Kryptografie a počítačová bezpečnost

Režimy činnosti symetrických algoritmů

Literatura

- https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf
- Kapitola 7.2 – 7.6

Režimy činnosti blokových symetrických algoritmů

- Bloková šifra sama o sobě je vhodná pouze pro bezpečnou kryptografickou transformaci jedné skupiny bitů pevné délky, tedy jednoho bloku. Režim činnosti popisuje, jak opakovaně použít bezpečnou transformaci množství dat většího než jeden blok
- 5 režimů
  - ECB (Electronic Codebook Mode)
  - CBC (Cipher Block Chaining Mode)
  - OFB (Output Feedback Mode)
  - CFB (Cipher feedback Mode)
  - Counter Mode
  - …
  - https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

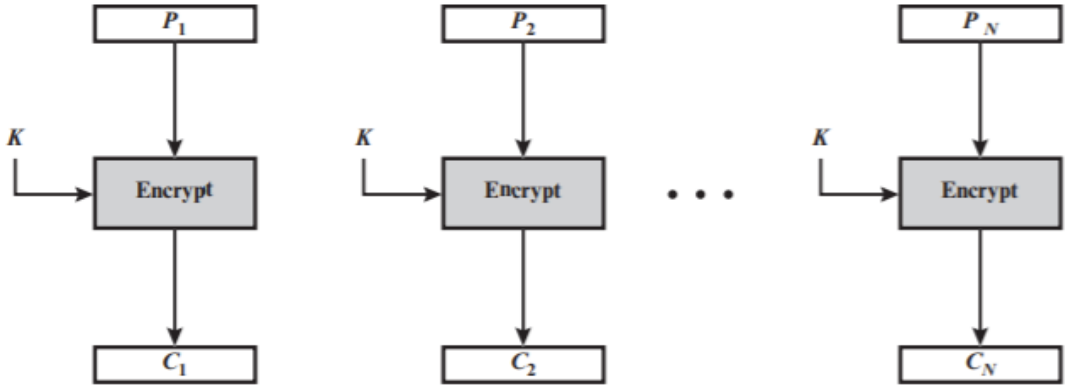
Režimy činnosti blokových symetrických algoritmů

- **Kryptografický režim** obvykle kombinuje algoritmus, nějaký druh zpětné vazby a jednoduché operace (**NIST** (National Institute of Standards and Technology) FIPS 81, Special Publication 800-38A).
- Hlediska bezpečnosti algoritmu:
  - ukrytí statistických vzorků otevřeného textu,
  - vstup pro šifru náhodný (např. náhodné generování klíče),
  - manipulace s otevřeným textem prostřednictvím chyb v šifrovém textu má být obtížná,
  - má být možno opakovaně použít tentýž klíč pro šifrování více zpráv,
  - účinnost režimu nemůže být menší než účinnost šifry,
  - odolnost proti chybám.

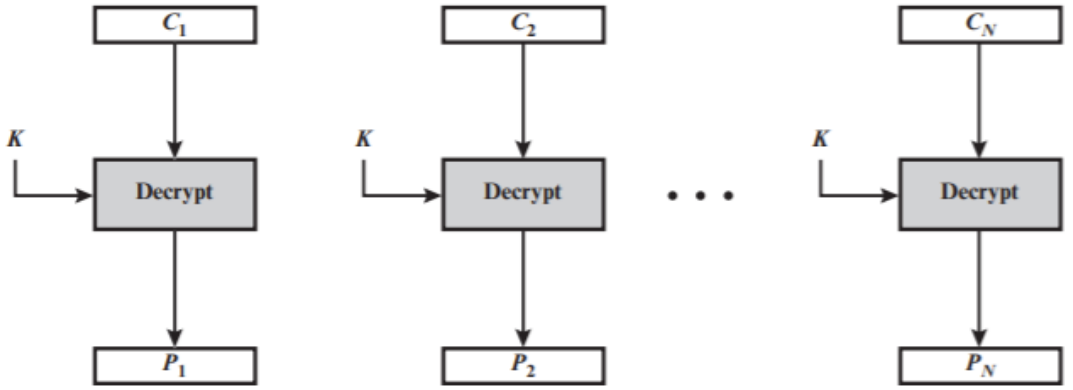
Režimy činnosti blokových symetrických algoritmů

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of plaintext bits is encoded independently using the same key.	• Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next block of plaintext and the preceding block of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.	• Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements

Electronic Codebook Mode ECB



(a) Encryption

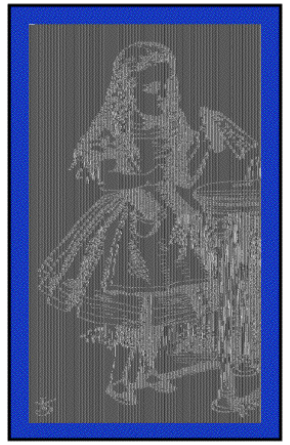


(b) Decryption

Electronic Codebook Mode

- ✓ Nejjednodušší a nejrychlejší blokový režim.
- ✓ Je to vlastně prostá substituce, kdy je blok otevřeného textu šifrován do bloku šifrového textu, necht' $i \geq 1$, $c_i = e_k(m_i), m_i = d_k(c_i)$.
- ✓ **Padding** - doplnění posledního bloku M, který může být kratší než je délka bloku
- ✓ Každý blok je šifrován nezávisle, celý proces může být paralelizován.
- ✓ *Stereotypní* začátky a konce zprávy.
- ✓ Vhodné pro krátké zprávy (šifrování a rozesílání klíčů...) .
- ✓ Vhodné pro poruchová spojení (změna nebo ztráta jednoho bloku neovlivní šifrování ostatních bloků).

Electronic Codebook Mode



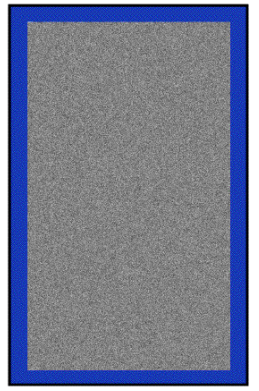
- × Nezašifrovaný text není skrýván.
- × Snadná kryptoanalýza.
- × Opakovaný blok je šifrován shodně - lze budovat *kódovou* knihu odposlechem bez znalosti klíče K.
- × **Pasivní útok**: informace, vyplývající ze shody bloků šifrových textů (databáze, kódová kniha, slovníkový útok)
- × **Aktivní útoky** vložením - Útočník může modifikovat, odstranit nebo zopakovat libovolný blok šifry bez znalosti klíče nebo algoritmu.
- Řešením je **chaining** (zřetězení).

databáze platů .....os.č. 162 ...**025 103**,-Kč ....os.č. 163 ...**027 038**,-Kč .....
kajsůkuiůooiwpqwqqwekaouiolwerkweiosdvůoipášqpéáčcéůywuíta3tdszj34hkf...

..... 3tdszj34 j7čžuths **bgžc4rš7** rg43č7řz .....
..... převeďte 1 0 0 0 ,- Kč .....

..... 3tdszj34 j7čžuths **bgžc4rš7 bgžc4rš7** rg43č7řz .....
..... převeďte 1 0 0 0 0 0 0 ,- Kč .....

Cipher Block Chaining Mode CBC

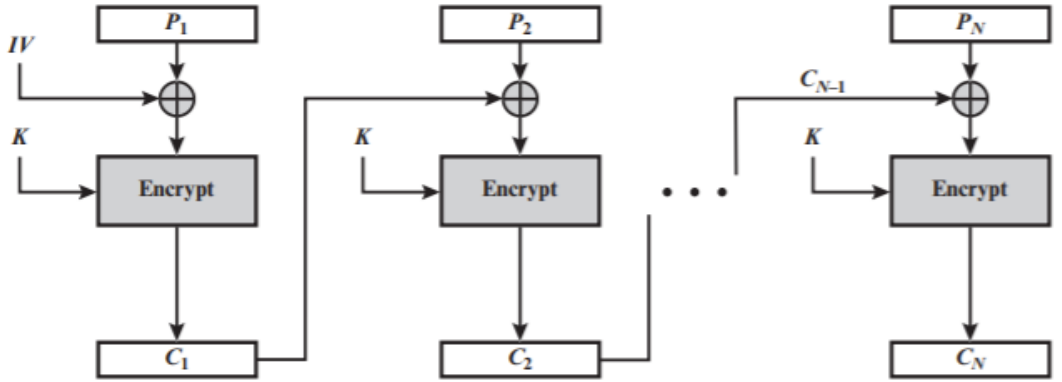


- Přidává k algoritmu mechanismus ***zpětné vazby*.**
- Každý blok šifrového textu (ŠT) je použit pro zašifrování dalšího bloku otevřeného textu (ŠT bloku je kontextově závislý).
- Každý blok ŠT je závislý na všech předešlých blocích otevřeného textu.
- Blok m_i je XORován se šifrou bloku m_{i-1} před šifrováním / po dešifrování:

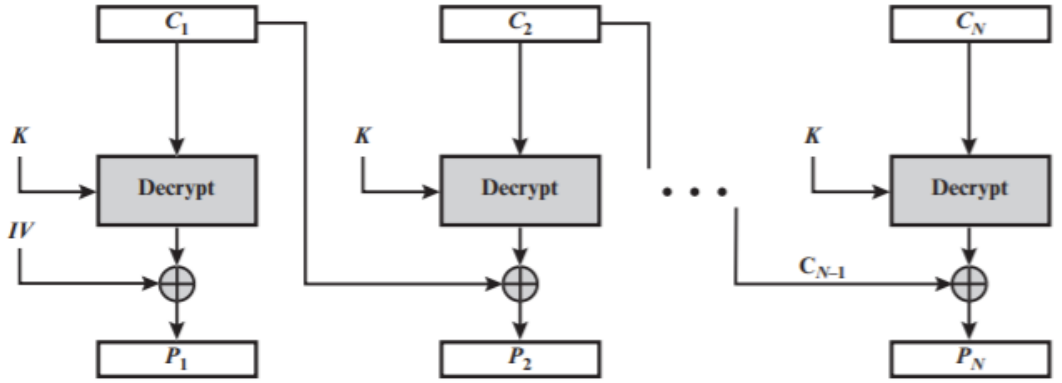
  $c_i = e_k(m_i \oplus c_{i-1})$, $m_i = c_{i-1} \oplus d_k(c_i)$, pro i >1
- Pro šifrování prvního bloku používá inicializační vektor IV (pseudonáhodná data):

  $c_1 = e_k(m_1 \oplus IV)$, $m_1 = IV \oplus d_k(c_1)$
- IV se šifruje v ECB režimu
- Opakovaný blok je šifrován odlišně, pouze když je odlišný některý z předchozích bloků M.

Cipher Block Chaining Mode



(a) Encryption



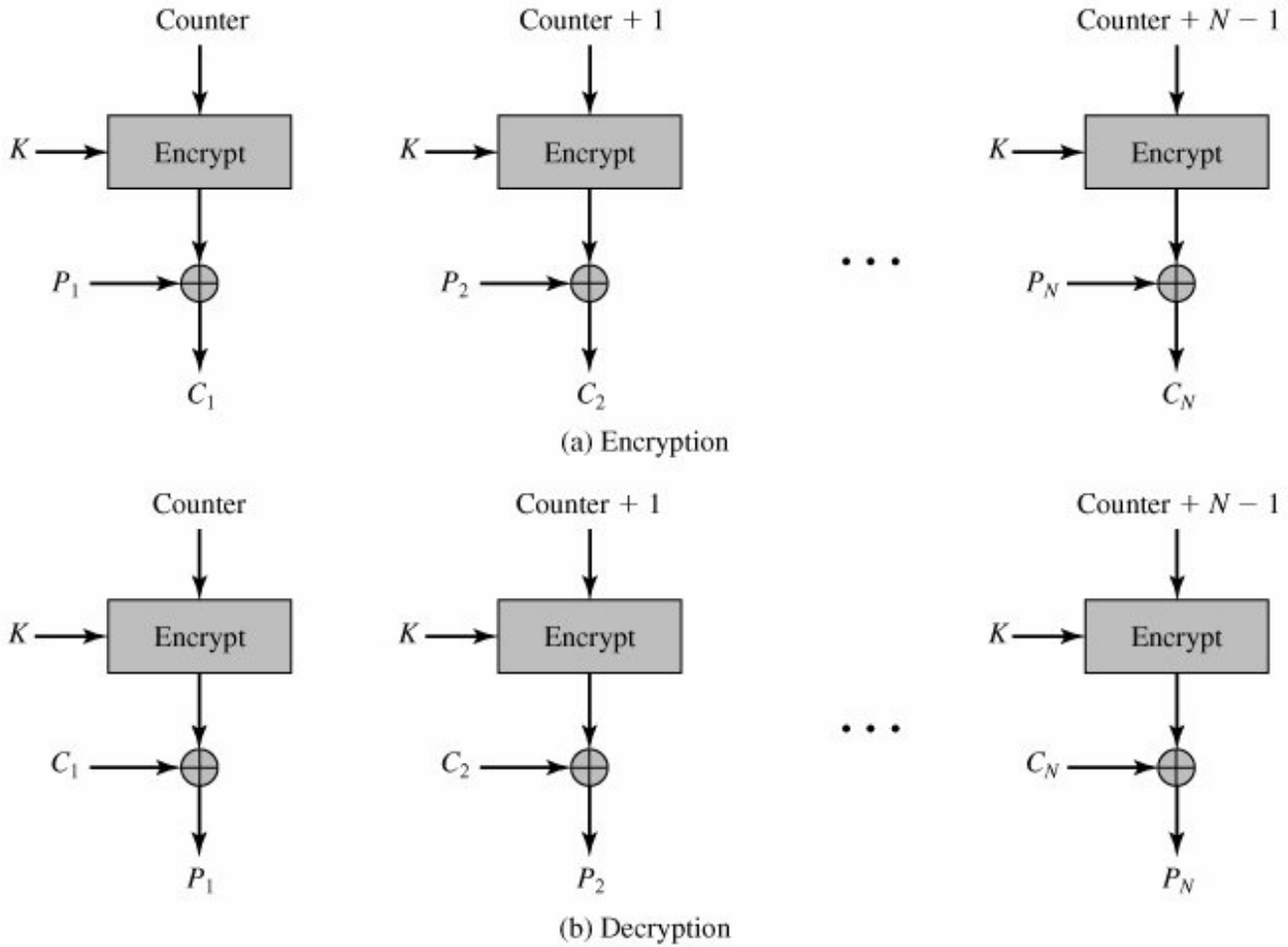
(b) Decryption

Cipher Block Chaining Mode

- ✓ Chyba v jednom bitu M tolik nevadí, po dešifrování se v M objeví zase jen tato chyba.
- ✓ Chyba v C je obvyklejší (poruchový spoj, chyba na paměťovém médiu) - chyba v jednom bitu bloku C_i ovlivní dešifrování tohoto a následujícího bloku C_{i+1}, nazývá se *error extension,* z této chyby se systém zotaví - CBC je *self recovering.*
- ✓ Nešifrovaný text je skrýván (je XORován).
- ✓ Snadná softwarová implementace.
- ✓ Šifrování je neparalelizovatelné, dešifrování ano.
- ✓ Vhodný pro šifrování souborů.
- ✓ Bezpečnější než ECB.

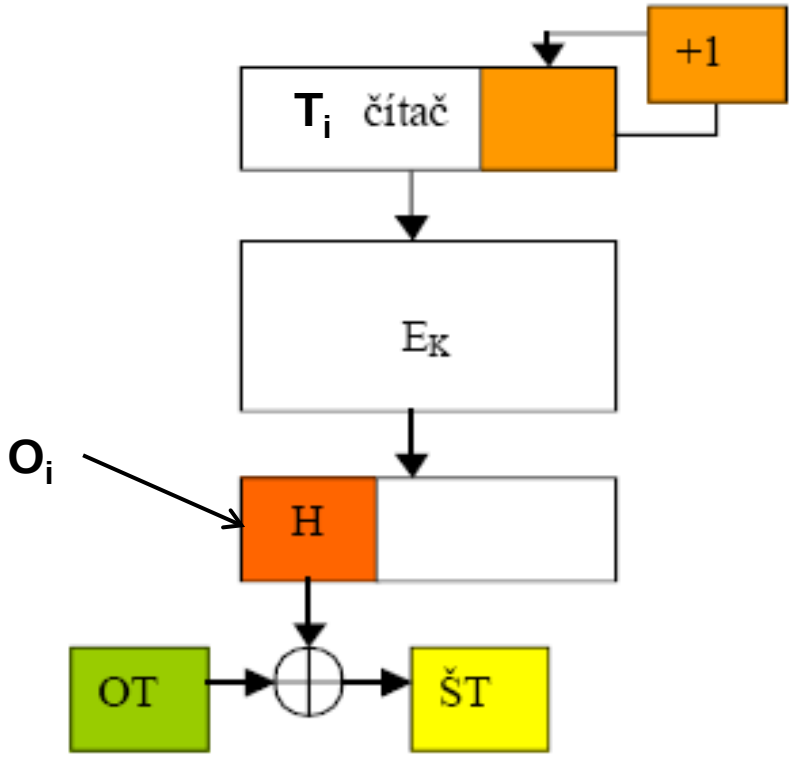
- × Pokud však je bit do šifry C přidán či z ní ztracen, z této chyby se systém nezotaví.
- × Vaudenay 2002 - útok postranním kanálem (postranní kanály viz později) – využitím chybového hlášení

CTR režim


Counter
Counter + 1
Counter + N − 1
K
Encrypt
P_1
P_2
P_N
C_1
C_2
C_N
(a) Encryption
Counter
Counter + 1
Counter + N − 1
K
Encrypt
C_1
C_2
C_N
P_1
P_2
P_N
(b) Decryption

CTR režim

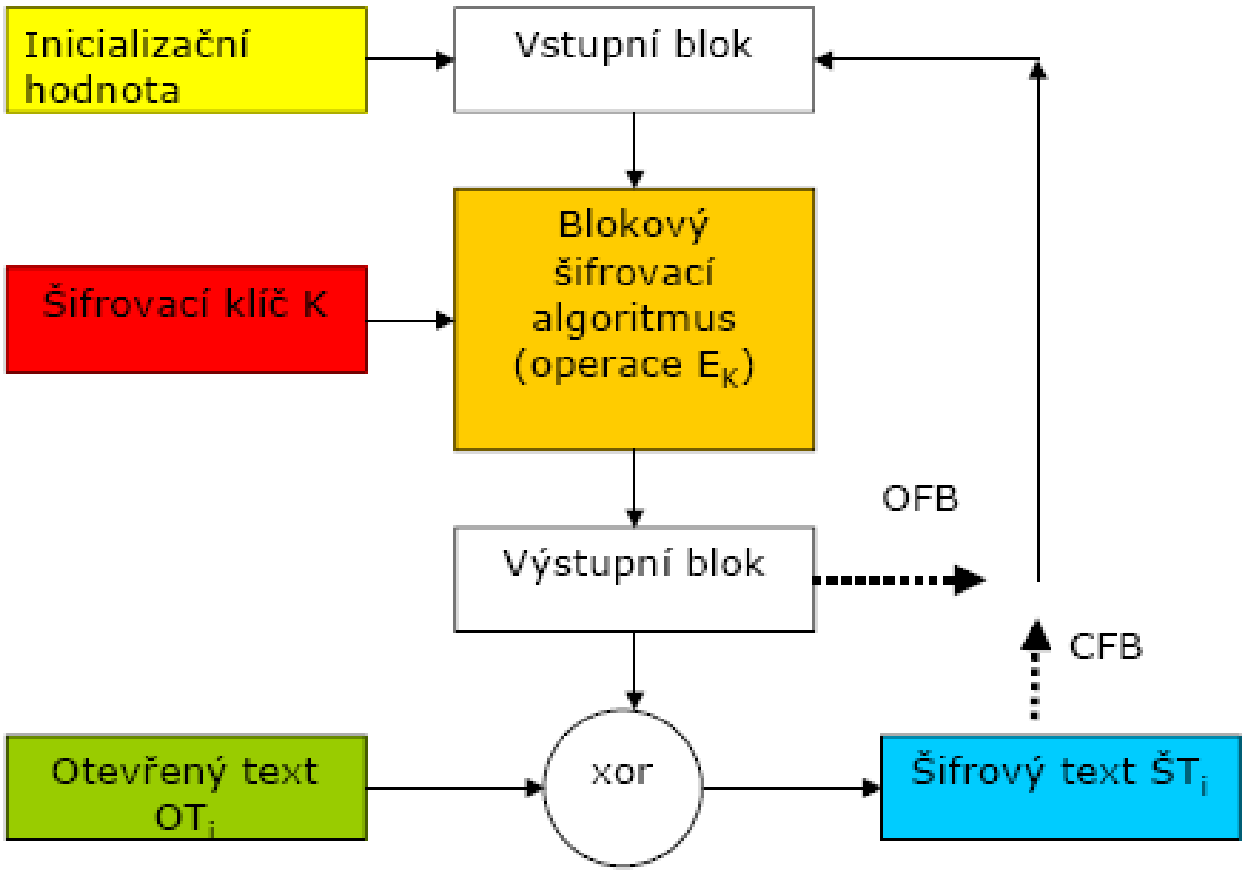
- Režim ***Counter mode*** používá posloupnost čítačů T_1, T_2, ..., T_n, pro které platí, že každý blok T_i je jiný než všechny ostatní.
- používá pouze šifrovací alg.E_K
- výstup lze použít celý nebo část
- různé způsoby inkrementace
- čítač se může týkat jen (dolní) části registru inicializačního vektoru
- smyslem je zaručit různé hodnoty čítače použité během životnosti jednoho klíče
- **hlavní výhoda:** heslo O_i může být vypočítáno jen na základě pozice a IV, nezávisle na ničem jiném



CTR režim

- Režim CRT může být definován takto:
  - $O_i = e_k(T_i)$ pro i = 1, .., n − 1, $c_i = m_i \oplus O_i$ pro i = 1, .., n − 1, $c_n = m_n \oplus msb_u(O_n)$,
  - $O_i = e_k(T_i)$ pro i = 1, .., n − 1, $m_i = c_i \oplus O_i$ pro i = 1, .., n − 1, $m_n = c_n \oplus msb_u(O_n)$.
- Pro poslední blok dat, který může mít jen *u* bitů (msb - most significant bits) se neprovádí padding. Operace XOR se provede jen pro těchto *u* platných bitů.

Blokové šifry v proudovém režimu (CFB, OFB)



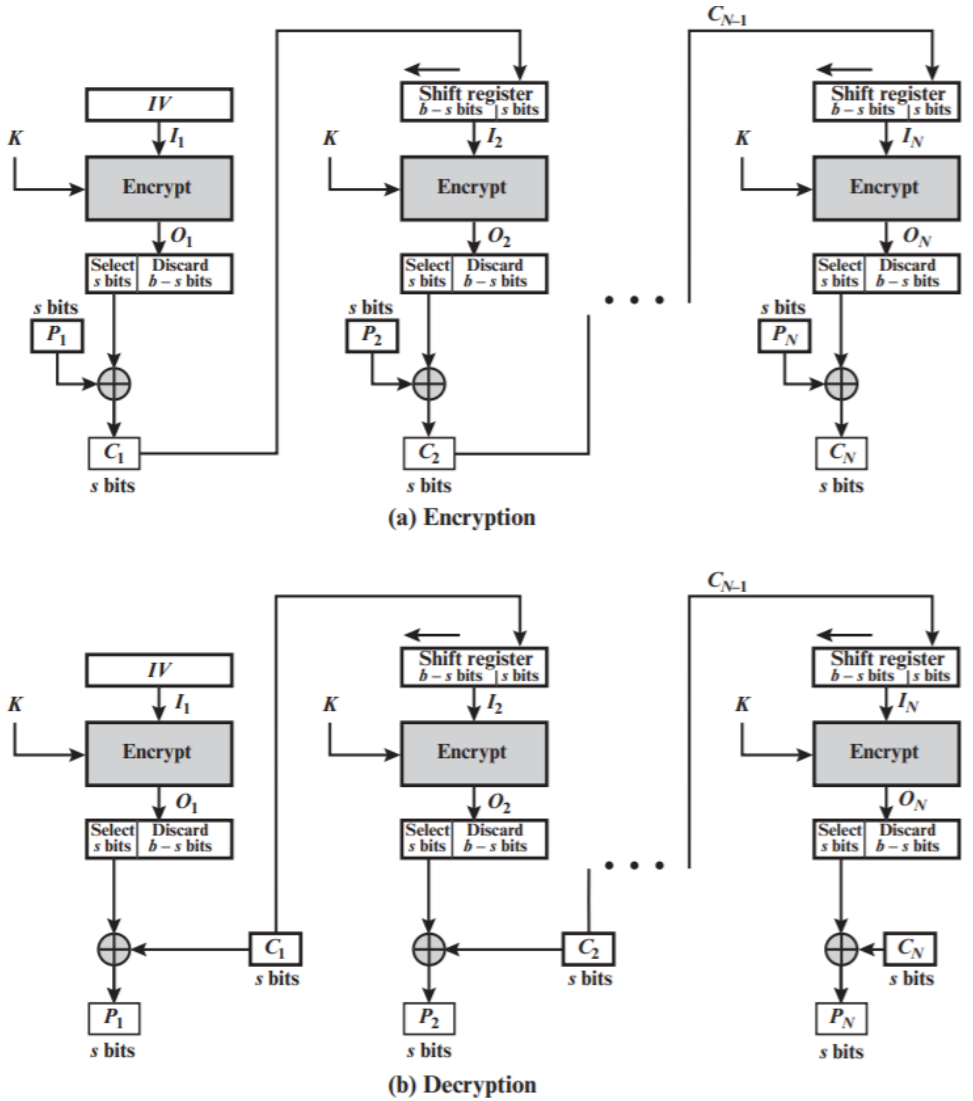
Cipher-Feedback Mode CFB

- U CFB se nemusí zpráva rozdělovat na bloky o velikosti odpovídající velikosti bloku, data mohou být šifrována po jednotkách menších než je velikost bloku. Se zprávou se pracuje jako s plynulým proudem dat o libovolné velikosti.
- Obecně máme dva parametry j a n → blokové šifry pracují jako proudové
  - j odpovídá délce úseků, na které je blok zprávy rozdělen (typicky j=8),
  - n reprezentuje velikost bloku blokové šifry (nejméně 128 bitů).
- Šifrování a dešifrování používá stejný algoritmus E, tedy bloková šifra slouží jako generátor pseudonáhodné posloupnosti, která je použita pro zašifrování otevřeného textu operací XOR.
- Generátor je ovlivňován zpětnou vazbou získanou ze šifrového textu.
- Bity klíče jsou funkcí předchozích bitů šifrového textu
- Opakované vzorky otevřeného textu nedávají opakované vzorky v textu šifrovém.

Cipher-Feedback Mode

- Vstupem algoritmu jedinečný IV, který je nutno generovat nový pro každou novou zprávu.
- Šifrování je neparalelizovatelé, dešifrování ano.
- Používá se pro přenosy proudové povahy, např. pro šifrování znakových terminálů (8-bitový CFB), dále např. pro autentizaci.
- Více než jedna zpráva může být šifrována stejným klíčem.
- Má samosynchronizující vlastnost, ale je třeba $\lceil n/j \rceil$ bloků pro zotavení.
  - Změna pořadí bloků šifrového textu ovlivní dešifrování. Korektní dešifrování bloku vyžaduje korektních $\lceil n/j \rceil$ předcházejících bloků šifrového textu.
  - Chyba v bitu j-bitového šifrového textu ovlivní jeho dešifrování a dešifrování následujících $\lceil n/j \rceil$ bloků šifrového textu.
- Vnější zpětná vazba algoritmu v režimu CFB zvyšuje jeho náchylnost na chybovost způsobovanou poruchami spoje.

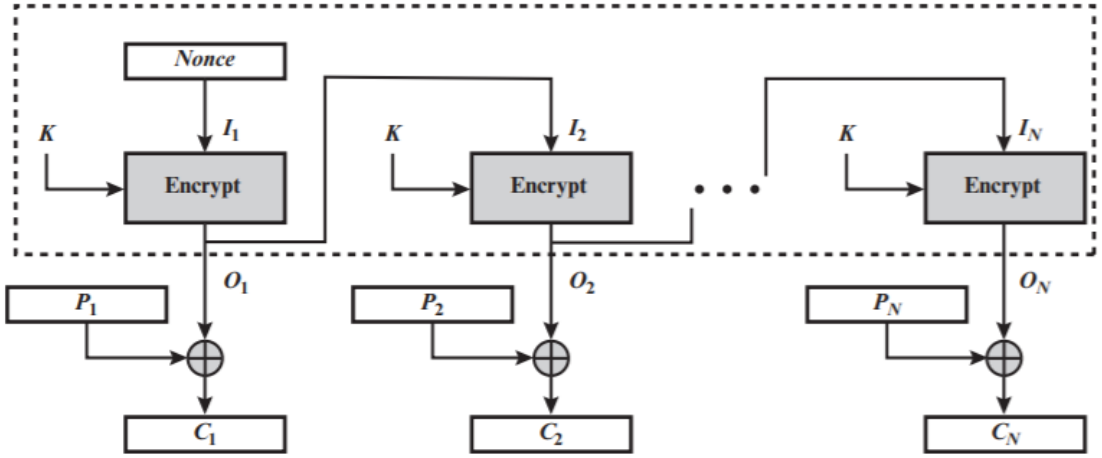
Cipher-Feedback Mode



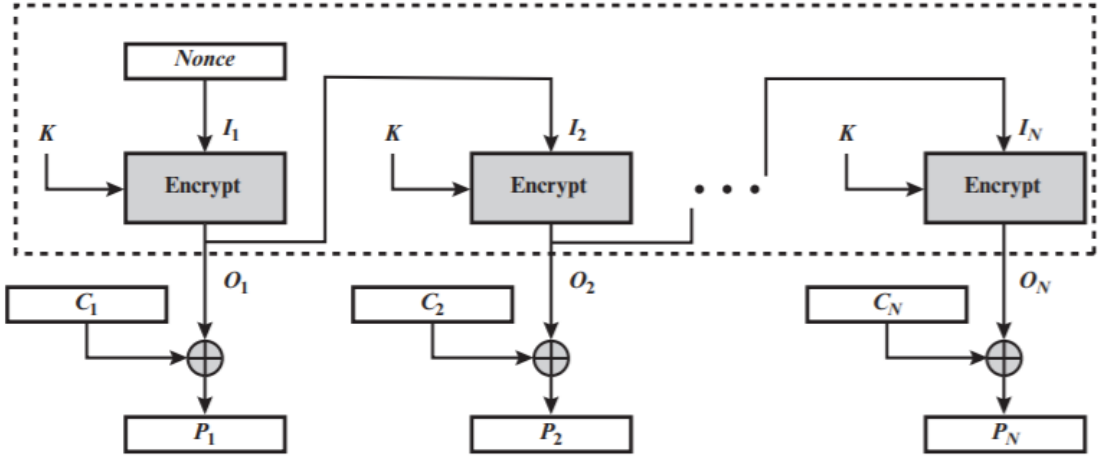
Output-Feedback Mode OFB

- Opakované vzorky otevřeného textu nedávají opakované vzorky v textu šifrovém.
- Generátor není ovlivňován šifrovým textem, ale pouze výstupem samotného generátoru.
- Proud bitů klíče je nezávislý na m i c.
- Vstupem je jedinečný IV. Tj. více než jedna zpráva může být šifrována se stejným klíčem, ale IV musí být jedinečný, je-li znovu použit stejný klíč.
- Šifrování je neparalelizovatelé, dešifrování také.
- Je vhodný pro vysokorychlostní systémy s nepřípustným šířením chyb (satelitní systémy).
- Chyba v bitu šifrového textu ovlivní pouze odpovídající bit otevřeného textu, ale ztráta bloku (bitu) šifrového textu vede k chybnému dešifrování a tedy ke ztrátě synchronizace přenosu .
- Zpětná vazba algoritmu v režimu OFB nezvyšuje jeho náchylnost na chybovost způsobovanou poruchami spoje, ale režim je náchylnější k manipulaci se zprávou (pokud útočník zná otevřený text, umí vypočítat proud bloků a zkonstruovat šifrový text k otevřenému textu, který si zvolí (stejné délky)).

Output-Feedback Mode OFB



(a) Encryption



(b) Decryption

Kryptografie a počítačová bezpečnost

Matematický background

Opakování pojmů z teorie čísel

- Dělitel, triviální dělitel, společný dělitel, celé číslo, prvočíslo (testování prvočíselnosti)
- Každé přirozené číslo číslo $n \geq 2$ se dá zapsat jednoznačně (až na pořadí) *v* **kanonickém tvaru**

  $n = p_1^{a1} * p_2^{a2} * \ldots * p_k^{ak}$, kde $p_1, p_2, \ldots, p_k$ jsou navzájem různá prvočísla a $a_1, a_2, \ldots, a_k$ jsou přirozená čísla
  - např. $1400 = 2^3 * 5^2 * 7$.

Motivace

- Shift Cipher
  - $M=C=K=Z_{26}$,
  - $Z_{26}=\{0,1,2,\ldots,25\}$ je konečná podmnožina množiny celých čísel, množina celých čísel modulo 26
  - zpráva m se šifruje znak po znaku

    $e_k(m)=(m+k) \mod 26$

    $d_k(c)=(c-k) \mod 26$
  - 25 (26) možných klíčů
- →Aritmetické operace s prvky konečné podmnožiny nekonečné množiny celých čísel →
- Kolik různých operací potřebujeme? Chceme jich co nejméně, časově a implementačně efektivní operace, …