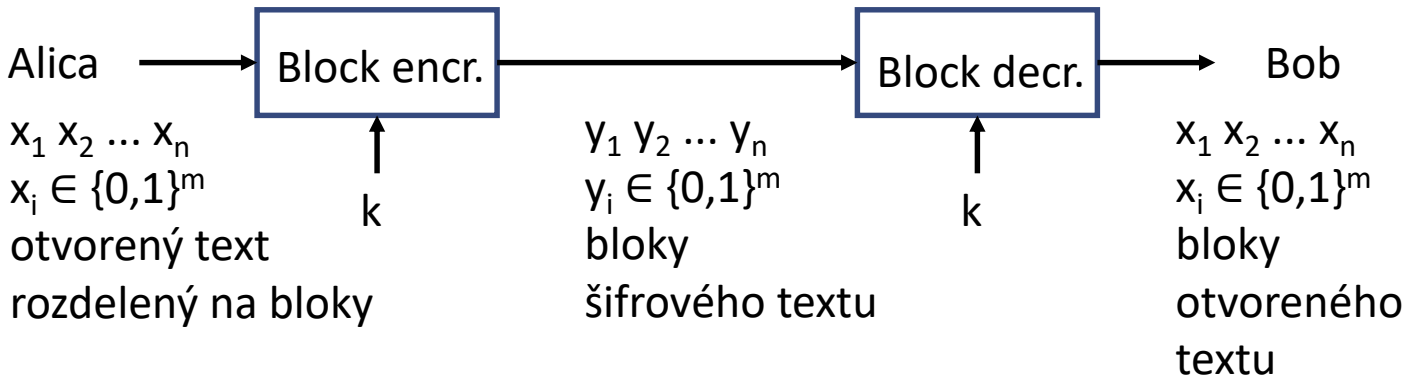
Kryptografické systémy
Blokové šifry 2

doc. RNDr. Jozef Jirásek, PhD.

ZS 2023

Blokové symetrické šifrovacie systémy

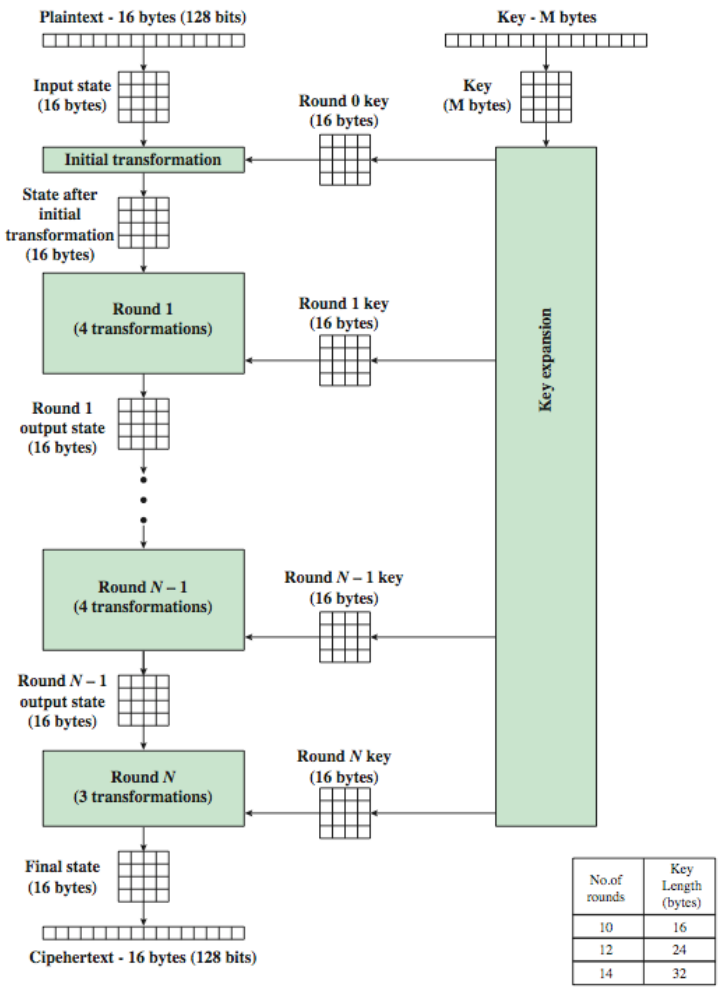


- delenie textu na bloky rovnakej veľkosti (pre difúzie)
- šifrovanie rovnakých blokov tým istým kľúčom bude rovnaké – blok musí byť dostatočne veľký, aby sa nedali využiť štatistické metódy resp. kódovacie tabuľky pre každý kľúč
- kľúč aspoň taký veľký ako blok
- efektívny výpočet na existujúcom hw

AES (Advanced Encryption Standard) konkurz

- NIST – 1997-2000 – konkurz na novú blokovú šifru
  - 128 bitové bloky
  - 128, 192, 256 bitové kľúče
  - pre rôzne typy procesorov
  - „lepší“ ako 3DES
- 1999 finalisti Mars, RC6, Rijndael, Serpent, Twofish
- 2001 za AES bol vybratý Rijndael (Rijmen, Daemen)

AES proces



No.of rounds	Key Length (bytes)
10	16
12	24
14	32

- 128 bitové bloky
- 128, 192, 256 bitové kľúče
- SPN s 10, 12, 14 rundami (nie Feistelovho typu)

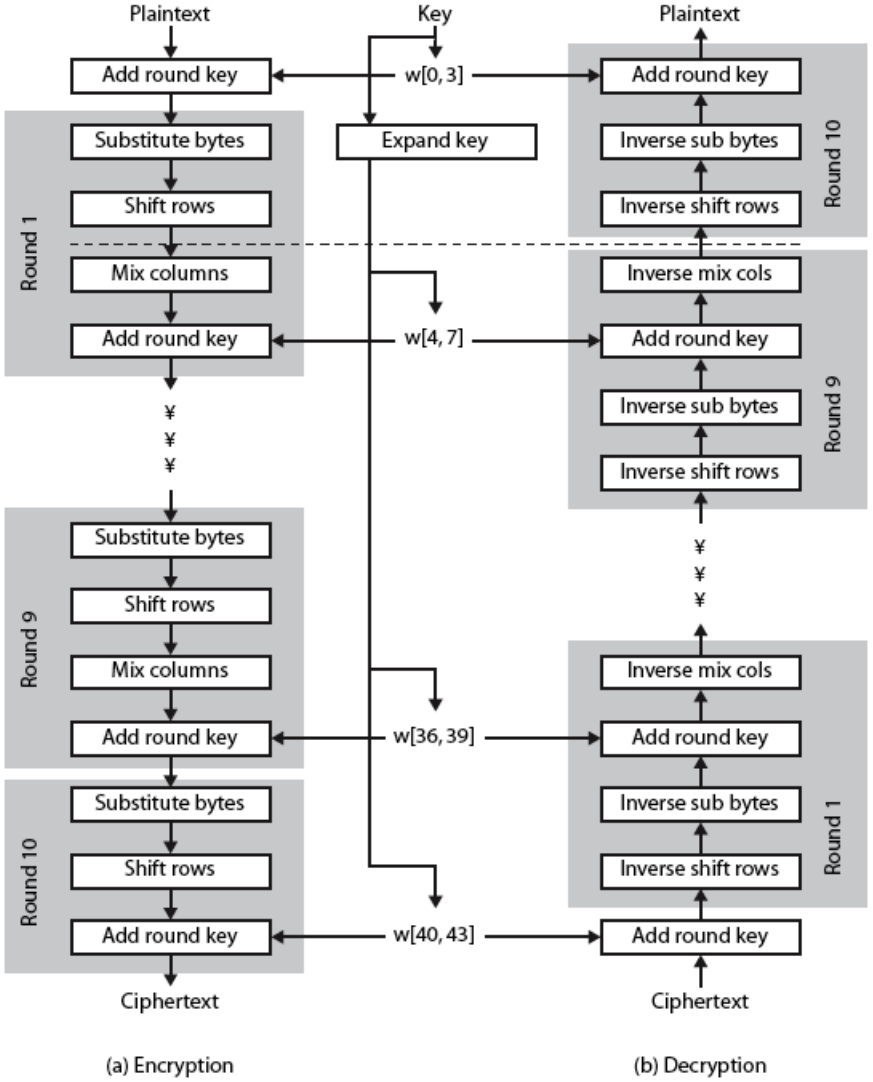
pracuje s 4x4 8-bitovými blokmi (8b, 32b, 128b µP)

8-bitové substitúcie s jediným S-boxom

len XOR a prehľadávanie tabuliek

whitening

AES štruktúra



- striedanie štyroch štádií

`AddRoundKey` – jediná používa kľúč – XOR spôsobom

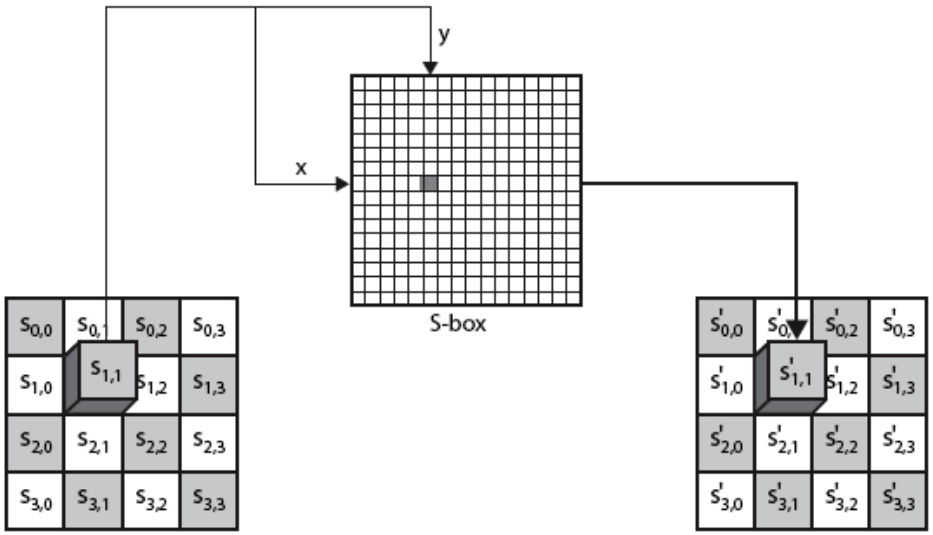
`SubBytes` – S-box substitúcia po bajtoch (tabuľkou)

`ShiftRows` -transpozícia

`MixColumns` – kombinácia stĺpcov

- pri dešifrovaní - inverzné funkcie a opačné poradie kľúčov
- štádiá SR,SB a MC,ARK sú navzájom komutatívne

AES SubBytes



- jednoduchá substitúcia po bajtoch
- tabuľka 16x16 s permutáciou 256 rôznych bajtov (dá sa aj vypočítať)
- 4 b riadok, 4 b stĺpec
- inverzná tabuľka pre inverznú substitúciu

jediná (dokázateľne) nelineárna operácia $SB(x) + SB(y) \neq SB(x+y)$

AES SubBytes

6e = 6 e

S(6e) = 9f

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
4x	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

AES SubBytes

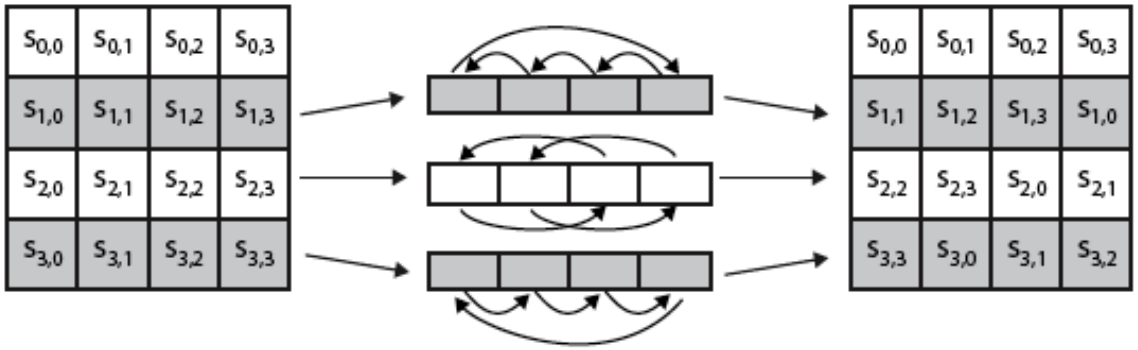
S-box

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

inverse S-box

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1x	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2x	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3x	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4x	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5x	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6x	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7x	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8x	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9x	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
ax	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
bx	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
cx	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
dx	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
ex	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
fx	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

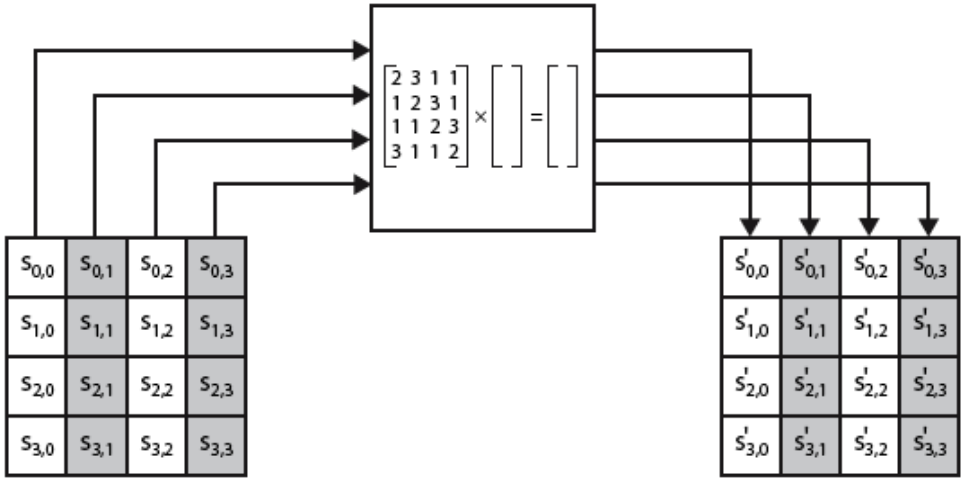
AES ShiftRows



- rotácia (cyklický posun) vľavo

  2. riadok o 1 bajt, 3. riadok o 2 bajty, 4. riadok o 3 bajty
- inverzná funkcia – rotácia vpravo
- permutácia bajtov v riadkoch
- proti „Square attack“ a iným diferenciálnym útokom

AES MixColumns



- permutácia a lineárna kombinácia v stĺpcoch
- násobenie polynómov v GF(2^8) modulo

$$x^8 + x^4 + x^3 + x + 1$$
$$(100011011)$$

$01 \circ a = a$

$02 \circ a = lsh(a) \oplus$

$\oplus (msb(a) * 100011011)$

$03 \circ a = (02 \circ a) \oplus a$

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} s_{0,i} \\ s_{1,i} \\ s_{2,i} \\ s_{3,i} \end{pmatrix} = \begin{pmatrix} s'_{0,i} \\ s'_{1,i} \\ s'_{2,i} \\ s'_{3,i} \end{pmatrix}$$

$$s'_{0,i} = (02 \circ s_{0,i}) \oplus (03 \circ s_{1,i}) \oplus (01 \circ s_{2,i}) \oplus (01 \circ s_{3,i}) =$$

$$= lsh(s_{0,i}) \oplus (msb(s_{0,i}) * 100011011) \oplus lsh(s_{1,i}) \oplus (msb(s_{1,i}) * 100011011) \oplus$$
$$\oplus\, s_{1,i} \oplus s_{2,i} \oplus s_{3,i}$$

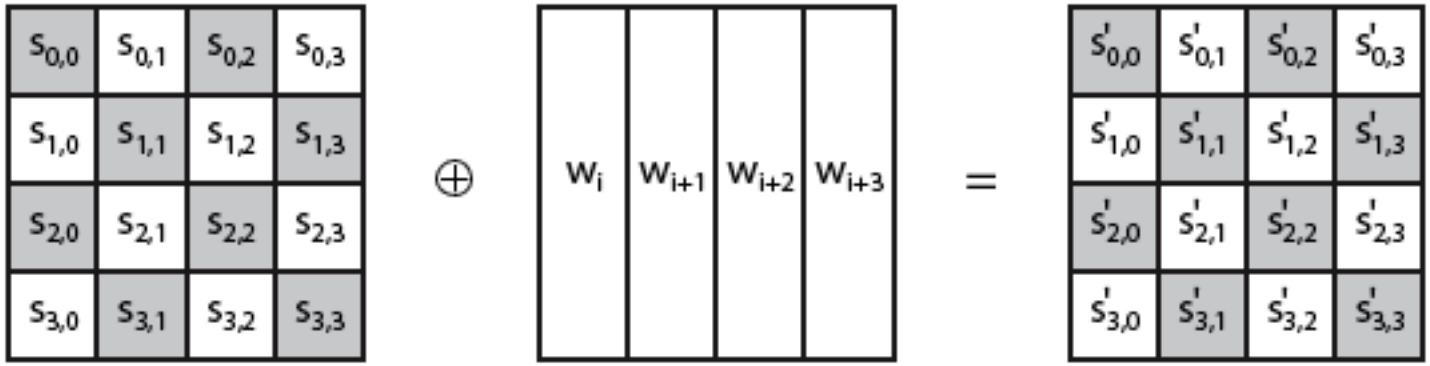
AES `MixColumns`

- lineárny kód s maximálnou vzdialenosťou medzi kódovými slovami
- inverzná matica je zložitejšia – výpočet je dlhší

$$\begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix}$$

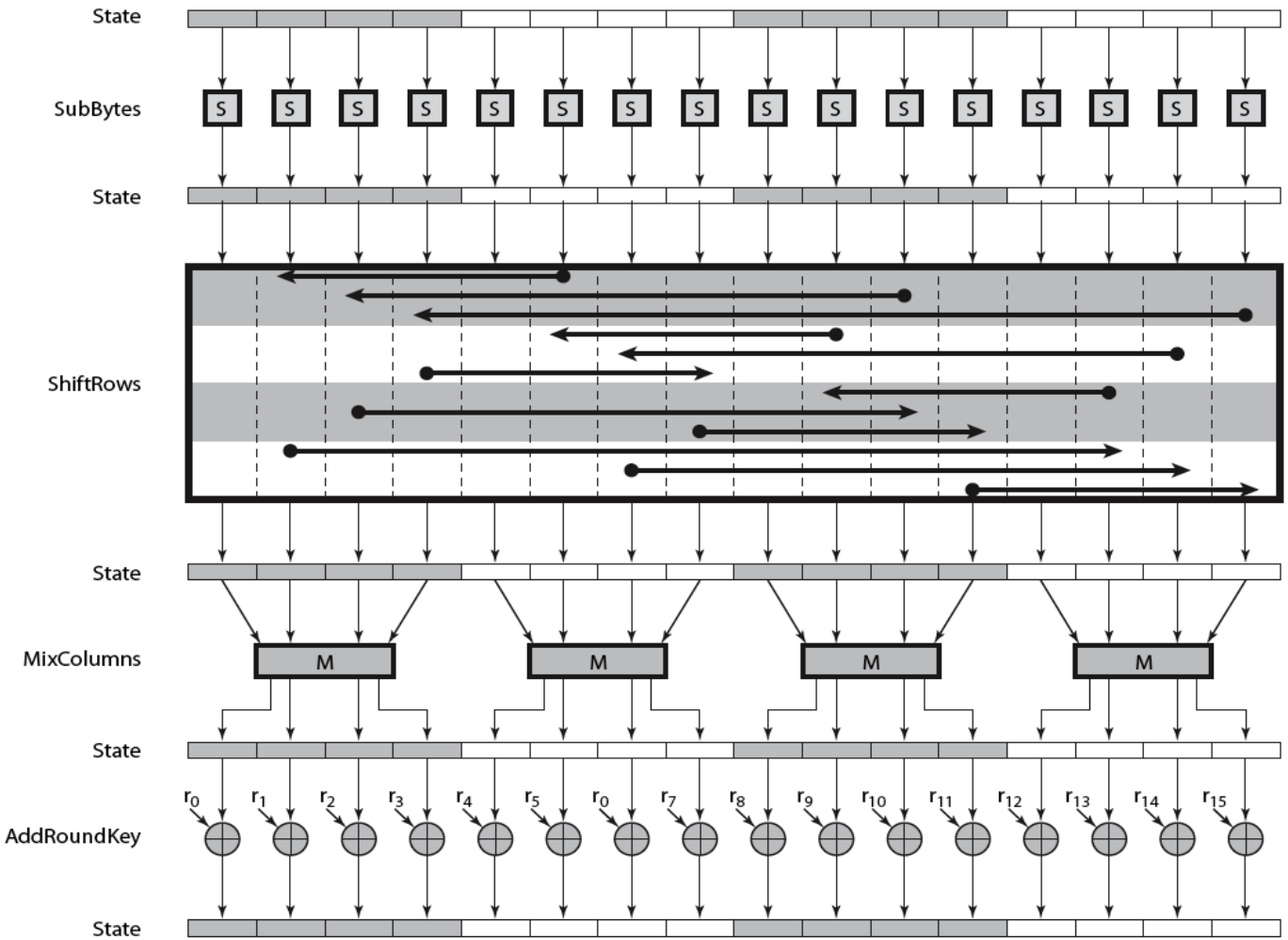
$$\begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix} \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} = \begin{pmatrix} 01 & 00 & 00 & 00 \\ 00 & 01 & 00 & 00 \\ 00 & 00 & 01 & 00 \\ 00 & 00 & 00 & 01 \end{pmatrix}$$

AES AddRoundKey

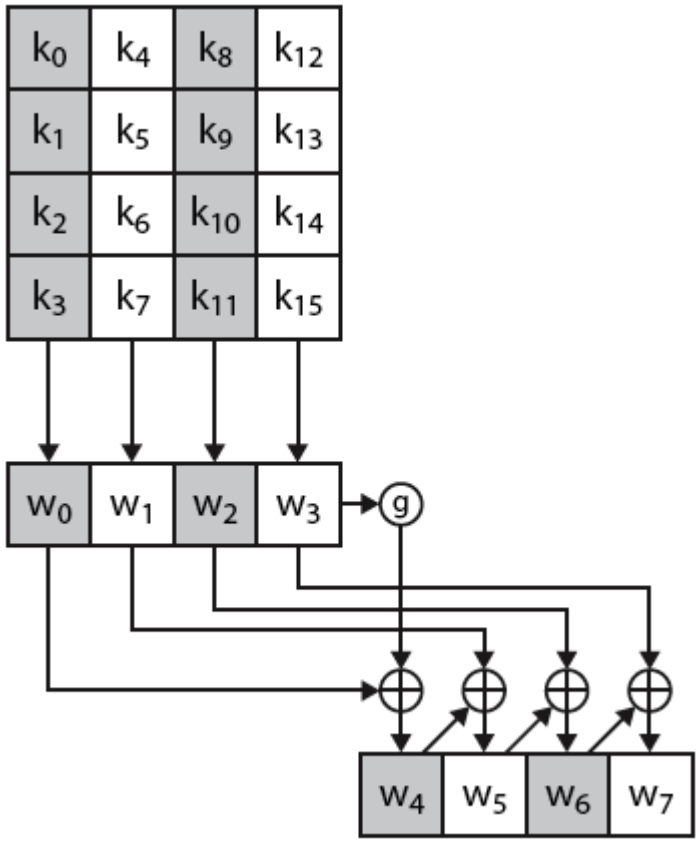


- XOR po stĺpcoch (Vernam)
- inverzná operácia je identická

AES runda pre 128 bitové spracovanie



AES generovanie kľúčov



- generovanie po 32-bitových slovách
- 44, 52, resp. 60 slov
- prvé 4 sú 32-bitové slová podľa kľúča
- $w_i = w_{i-4} \oplus w_{i-1}$ pre i mod 4 ≠ 0
- inak $w_i = w_{i-4} \oplus \mathrm{SubWord}(\mathrm{RotWord}(w_{i-1})) \oplus \mathrm{Rcon}(i/4)$
  Rcon = [1,2,4,8,10,20,40,80,1B,36]

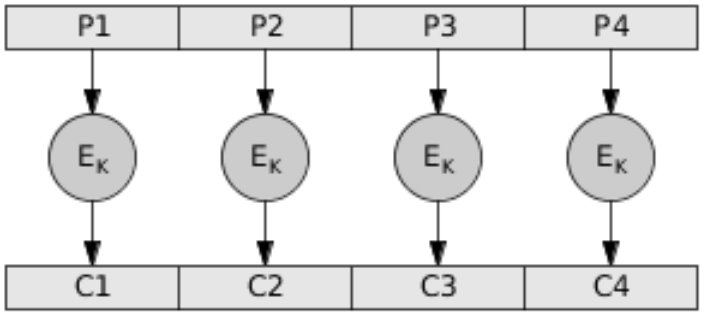
AES

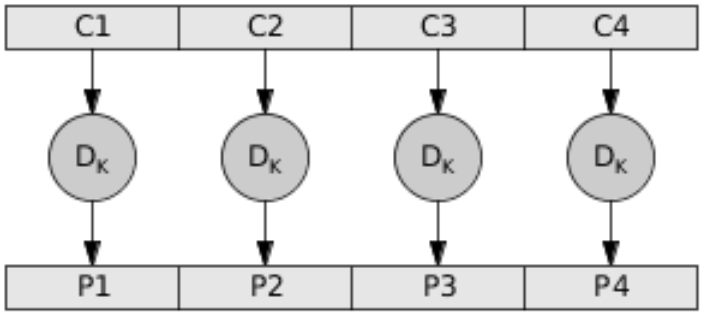
- “related-key” útoky na 8-round AES-128 (2^{48} pokusov, 2^{32} bitov pamäte), 9-round AES-256 (2^{39}), 10-round AES-256 (2^{45}), 11-round AES-256 (2^{70})
- (2011-2015) AES-128 na $2^{126.1}$ pokusov a 2^{56} b dát,
  AES-196 na $2^{189.7}$ pokusov a 2^{48} b dát,
  AES-256 na $2^{254.3}$ pokusov a 2^{40} b dát
- side channels – timing attack, power consumption (smart cards), magnetic fields, RF emissions
- implementácia AES-128-CBC sw 1 Gb/s AES-NI 6 Gb/s
  AES-128-CTR AES-NI 24 Gb/s ASIC, FPGA 40 Gb/s

Režimy využívania blokových šifier

- pre vstupy dlhšie ako jeden blok
- do dĺžky bloku sa pridá výplň – padding (napr. PKCS#7 – počet bajtov výplne)
- spôsob použitia blokového šifrovania môže viesť k zníženiu bezpečnosti
- podľa požiadaviek na rýchlosť resp. bezpečnosť resp. paralelizáciu resp. použitie PRNG
- neuchránia pred modifikáciou šifrovaného textu

ECB Electronic Code Book

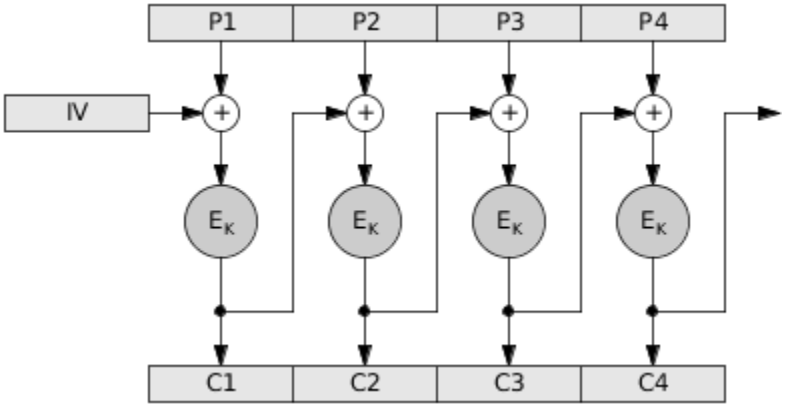


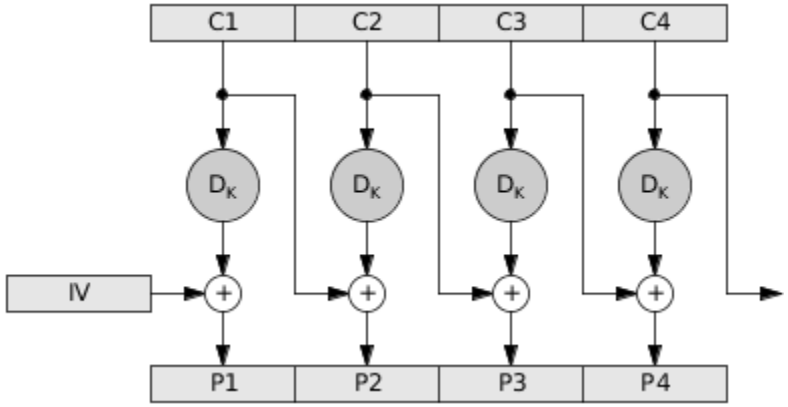


$C_n = E_K(P_n) \qquad P_n = D_K(C_n)$

- každý blok sa šifruje samostatne, nie je potrebná synchronizácia
- prenosová chyba sa prejaví len v jednom bloku
- možno dobre paralelizovať
- rovnaké bloky otvoreného textu sa šifrujú rovnako - štatistika
- je možné zistiť opakované vyslanie správy, preusporiadať, vymeniť bloky

CBC Cipher Block Chaining

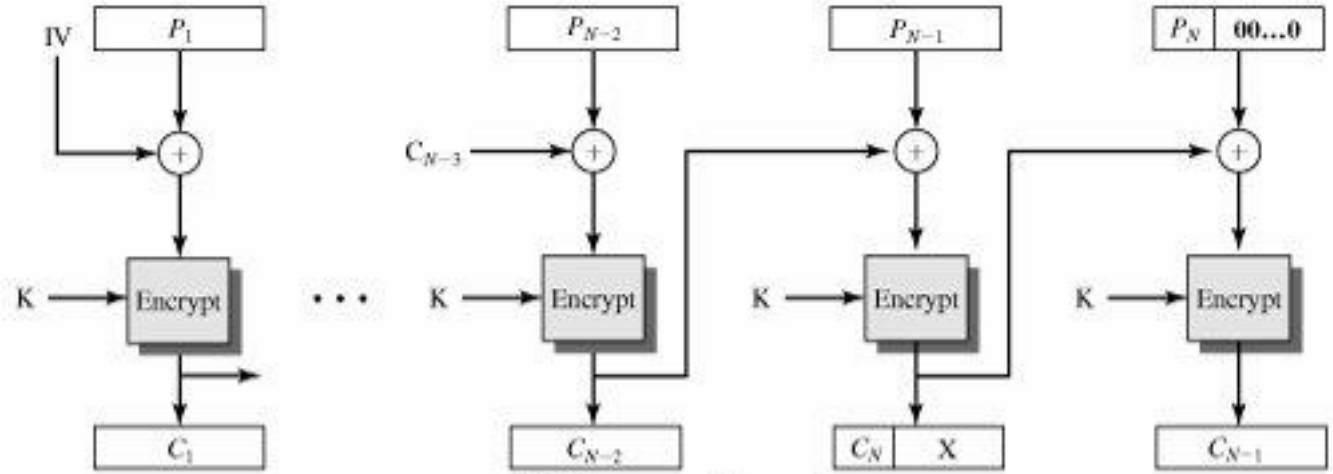




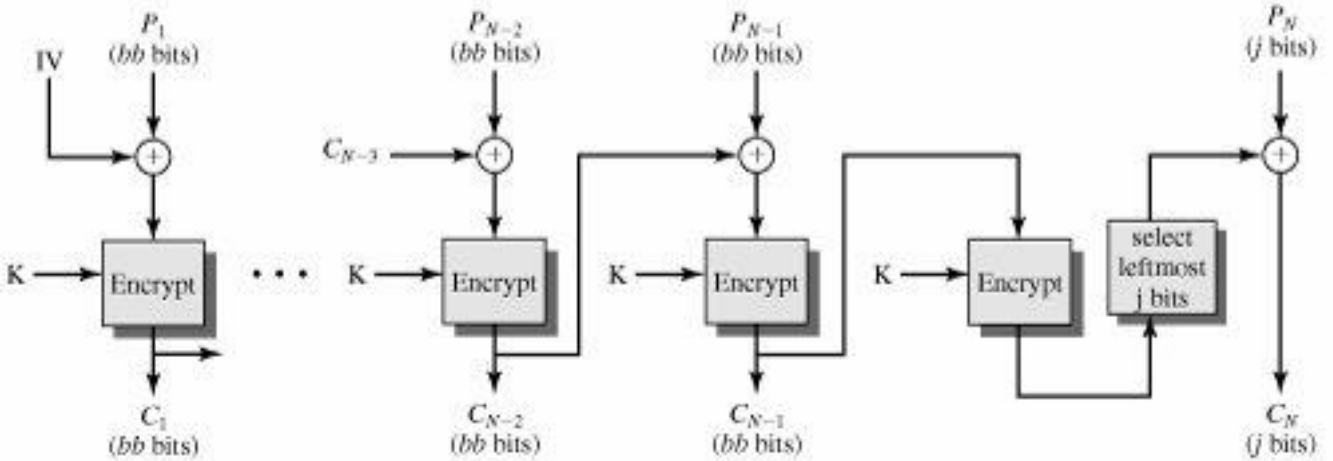
$C_0 = IV \quad C_n = E_K(C_{n-1} \oplus P_n) \qquad P_n = C_{n-1} \oplus D_K(C_n)$

- šifrovanie bloku závisí aj od šifrovania predchádzajúceho bloku
- IV – inicializačný vektor – randomizuje šifrovanie – nie je možné použiť šifrované bloky opakujúceho sa otvoreného textu
- IV nie je potrebné utajovať, má byť nepredikovateľné
- zmena v otvorenom texte resp. IV sa prenáša do celého výstupu
- kľúč je potrebné po čase zmeniť (útok na rovnaké bloky $C_i = C_j$)

CBC ciphertext stealing (CTS)



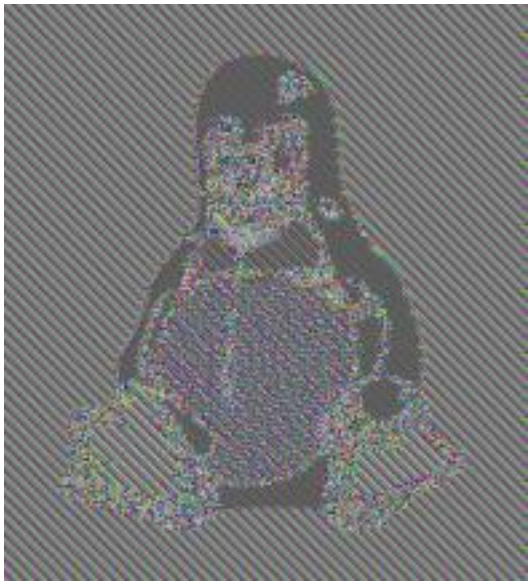
(a) Cipheretext stealing mode



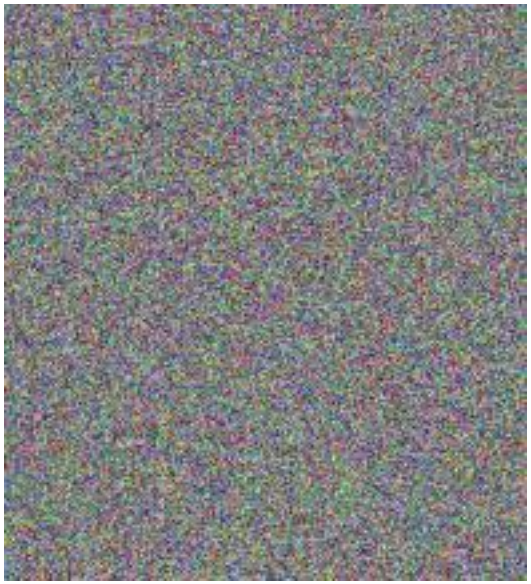
(b) Alternative method

porovnanie šifrovania v režime ECB a CBC

Plain



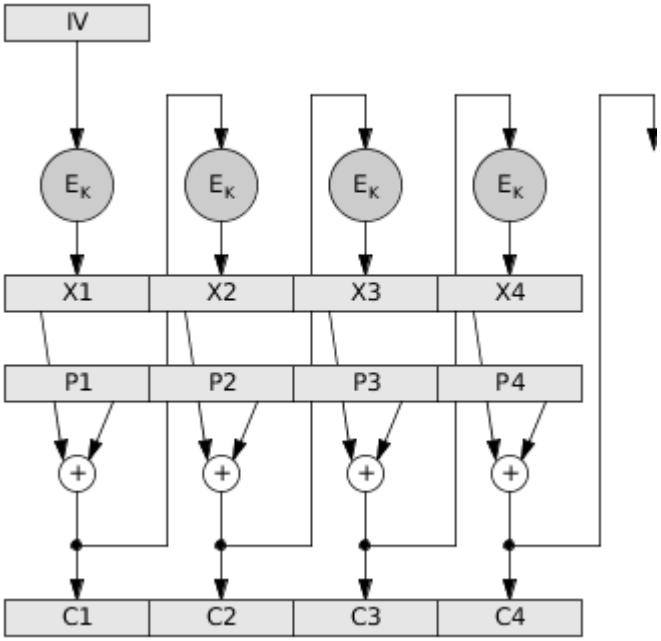
ECB

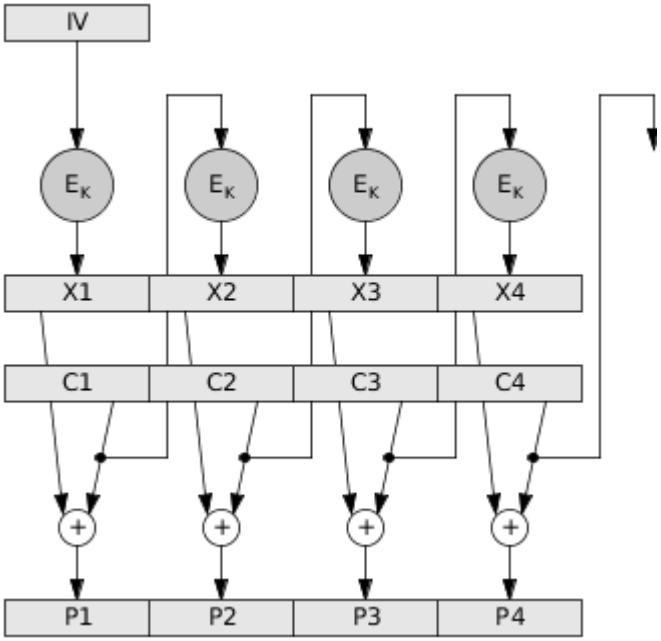


CBC

Zdroj: wikipedia.org

CFB Cipher Feedback mode

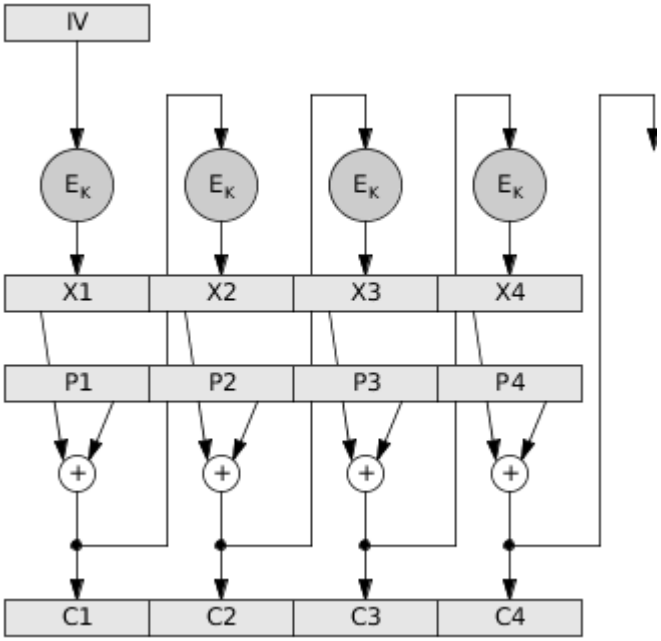


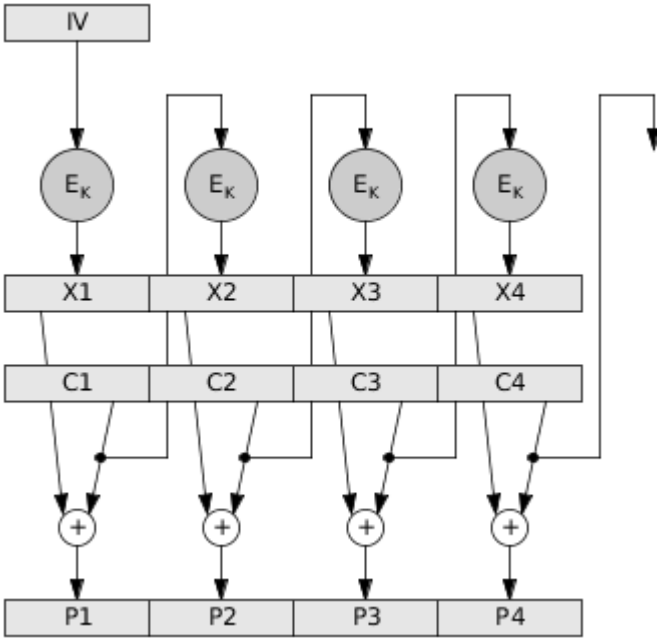


$C_0 = IV \quad C_n = P_n \oplus E_K(C_{n-1}) \qquad P_n = C_n \oplus E_K(C_{n-1})$

- používa (posunutý) šifrovaný text ako stream v prúdovej šifre
- IV spôsobuje nedeterministickosť (randomizuje výsledok)

CFB Cipher Feedback mode

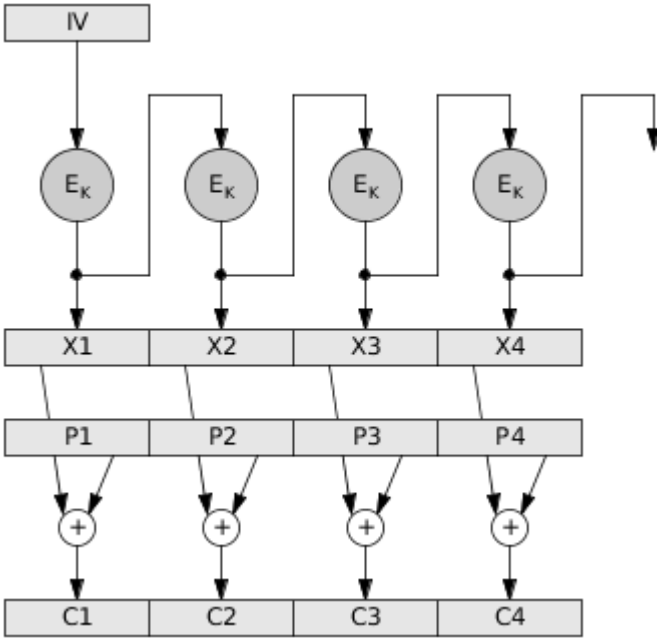


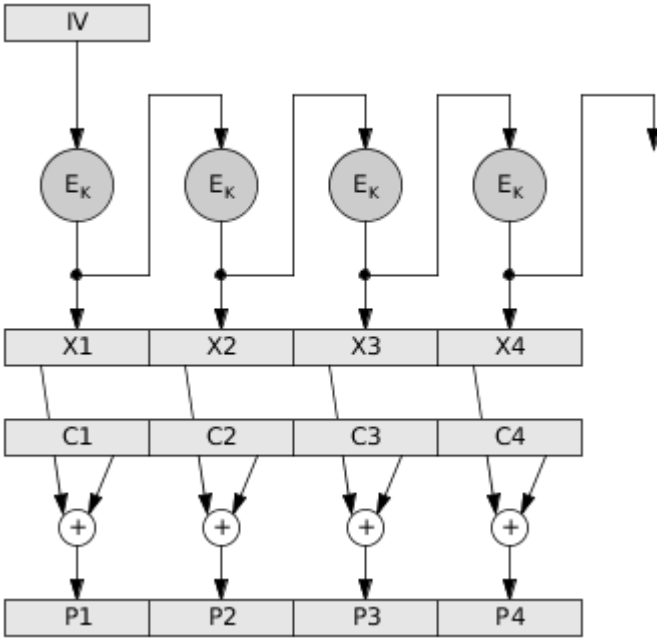


$C_0 = IV \quad C_n = P_n \oplus E_K(C_{n-1}) \qquad P_n = C_n \oplus E_K(C_{n-1})$

- používa (posunutý) šifrovaný text ako stream v prúdovej šifre
- IV spôsobuje nedeterministickosť (randomizuje výsledok)
- nie je potrebná dešifrovacia funkcia !!!

OFB Output Feedback mode

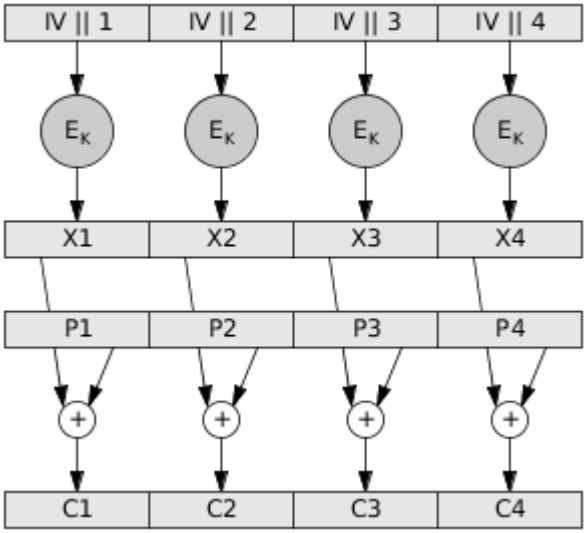


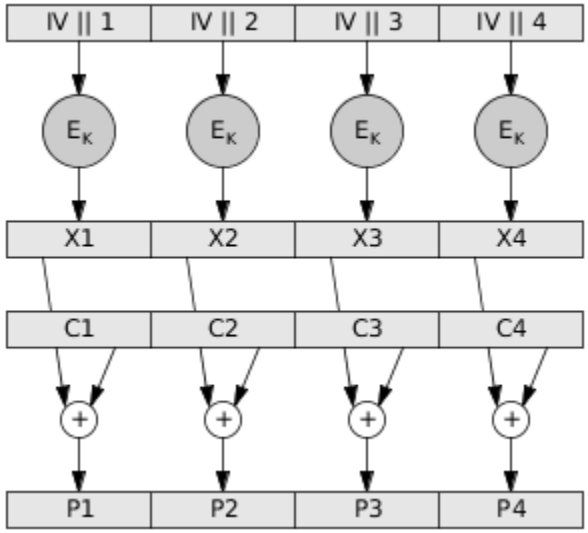


$X_0 = IV \quad X_n = E_K(X_{n-1}) \qquad C_n = P_n \oplus X_n \qquad P_n = C_n \oplus X_n$

- pomocou blokového šifrovania sa vytvorí prúd pre prúdovú šifru
- prúd je možné generovať nezávisle
- IV – randomizácia – nie je možné použiť viackrát!
  (riziká ako pri prúdovej šifre)

CTR Counter mode

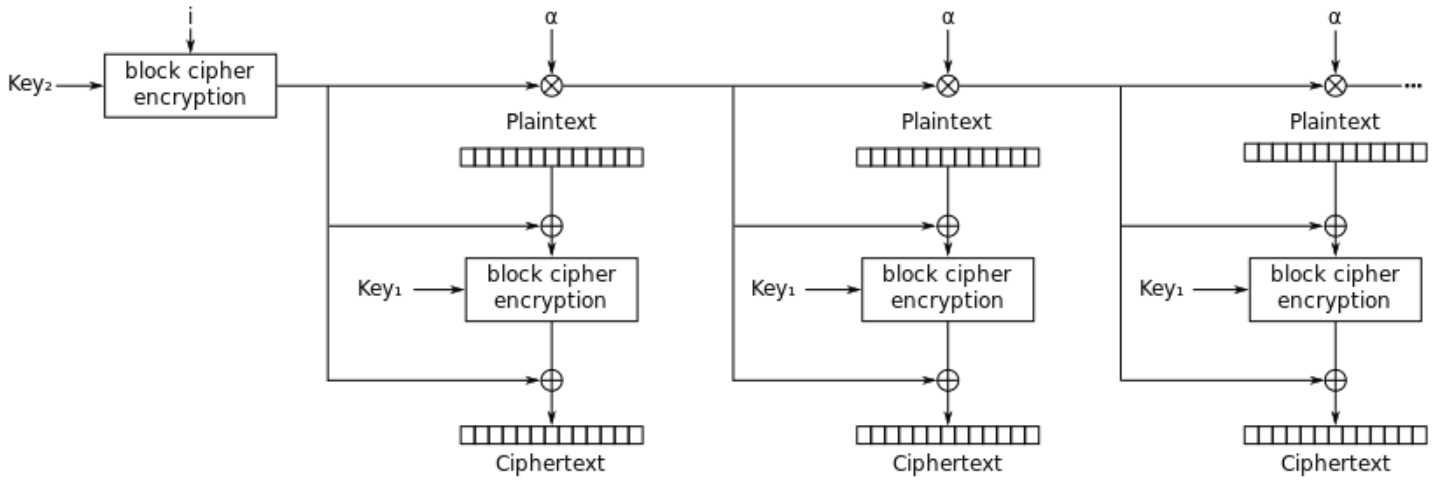




$C_n = P_n \oplus E_K(IV \mid n)$ $\qquad$ $P_n = C_n \oplus E_K(IV \mid n)$

- prúd pre prúdovú šifru sa vytvorí po blokoch
- je možné paralelizovať, priamy prístup (seek)
- IV – nie je možné použiť viackrát
- obmedzená dĺžka (ctr sa nesmú opakovať)

XEX režim



XEX mode encryption

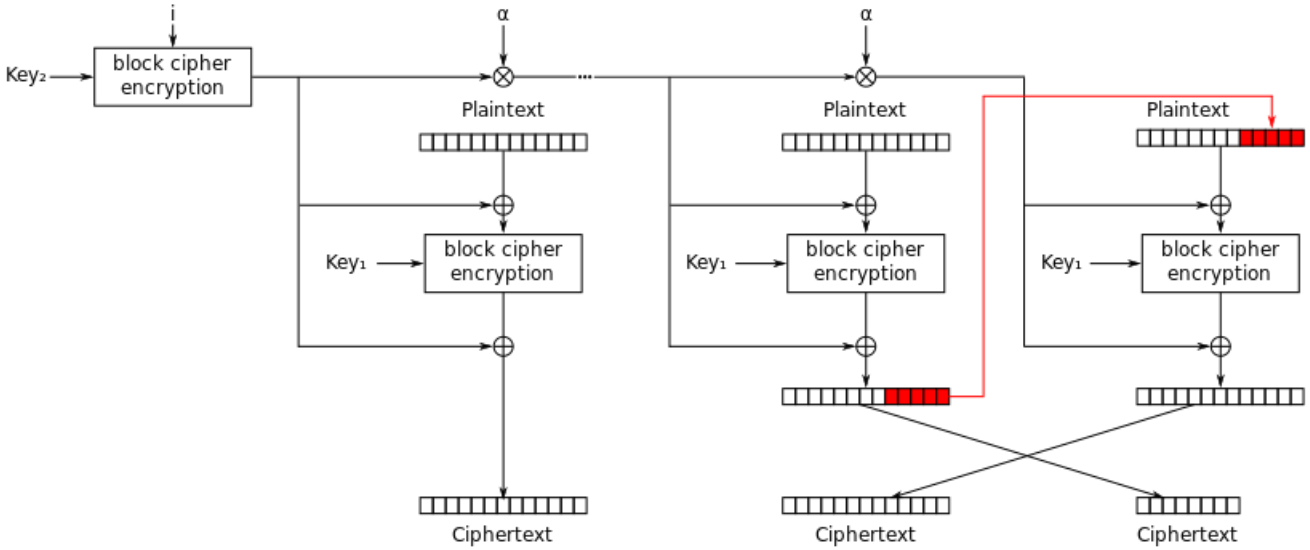
$X_n = E_{K2}(I) \otimes \alpha^n \qquad C_n = E_K(P_n \oplus X_n) \oplus X_n$

$\alpha = x \quad \{10\} \qquad \otimes$ násobenie v $GF(2^{128})$ modulo

$x^{128} + x^7 + x^2 + x + 1 \quad \{10...010000111\}$

- XEX (xor-encrypt-xor) šifrovanie súborov na disku
- tweak α^j - ťahák pre prístup k j-temu bloku

XTS ciphertext stealing



XEX with tweak and ciphertext stealing (XTS) mode encryption

- vypĺňanie posledného neúplného bloku (*padding*)

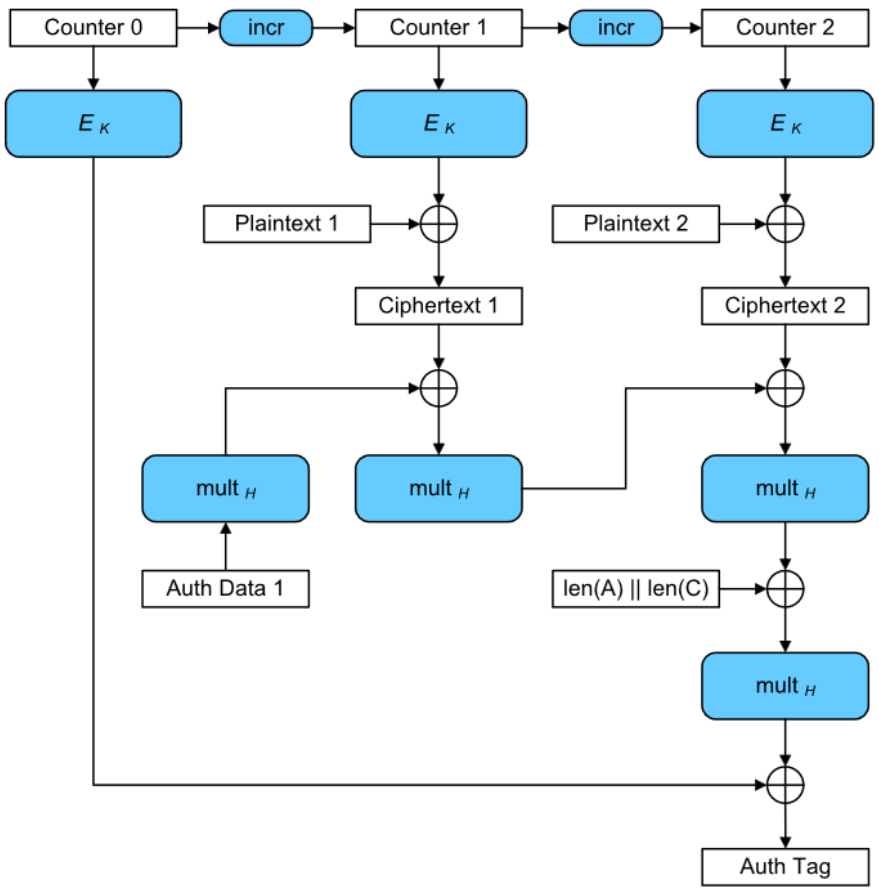
$C_{n-1} = XEX_n(P_n \,|XEX_{n-1}(P_{n-1})[(m-k+1):m]); \;\; C_n = XEX_{n-1}(P_{n-1})[1:(m-k)]$

$P_{n-1} = XEX`_{n-1}(C_n \,|XEX`_n(C_{n-1})[(m-k+1):m]); \; P_n = XEX`_n(C_{n-1})[1:(m-k)]$

predikovateľné hodnoty IV

- pri šifrovaní disku – watermarking
  (sektory s rovnakými prvými blokmi, potom pri CBC režime dostanem $b \oplus IV_1 = b \oplus IV_2$)
- pre CTR ESSIV šifrovaný IV $IV_n = E_{h(K)}(n)$

GCM Galois Counter Mode



- $CTR_0 = IV \mid 0^{31} \mid 1$,
  $CTR_n = CTR_{n-1} + 1$
- $C_i = E_K(CTR_i) \oplus P_i$

autentifikácia správy

- $H = E_k(0^{128})$ $\quad g_0 = AD \otimes H$

$\otimes$ Galois field multiplication $GF(2^{128})$ ako v XEX

- $g_i = (g_{i-1} \oplus C_i) \otimes H$
- $g_{n+1} = g_n \oplus (len(A) \mid len(C))$
- $T = (g_{n+1} \otimes H) \oplus E_k(CTR_0)$

Ďakujem za pozornosť.

jozef.jirasek@upjs.sk