Symetrické blokové šifry

Milan Radojčić

SSPŠaG – KBB

23. února 2026

Hlavní body

Hlavní body

Klasifikace symetrických šifer

- **Symetrické šifry** používají **stejný** klíč pro šifrování i dešifrování.
- **Blokové šifry** dělí data na bloky a každý blok šifrují **stejným** klíčem.
- **Proudové šifry** dělí data na bloky a každý blok šifrují **jiným** klíčem.

Hlavní body

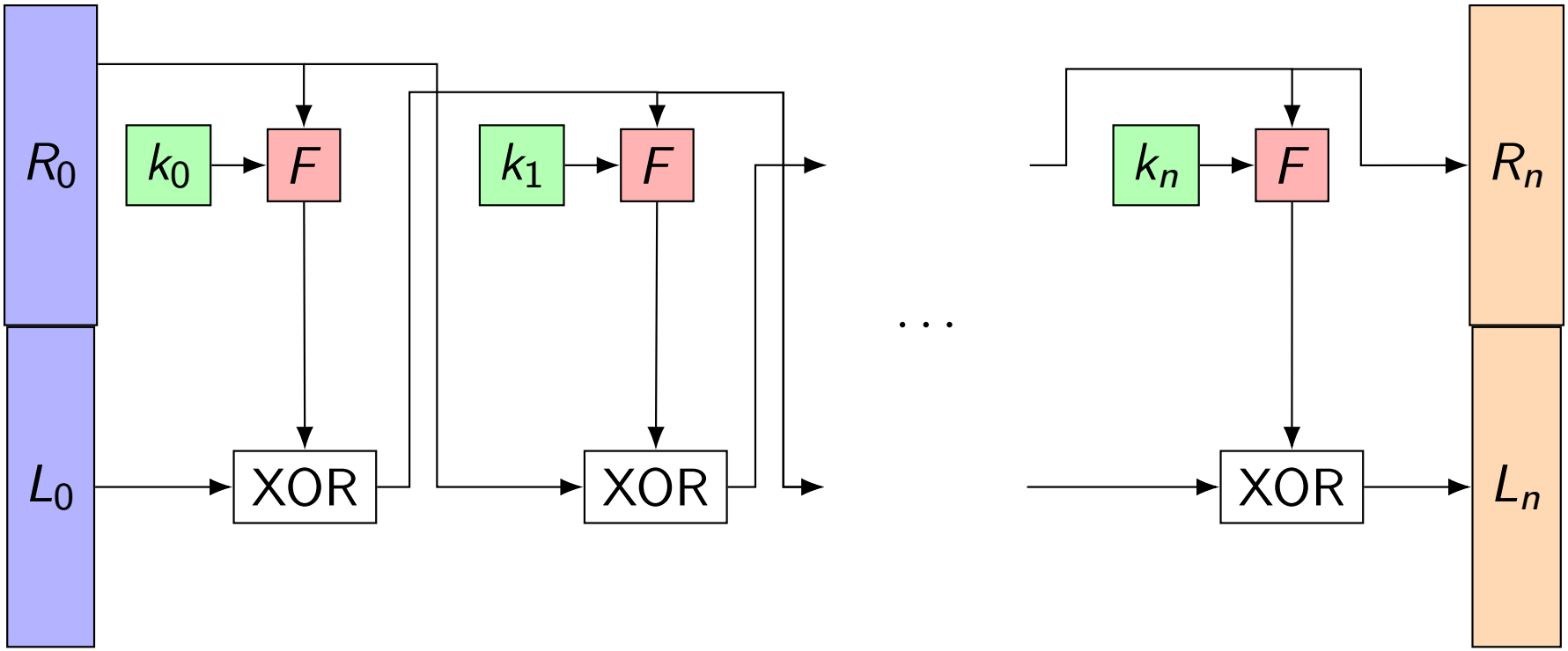
DES

- **Symetrická bloková** šifra.
- Poprvé publikována v roce 1975.
- Založena na tzv. **Feistelově síti** (někdy Feistelova šifra).
- Už v roce 1977 Whitfield Diffie a Martin Hellman upozorňovali na náchylnost šifry na útoky hrubou silou.

Feistelova síť

- Obecná struktura pro konstrukci blokových šifer.
- Založena na několikanásobném opakování nějaké rundovní funkce F.
- Šifrování i dešifrování probíhá velice podobně.

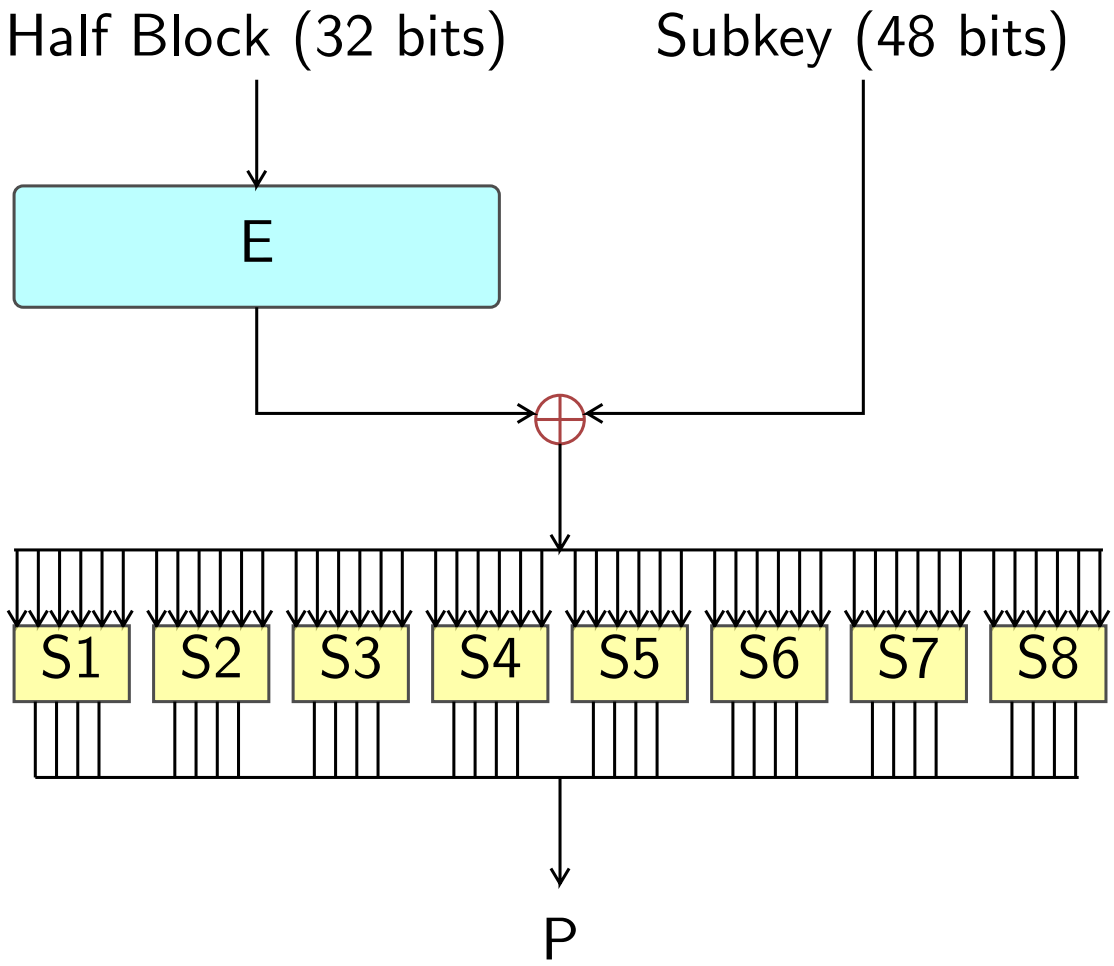
Feistelova síť



DES

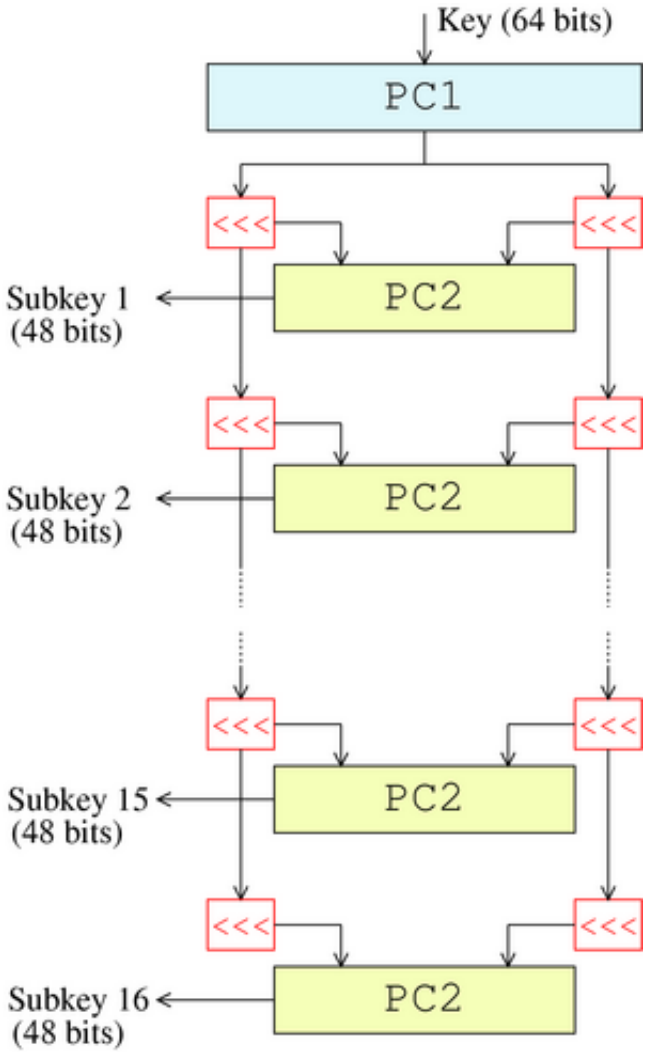
- Používá 56-bitový klíč (+ 8 bitů parita).
- Velikost jednoho bloku je 64 bitů.
- Rundovní funkce F:
  - Expanze – 32-bitová polovina bloku se expanduje na 48-bitů
  - Mixování s klíčem – XOR výstupu z fáze expanze s klíčem
  - Substituce – substituce 6-bitových bloků na 4-bitové podle tabulky
  - Permutace – bity z předchozího bloku jsou promíchány tak, aby se v příští rundě objevily v jiném bloku
- Počet rund je 16.

DES: rundovní funkce



https://commons.wikimedia.org/wiki/File:Data_Encription_Standard_Flow_Diagram.svg

DES: key schedule



https://en.wikipedia.org/wiki/File:DES-key-schedule.png

3DES

- DES provedený 3krát za sebou.
- V současné době už není bezpečný kvůli malé velikosti bloku.
- Lze použít 2 nebo 3 56-bitové klíče.
- Šifrování: $E_{k3}(D_{k2}(E_{k1}(\text{pt})))$
- Dešifrování: $D_{k1}(E_{k2}(D_{k3}(\text{ct})))$

Meet in the middle útok

Uvažujme Double DES: $E_{k2}(E_{k1}(\text{plaintext}))$. Jeden způsob, jak prolomit klíč, by bylo zkusit všechny možné kombinace $k2$ a $k1$, tj. $2^{56} \cdot 2^{56} = 2^{112}$ možností.

No ale pokud $C = E_{k2}(E_{k1}(P))$, potom $D_{k2}(C) = E_{k1}(P)$. To nám dovoluje zkoušet klíče $k1$ a $k2$ **nezávisle**. To je jen $2 \cdot 2^{56} = 2^{57}$ možností.

Hlavní body

Cesta k nahrazení DES

- DES byla šifra navržená IBM a NSA.
- K nalezení náhrady byla vypsána veřejná soutěž a vítězný algoritmus byl vybrán po několika kolech.
- Do finále se dostaly tyto šifry: MARS, RC6, **Rijndael**, Serpent a Twofish.

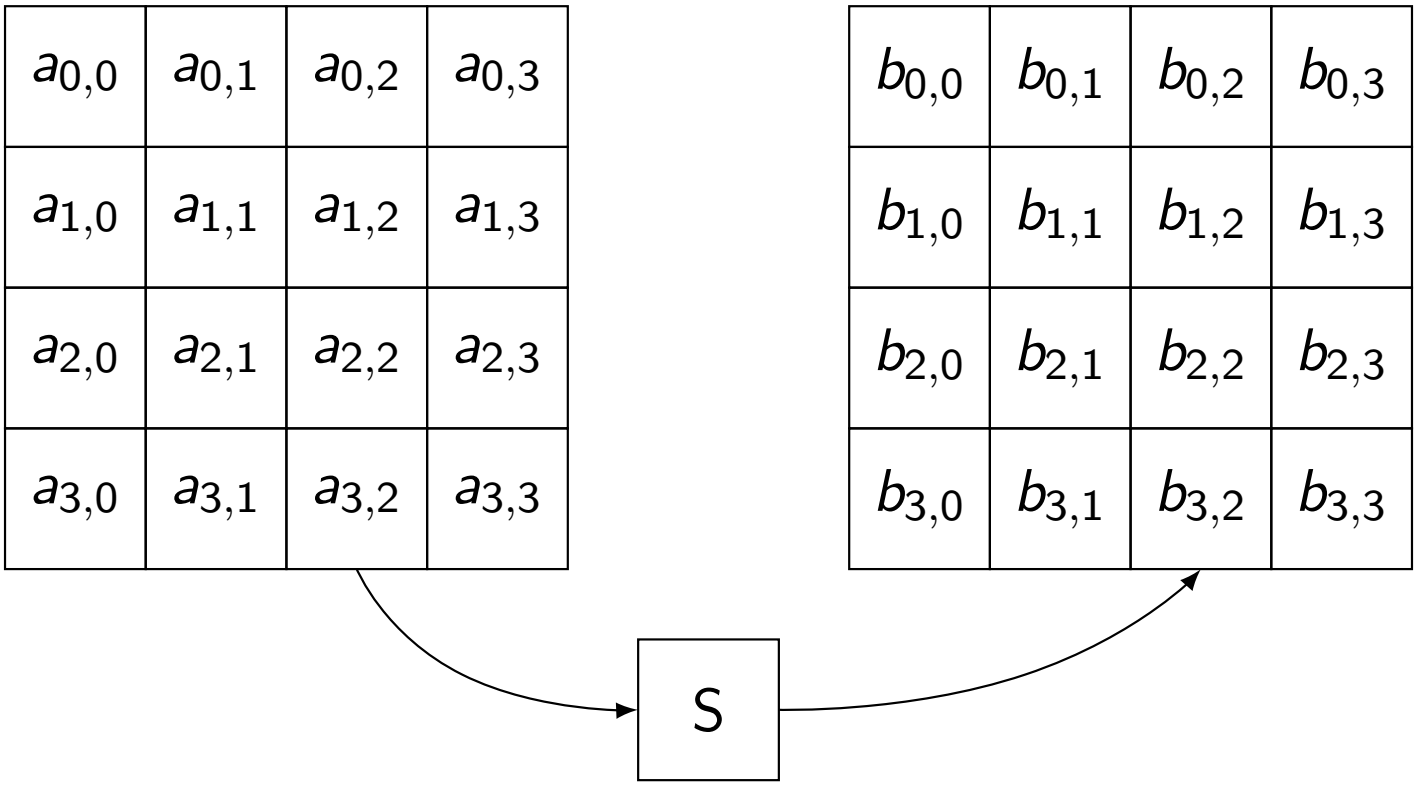
AES (Rjindael)

- **Symetrická bloková** šifra.
- Navržena v roce 1998 a standardizována v roce 2001.
- Není založena na Feistelově síti, ale také opakuje rundy a obsahuje podobné operace.
- Používá 128, 196 nebo 256 bitové klíče (a od nich se odvíjí počet rund).
- Velikost bloku je 128 bitů.

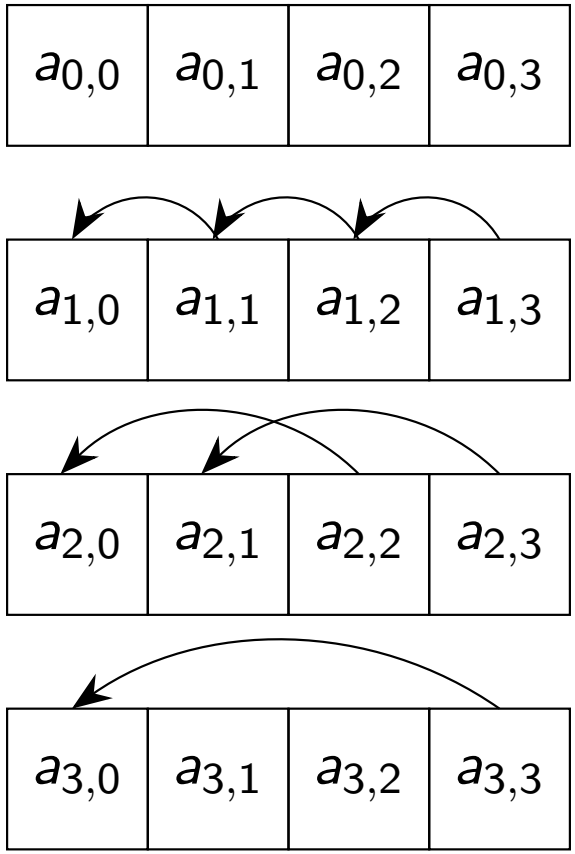
AES: Runda

- Na začátku se vnitřní stav inicializuje na vstupní data.
- Před první rundou se vnitřní stav xoruje s nultým rundovním klíčem.
- V každé rundě se pak opakuje:
  1. **SubBytes** — každý byte vnitřní stavu se nahradí podle tabulky
  2. **ShiftRows** — posun řádků vnitřního stavu podle indexu
  3. **MixColumns** (nedělá se v poslední rundě) — každý sloupec vnitřního stavu je vynásoben maticí
  4. **AddRoundKey** — XOR vnitřního stavu a rundovního klíče

SubBytes


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
S
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

ShiftRows



MixColumns

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} a_{0,i} \\ a_{1,i} \\ a_{2,i} \\ a_{3,i} \end{pmatrix} = \begin{pmatrix} b_{0,i} \\ b_{1,i} \\ b_{2,i} \\ b_{3,i} \end{pmatrix}$$

$$b_{0,i} = 2 \cdot a_{0,i} + 3 \cdot a_{1,i} + a_{2,i} + a_{3,i}$$

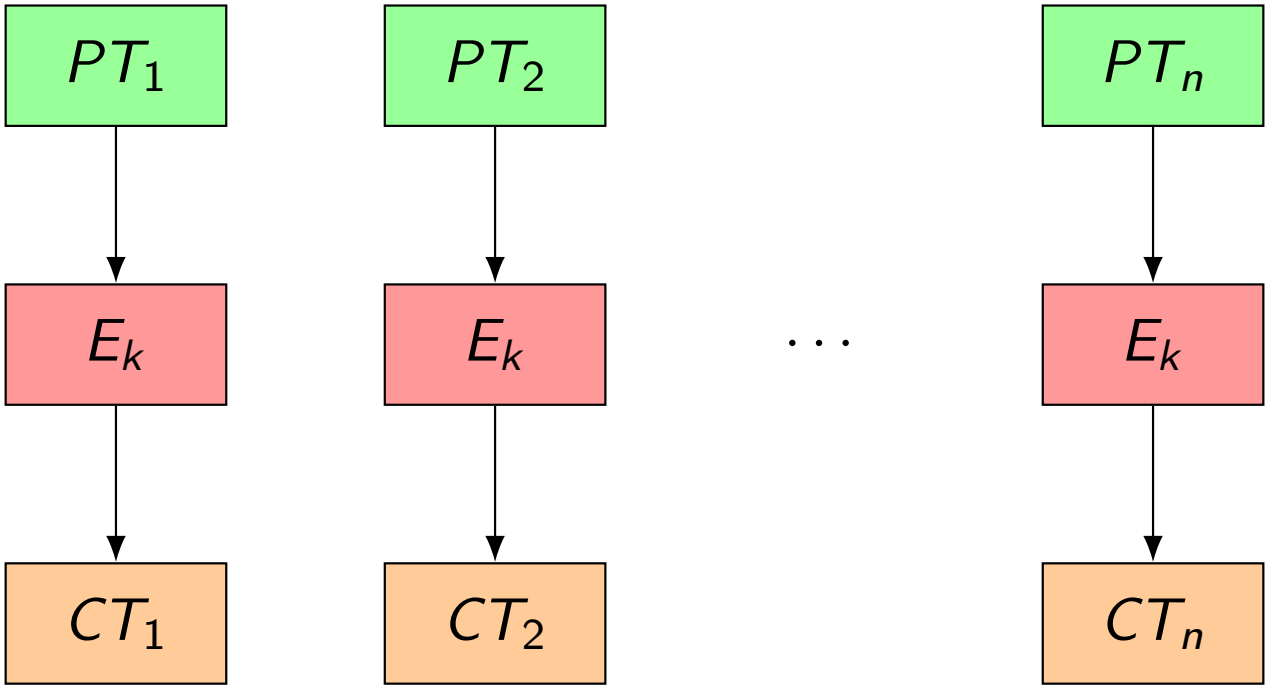
$$b_{1,i} = a_{0,i} + 2 \cdot a_{1,i} + 3 \cdot a_{2,i} + a_{3,i}$$

$$b_{2,i} = a_{0,i} + a_{1,i} + 2 \cdot a_{2,i} + 3 \cdot a_{3,i}$$

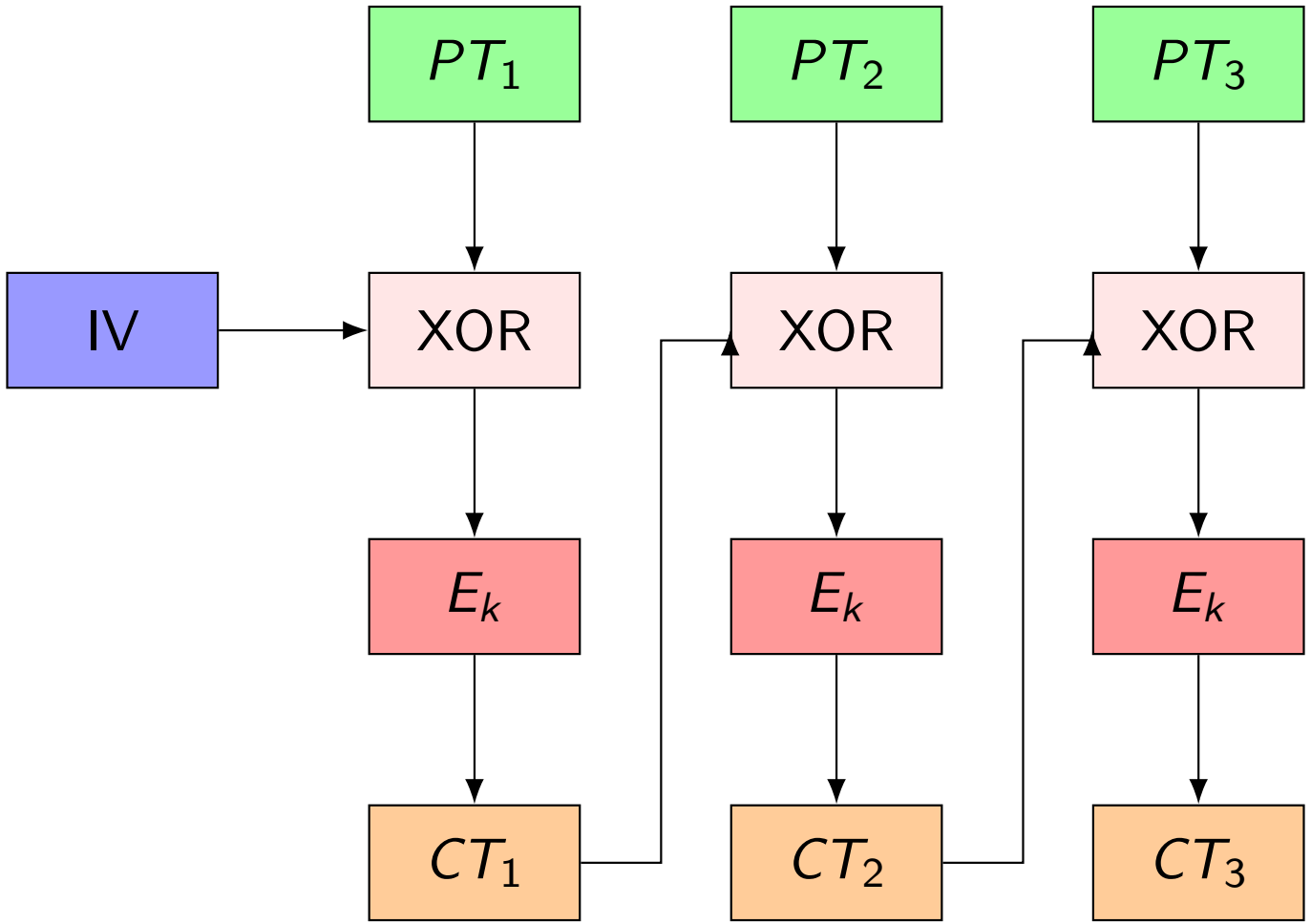
$$b_{3,i} = 3 \cdot a_{0,i} + a_{1,i} + a_{2,i} + 2 \cdot a_{3,i}$$

Hlavní body

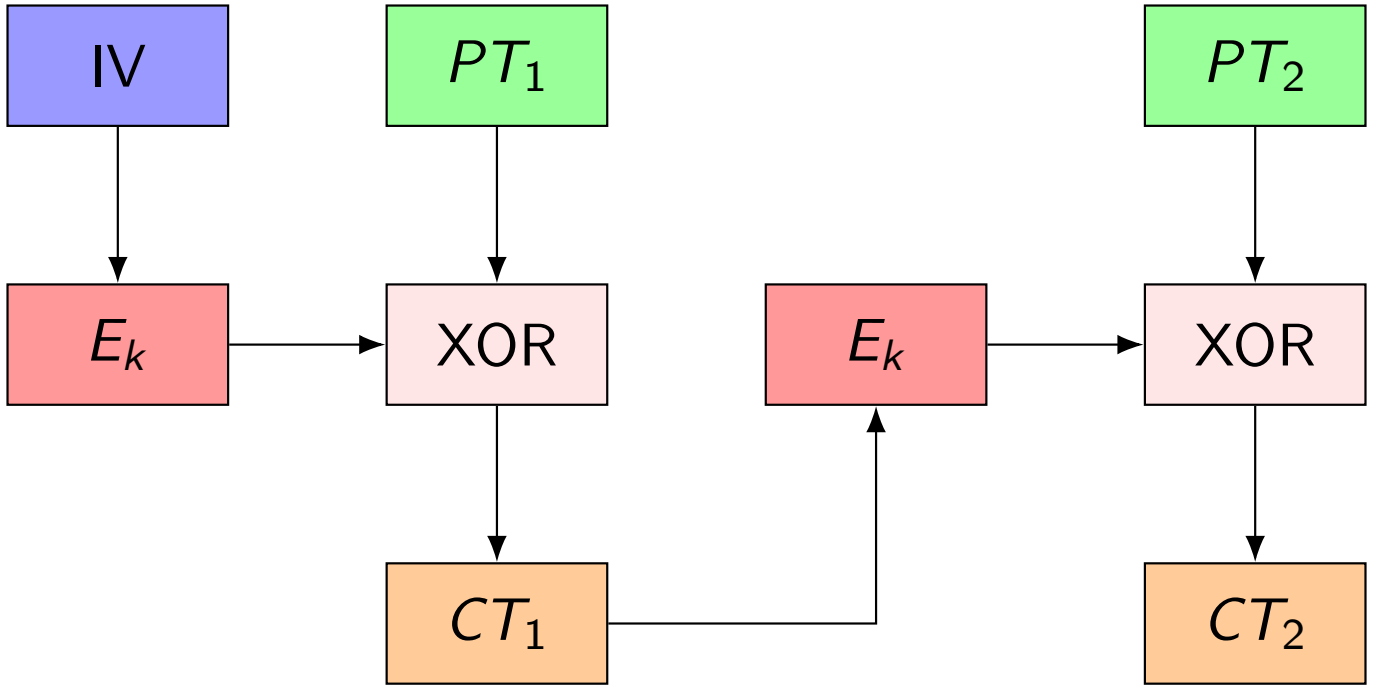
ECB (Electronic Codebook)



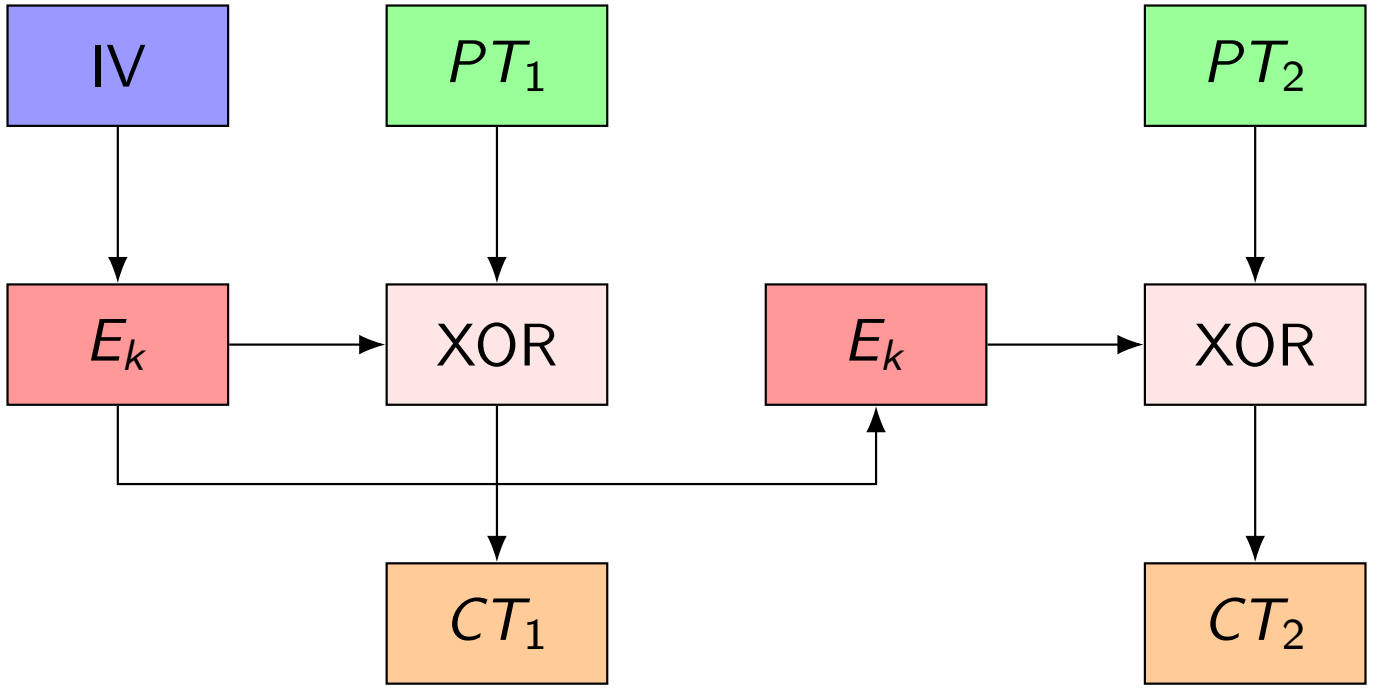
CBC (Cipherblock Chaining)



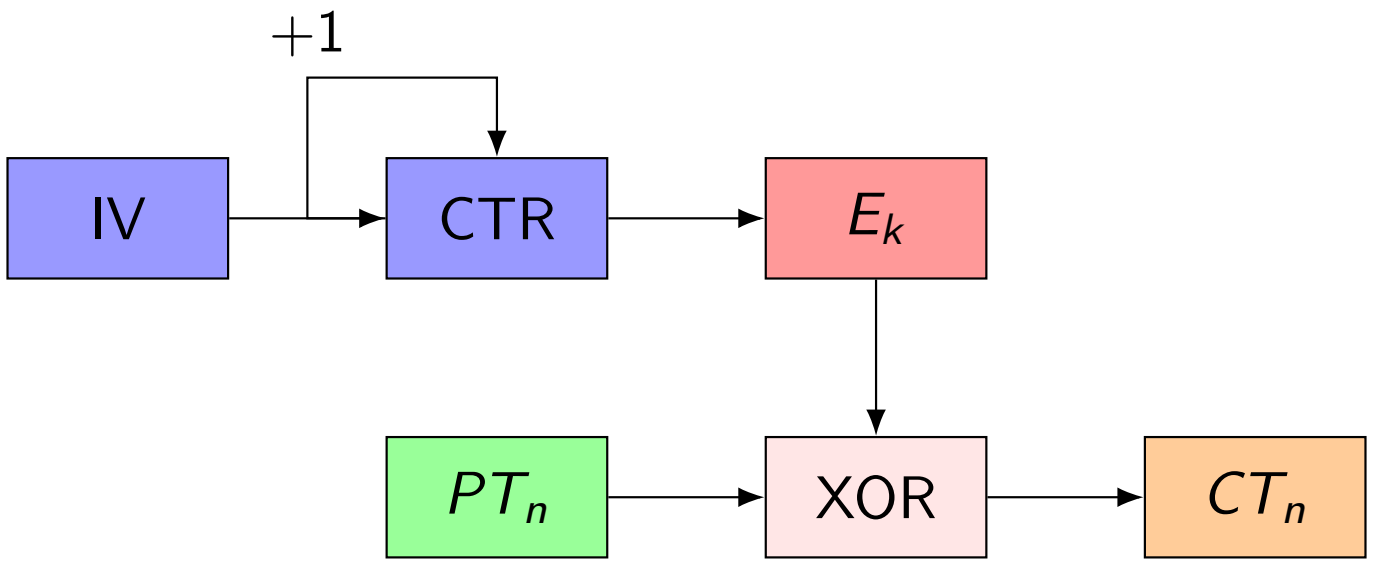
CFB (Cipher Feedback)



OFB (Output Feedback)



CTR (Counter)



Hlavní body

Detailní popisy algoritmů

- ChaCha20: RFC 7539
- DES: FIPS 46-3
- AES: FIPS 197