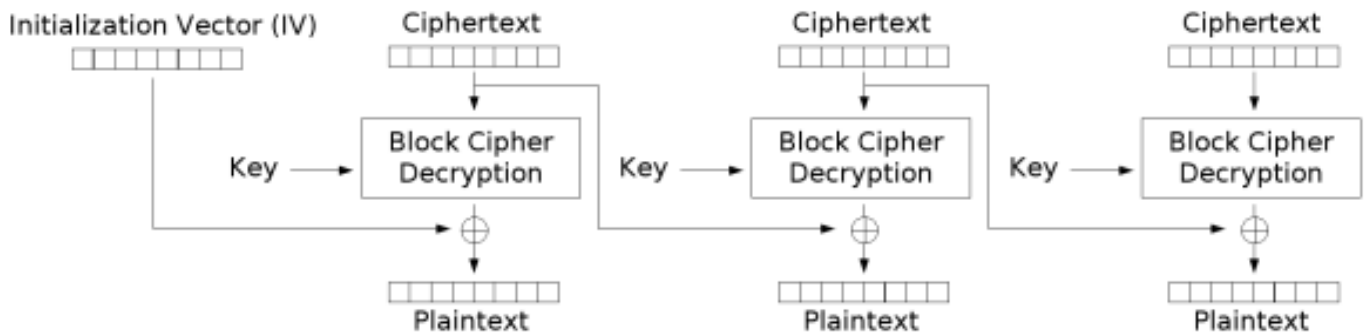
- útočník: přístup pouze k zašifrovanému souboru
- např:
  - prohození bloků 7 a 11
  - vložení bloku 7 i na pozici 11
- $\rightarrow$ nedoporučuje se použití ECB při šifrování zpráv delších než 1 blok

DES - Cipher Block Chaining (CBC) mode

(řetězení šifrového textu)

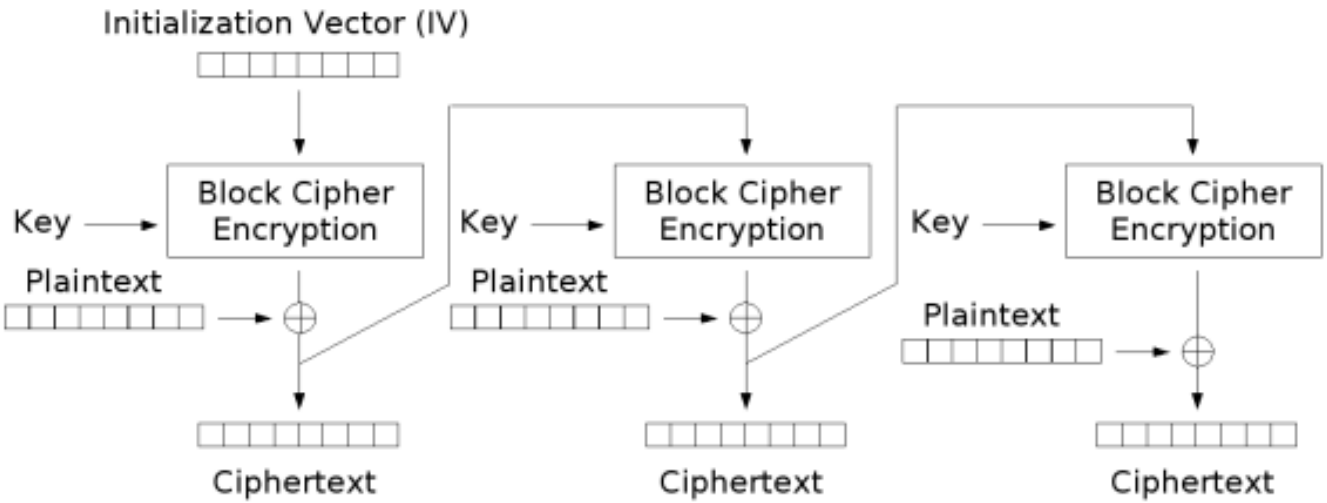


Cipher Block Chaining (CBC) mode encryption

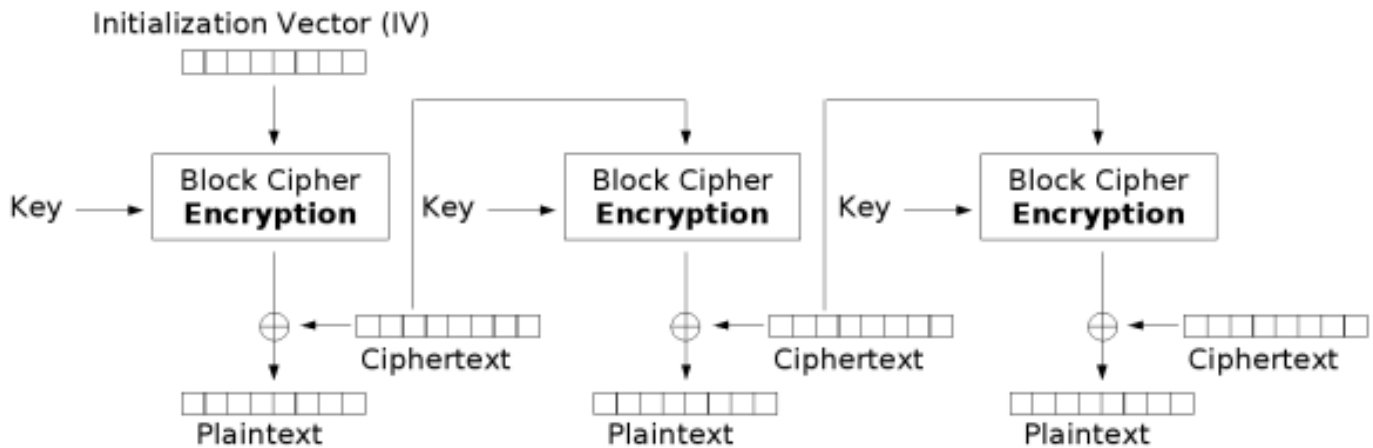


Cipher Block Chaining (CBC) mode decryption

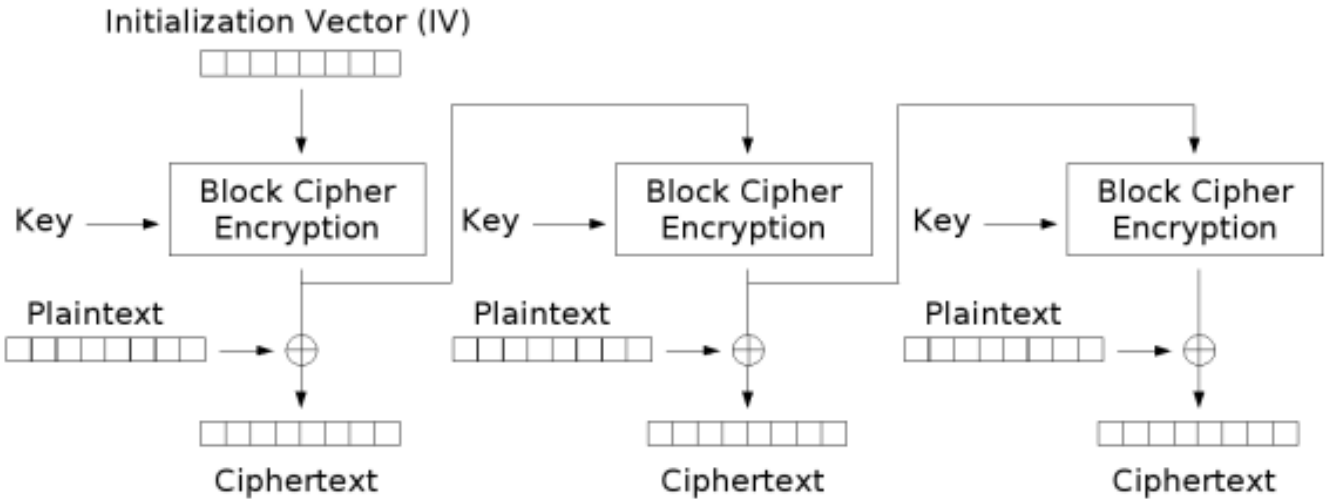
DES - Cipher FeedBack (CFB) mode



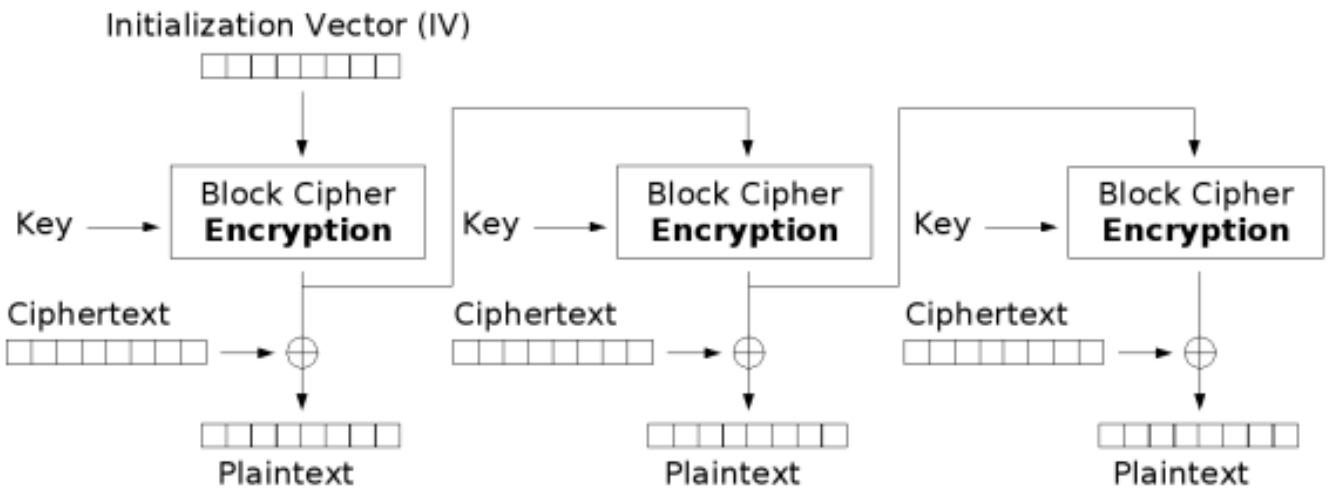
Cipher Feedback (CFB) mode encryption



DES - Output FeedBack (OFB) mode



Output Feedback (OFB) mode encryption



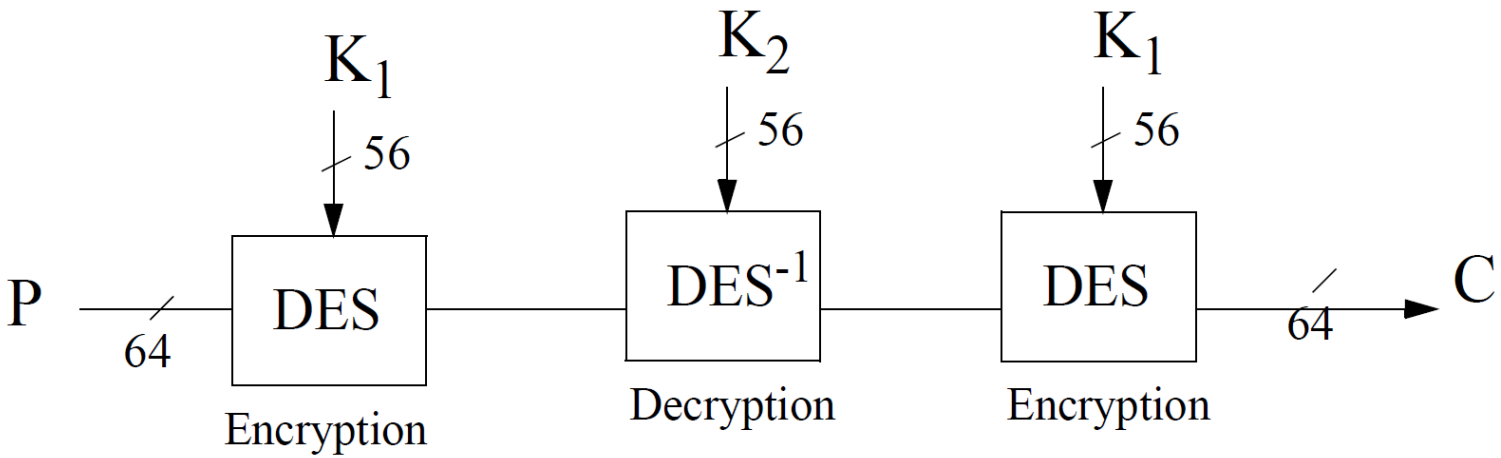
Slabé (a poloslabé) klíče

- rozdělení klíče na poloviny + rotace $\rightarrow$
- klíče samé 0 (nebo 1) v polovinách se nemění v iteracích algoritmu DES $\rightarrow$ *slabé*
- (hex. zápis) 0000000 0000000, FFFFFFF FFFFFFF, ...
- platí: $k_1, .., k_{16} = K$ shodné $\rightarrow E(E(P, K), K) = P$

Poloslabé klíče

- dvojice klíčů, která šifruje text na původní text, tj.
  - k_2 rozšifruje zprávu zašifrovanou klíčem k_1 (a naopak)
  - možno díky algoritmu generování klíčů
  - místo 16ti klíčů pouze 2, každý použit 8 krát
  - např (hex.): 01FE 01FE 01FE 01FE, FE01 01FE 01FE 01FE, ...
  - platí: $E(E(P, k_2), k_1) = P$ a $E(E(P, k_1), k_2) = P$
- **nepoužívat!**

Triple DES



- celkem možných klíčů 2^{112} ($\times$ jednoduchý DES $= 2^{56}$)
- možnost dále využívat HW & SW původního DES algoritmu
- dostatečná bezpečnost $\times$ rychlost
- paranoidní varianta: E-E-E se třemi různými klíči (2^{168} klíčů)

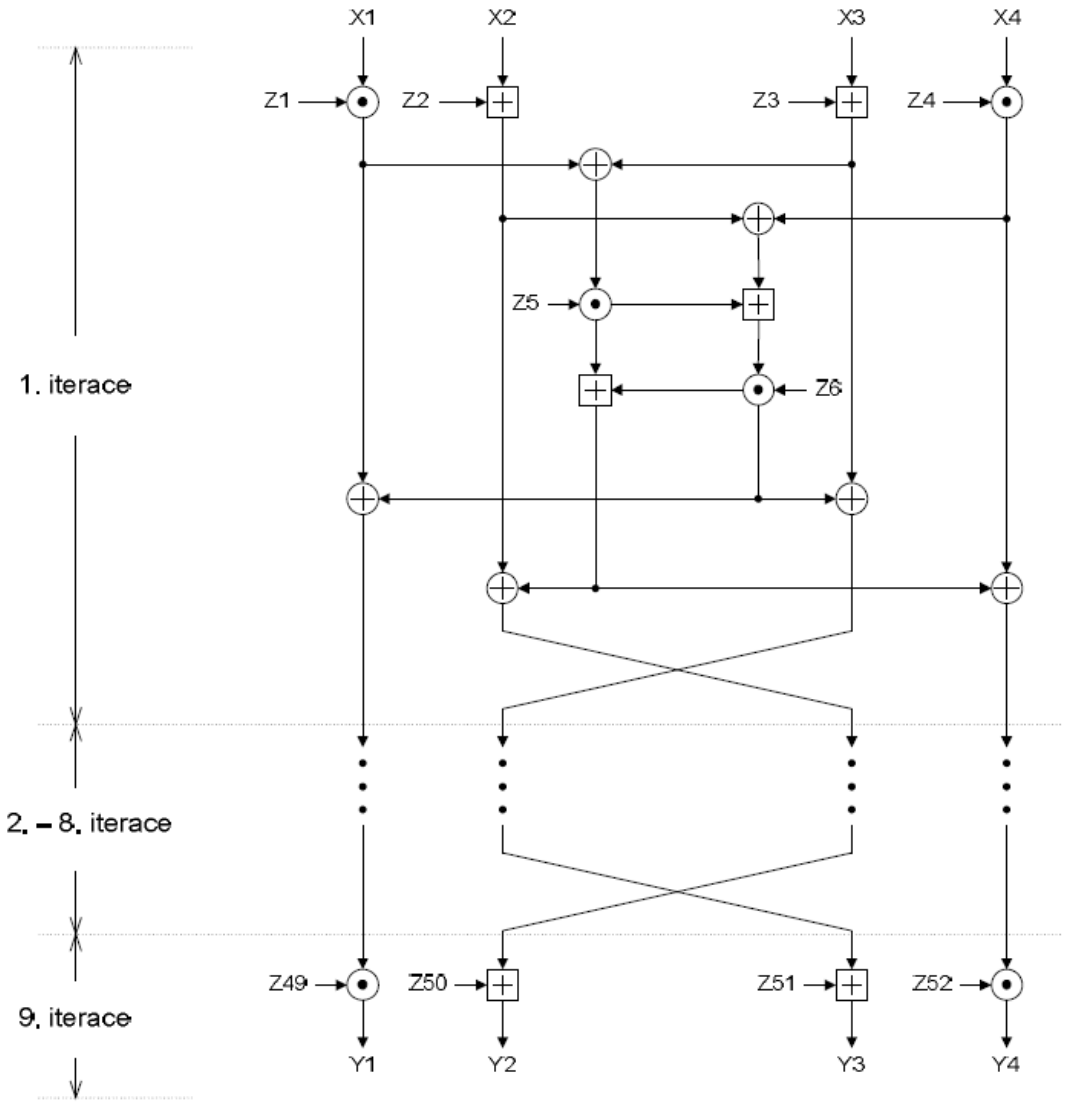
IDEA

- "nástupce" DESu, pravděpodobně nejlepší symetrický blokový algoritmus
- 1991 - návrh Xuejia Lai a James L. Massey ze Švýcarského národního technologického institutu (ETHZ)
- drobným přepracováním dřívější šifry Proposed Encryption Standard (PES)
- původní název Improved PES (IPES)
- komercializace pod názvem International Data Encryption Algorithm (IDEA)
- implementován v rámci protokolu SSL nebo jako součást PGP
- patentován, pro nekomerční použití zdarma

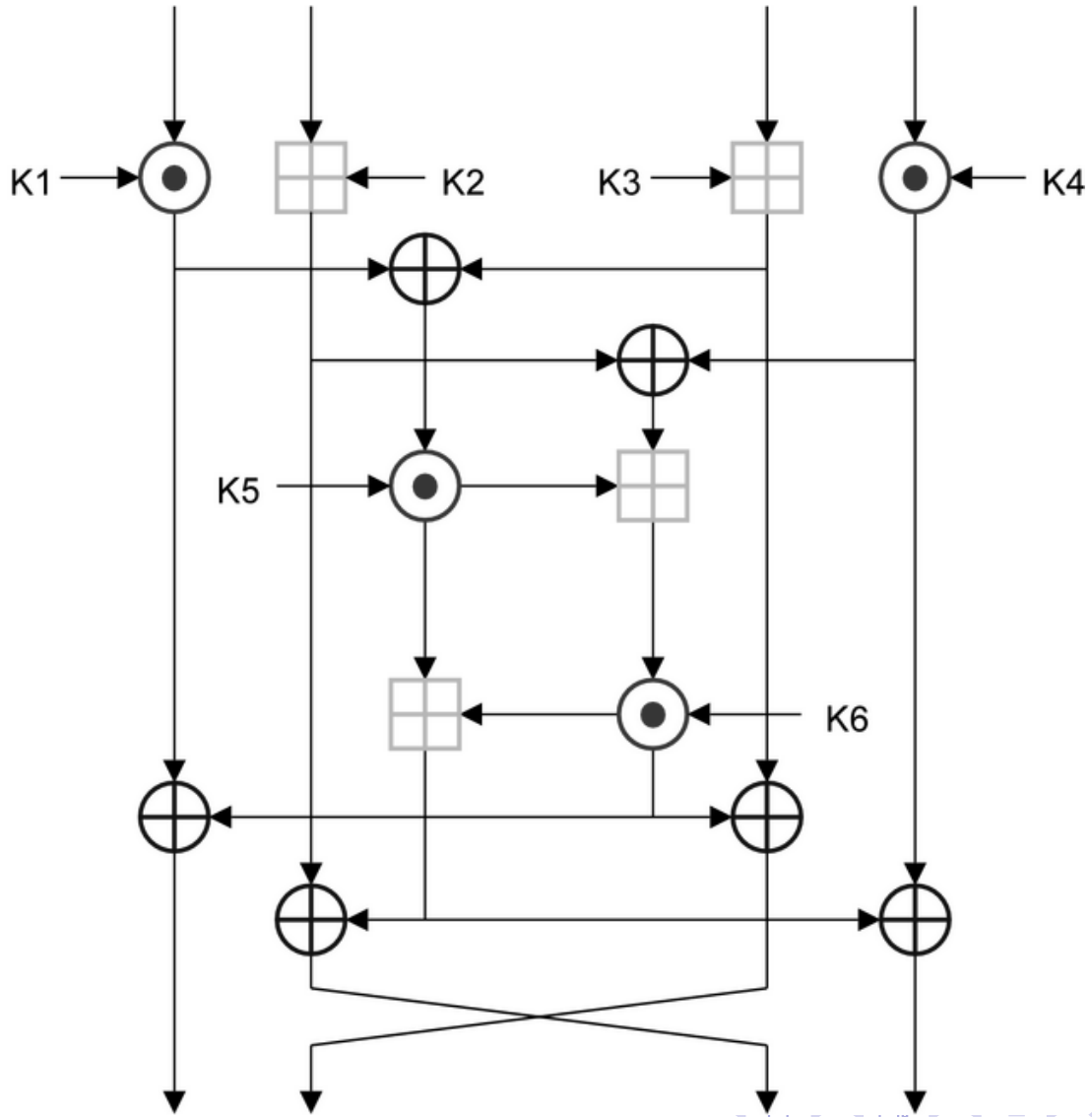
IDEA

- blok 64 bitů; klíč 128 bitů
- využití tří základních operací:
- $\oplus$: XOR 16-bit. subbloků: $a\ XOR\ b$
- $\boxplus$: modulární součet 16-bit. subbloků: $(a + b) mod 2^{16}$
- $\odot$: modulární násobení 16-bit. subbloků: $(a * b) mod 2^{16} + 1$

IDEA - schéma algoritmu (celek)



IDEA - schéma algoritmu (detail jedné iterace)



IDEA - poznámky, dešifrování

- výstup operace nikdy použit jako vstup operace stejného typu
- 2x rychlejší než DES $\times$ výrazně bezpečnější
- patentování šifry IDEA $\rightarrow$ vznik nepatentových šifer např v r. 1994 Blowfish a SAFER
- útoky: Daemen 1994-5: nalezení několika tříd slabých klíčů
  - pravděpodobnost náhodného výběru slabého klíče zanedbatelná $P = 2^{-77}$
- **bezpečná!**

Dešifrování:

- stejný algoritmus (schéma) jako šifrování
- dešifrovací klíče z šifrovacích (aditivní příp. multiplikativní inverze)

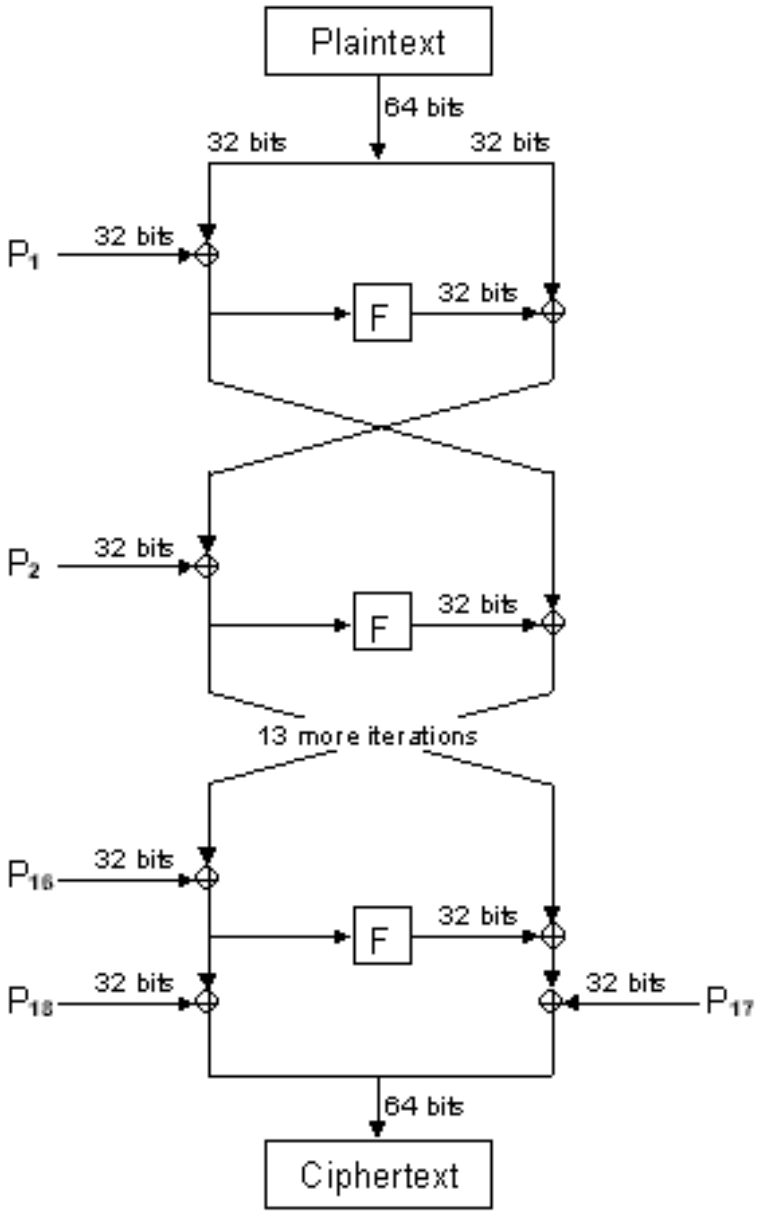
Blowfish

- navržena B. Schneierem; poprvé zveřejněna v r. 1994
- (opět) symetrická bloková šifra
  - blok délky 64 bitů
  - proměnná délka klíče: 32-448 bitů
  - Feistelova síť; 16 iterací

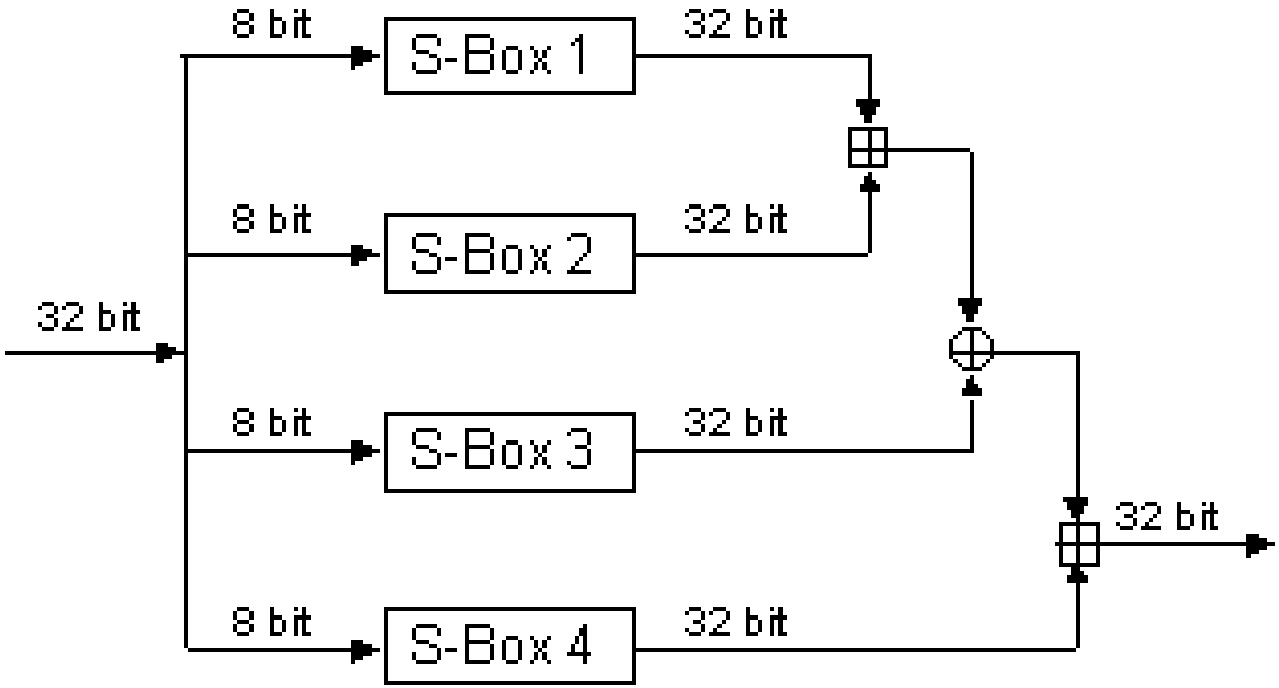
Algoritmus:

- expanze klíče (vytvořeno 18 podklíčů - uložení v P-polích - a obsah 4 S-Boxů)
- šifrování dat

Blowfish - schéma algoritmu



Blowfish - schéma šifrovací funkce



- vstup (32-bit): i $= (i_1, i_2, i_3, i_4)$
- výstup: $F(i) =$
  $((((S_1(i_1) + S_2(i2)) mod 2^{32})\ XOR\ S_3(i3)) + S_4(i_4)) mod 2^{32}$

Blowfish - poznámky, dešifrování

- nepatentována
- návrh pro implementaci na 32-bit. procesorech
- útoky: 1995 - Vaudenay
  - nalezení množiny slabých klíčů (pravděpodobnost $P = 2^{-14}$)
  - $\times$ zatím nenalezen způsob využití
- bezpečná

Dešifrování:

- stejné jako šifrování,
- klíče v opačném pořadí

Advanced Encryption Standard (AES)

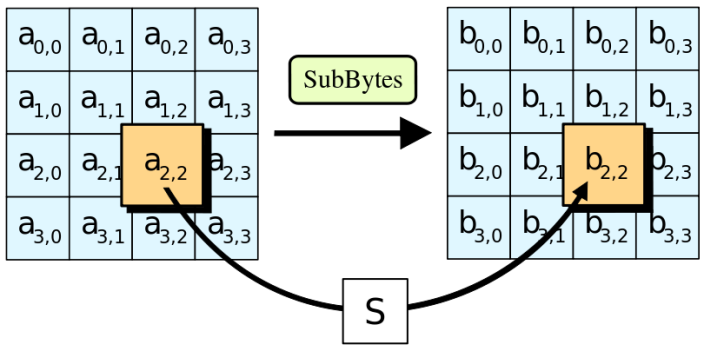
- neúspěch DES (jednoduchý není bezpečný, 3DES pomalý) $\rightarrow$ vyhlášení volné soutěže o návrh nového algoritmu
- 2002 - vítěz algoritmus Rijndael (podle tvůrců Rijmen & Daemen)
- $\rightarrow$ název Advanced Encryption Standard (AES)

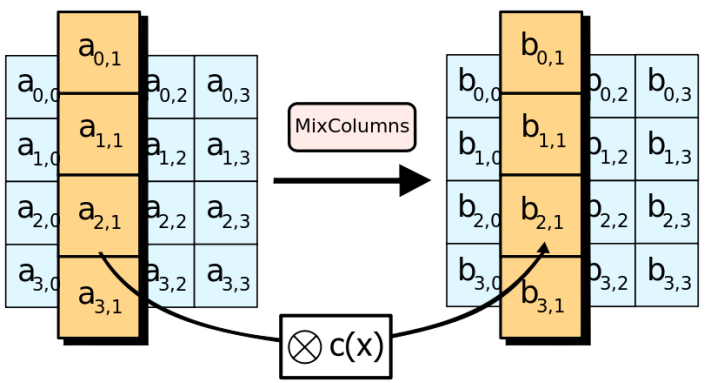
- různé délky bloku a klíče: 128, 192,256 (i 512)
- počet iterací dle dle délky bloku (klíče)
- dále popis pro délky 128 bitů
- data i klíč = matice 4×4 byty

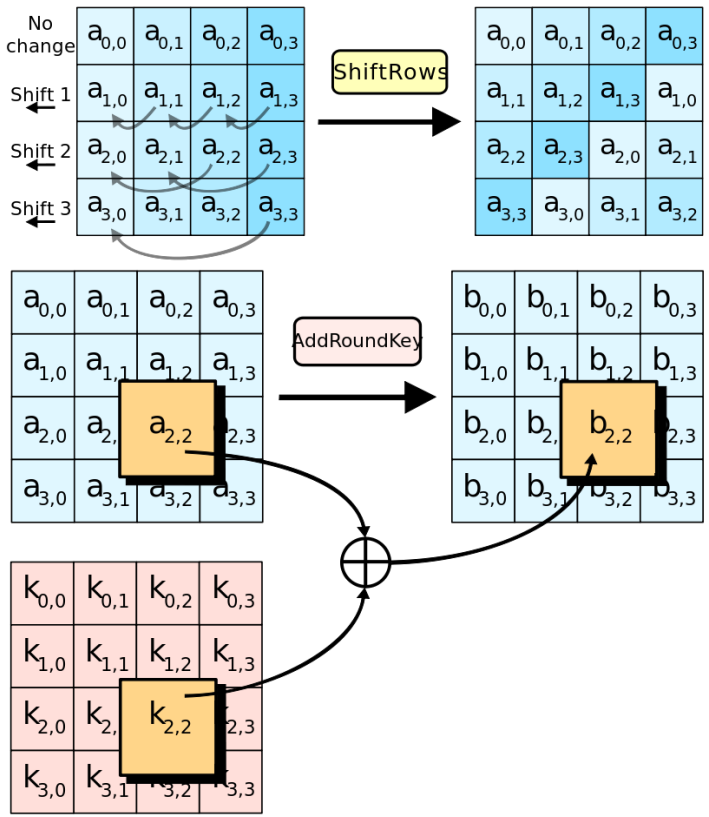
Advanced Encryption Standard (AES)

- začátek: *XOR* vstup + podklíč
- 10. iterací
  1. S-Box substituce - nelineární algoritmus $\rightarrow$ velký rozdíl v bezpečnosti $\times$ DES
  2. Permutace - cyklický posun řádků dat o 0, 1, 2 a 3 pozice
  3. MixColumns - násobení sloupců konst. polynomem
  4. AddRoundKey - šifrová fce. (*XOR* matice a podklíče)
- poslední iterace: vynechán krok (3)

Advanced Encryption Standard (AES)







Srovnání symetrických blokových šifer

	DES	3DES	IDEA	BlowFish	AES	SkipJack	WinCros
Délka klíče	56	112	128	448	128, 192, 256, 512	80	80-240
Popis	veřejný	veřejný	veřejný	veřejný	veřejný	veřejný	na základě smlouvy
Licenční poplatky	ne	ne	ano	freeware	ne	ne	obsaženy v pro-duktu
# iterací	16	3×16	8	16	dle délky klíče 10,..	32	8-63