Block Cipher

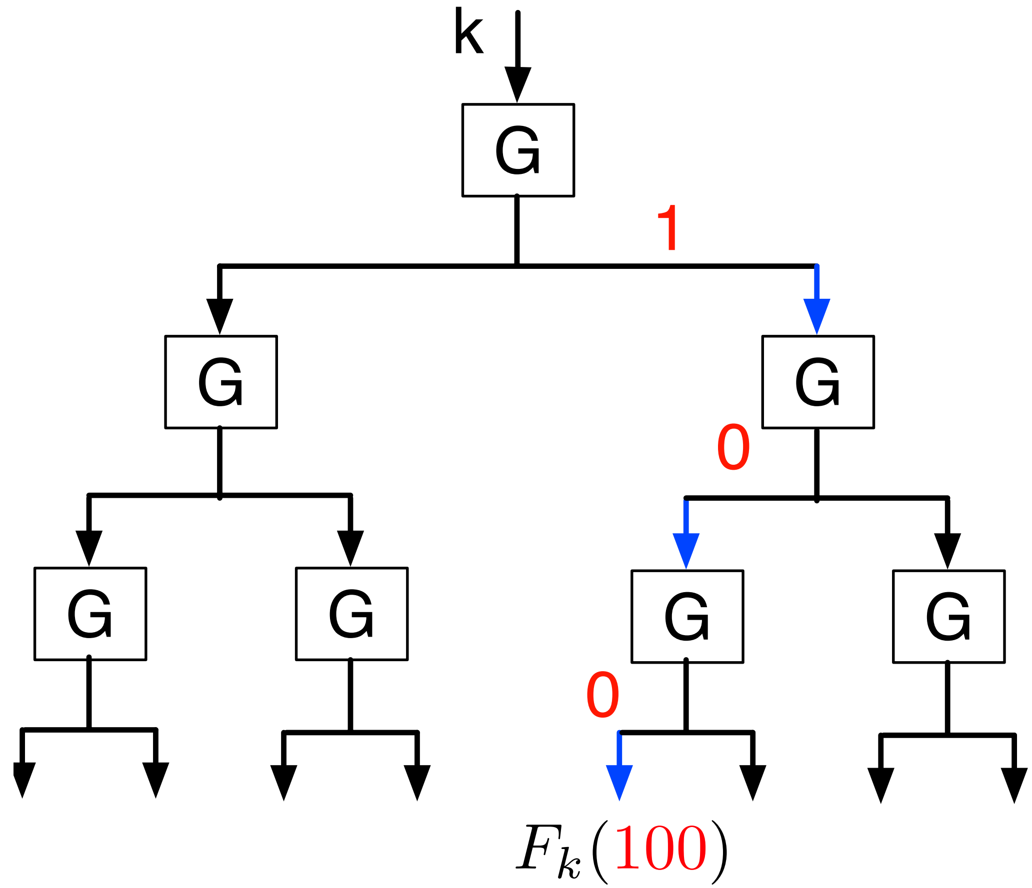
CS 5158/6058 Data Security and Privacy

Spring 2018

Instructor: Boyang Wang

GGM: From PRG to PRF

- A binary tree, each node is a PRG
- Output's left half is input of left child
- An output of PRF is a leaf's left/right half of the output
- Inputs of PRF decide the path in the tree



$F_k(100) = G_0(G_0(G_1(k)))$

GGM: From PRG to PRF

- Practice: GGM Method
- PRG, G: $\{0,1\}^n$ —> $\{0, 1\}^{2n}$, PRF, F: $\{0,1\}^m$ —> $\{0,1\}^n$
  - n=1, G(0) —> 10, G(1) —> 01
  - $F_k(x_1x_2x_3) = G_{x3}(\ G_{x2}(\ G_{x1}(k)\ )\ )$
  - $k = 1$, $x_1x_2x_3 = 110$, What is the output of $F_k(110)$?

- $G(k) = G(1) = 0\underline{1}$, $G_{x1}(k) = G_1(1) = 1$;
- $G(G_{x1}(k)) = G(1) = 0\underline{1}$, $G_{x2}(G_{x1}(k)) = G_1(1) = 1$;
- $G(G_{x2}(G_{x1}(k))) = G(1) = \underline{0}1$, $G_{x3}(G_{x2}(G_{x1}(k))) = G_0(1) = 0$
- $F_k(110) = G_{x3}(G_{x2}(G_{x1}(k))) = 0$

CPA-Secure Enc. from PRF

- $\textsf{KeyGen}(1^n) : k \xleftarrow{u} \{0,1\}^n$
- $\textsf{Enc}_k(m) : c \leftarrow \langle r, F_k(r) \oplus m \rangle,\ r \xleftarrow{u} \{0,1\}^n$
- $\textsf{Dec}_k(c)$ given $c = \langle r, s \rangle,\ m \leftarrow F_k(r) \oplus s$

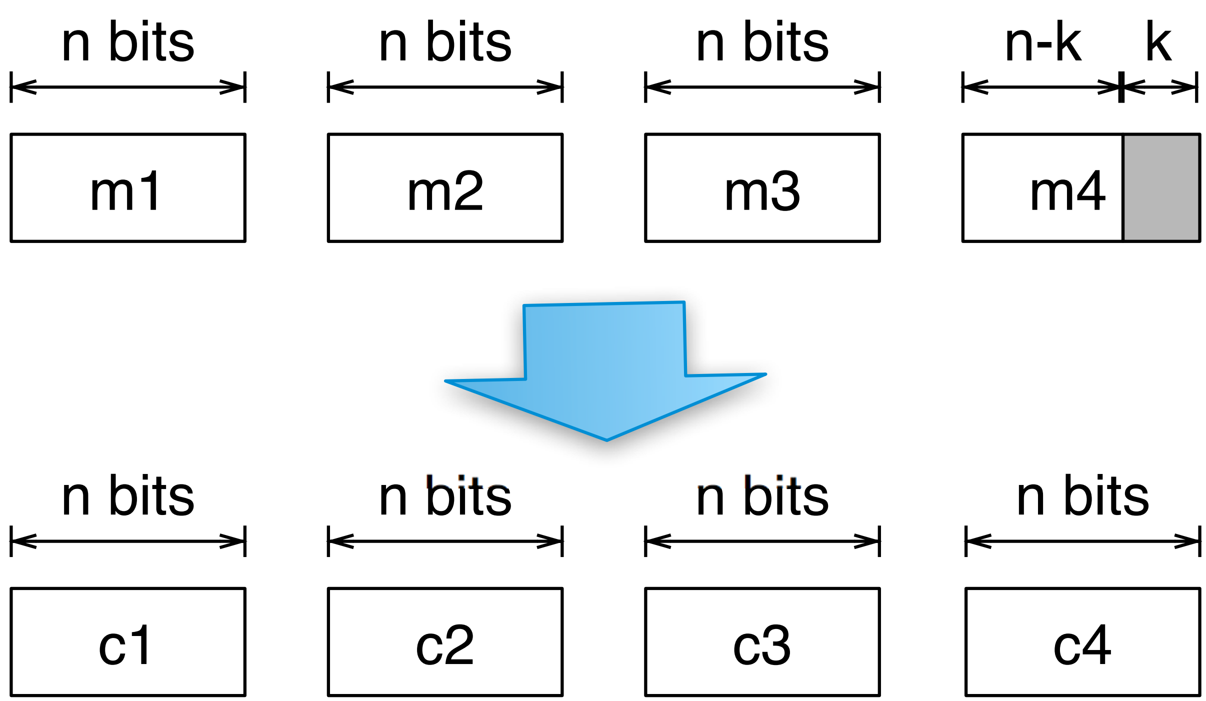
- Probabilistic encryption, CPA-secure
- <u>Message length is fixed</u>
  - n=2, can encrypt 2 bits, what if m = 1 or m =101
- We need a scheme for arbitrary message size

x	00	01	10	11
k=00,F(x)	11	00	01	10
k=01,F(x)	10	11	00	01
k=10,F(x)	01	10	11	00
k=11,F(x)	00	01	10	11

- Practice: given m=01, k=10, what is c=??
  - if r = 00, $F_k(r)$ = 01, $F_k(r) \oplus m$ = 00, c = (00, 00)
  - if r = 01, $F_k(r)$ = 10, $F_k(r) \oplus m$ = 11, c = (01, 11)
  - if r = 10, $F_k(r)$ = 11, $F_k(r) \oplus m$ = 10, c = (10, 10)
  - if r = 11, $F_k(r)$ = 00, $F_k(r) \oplus m$ = 01, c = (11, 01)
  - Probabilistic: same message, different ciphertexts

Block Ciphers

- Encrypt arbitrary-length plaintexts (from PRF/PRP)
  - Multiple blocks, each has n bits (e.g., 128 bits)
  - Pad the last block if necessary



ECB Mode

- Electronic Code Book (ECB)
  - Deterministic, decryption use inverse function
  - Normally, ECB is not used in practice

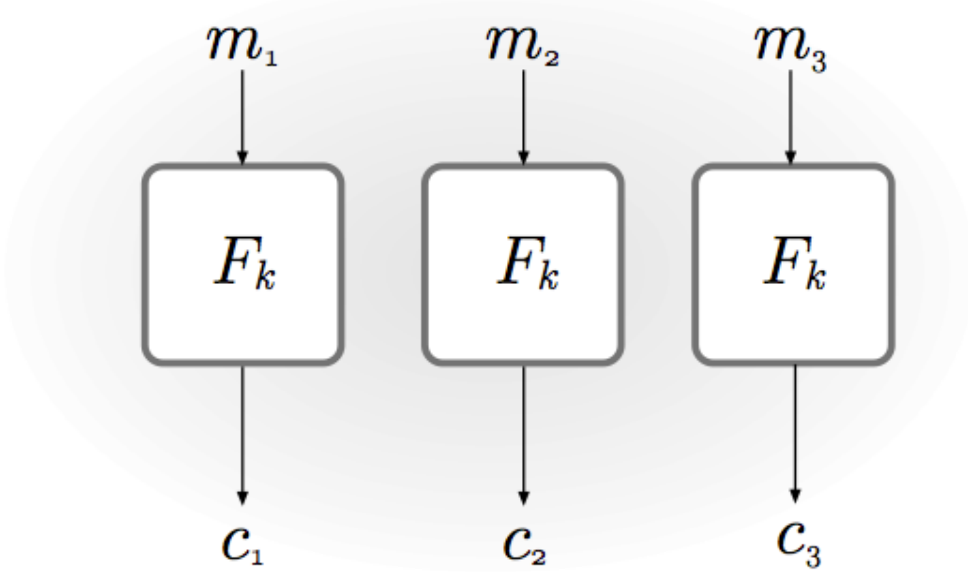


FIGURE 3.5: Electronic Code Book (ECB) mode.

$$c_i = F_k(m_i)$$

$$m_i = F_k^{-1}(c_i)$$

x	00	01	10	11
k=00,F(x)	11	00	01	10
k=01,F(x)	10	11	00	01
k=10,F(x)	01	10	11	00
k=11,F(x)	00	01	10	11

- Example
- ECB Mode Encryption:
  - M = 100111
  - k = 01
  - each block has 2 bits
  - C = ?? ?? ??

$$c_i = F_k(m_i)$$

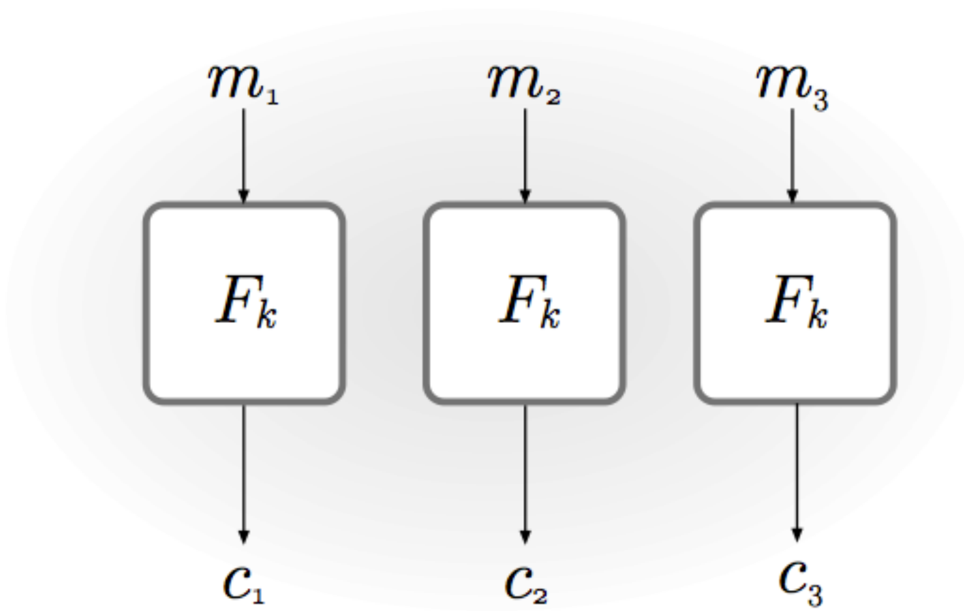


FIGURE 3.5: Electronic Code Book (ECB) mode.

x	00	01	10	11
k=00,F(x)	11	00	01	10
k=01,F(x)	10	11	00	01
k=10,F(x)	01	10	11	00
k=11,F(x)	00	01	10	11

M = 10 01 11 & k = 01

- $c_1 = F_k(10) = 00$
- $c_2 = F_k(01) = 11$
- $c_3 = F_k(11) = 01$
- C = 00 11 01
- deterministic

$$c_i = F_k(m_i)$$

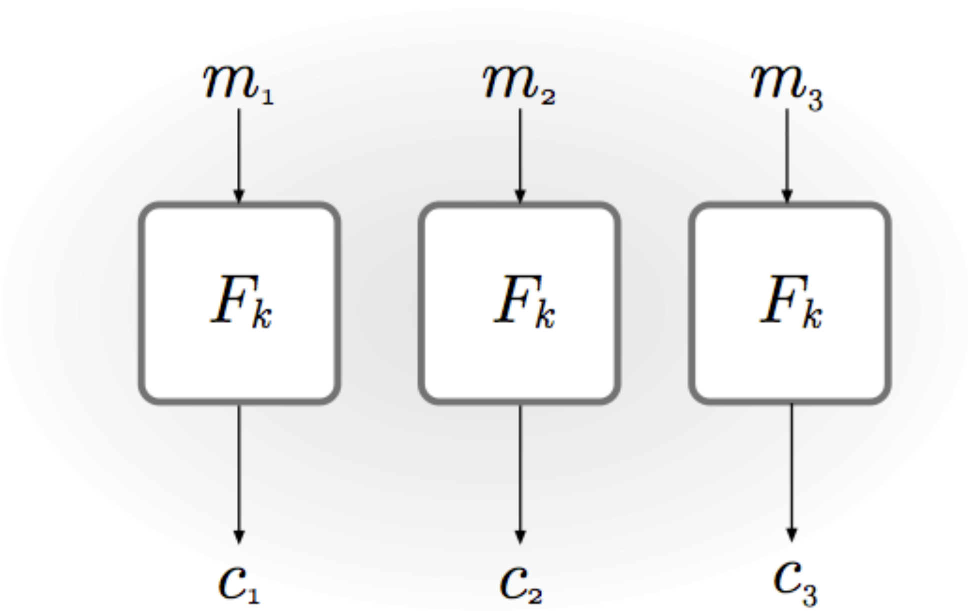


FIGURE 3.5: Electronic Code Book (ECB) mode.

x	00	01	10	11
k=00,F(x)	11	00	01	10
k=01,F(x)	10	11	00	01
k=10,F(x)	01	10	11	00
k=11,F(x)	00	01	10	11

- Practice:
- ECB Mode Encryption:
  - M =010010
  - k = 11
  - each block has 2 bits
  - C = ??????

$$c_i = F_k(m_i)$$

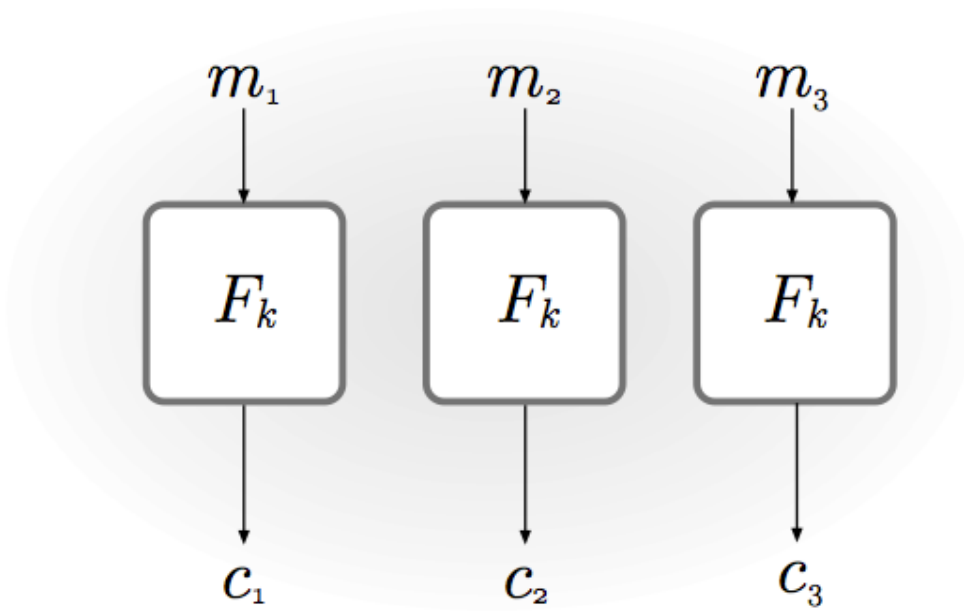


FIGURE 3.5: Electronic Code Book (ECB) mode.

x	00	01	10	11
k=00,F(x)	11	00	01	10
k=01,F(x)	10	11	00	01
k=10,F(x)	01	10	11	00
k=11,F(x)	00	01	10	11

- <u>Practice:</u>
- ECB Mode Decryption:
    - C = 110100
    - k = 10
    - each block has 2 bits
    - M = ??????

$$c_i = F_k^{-1}(m_i)$$

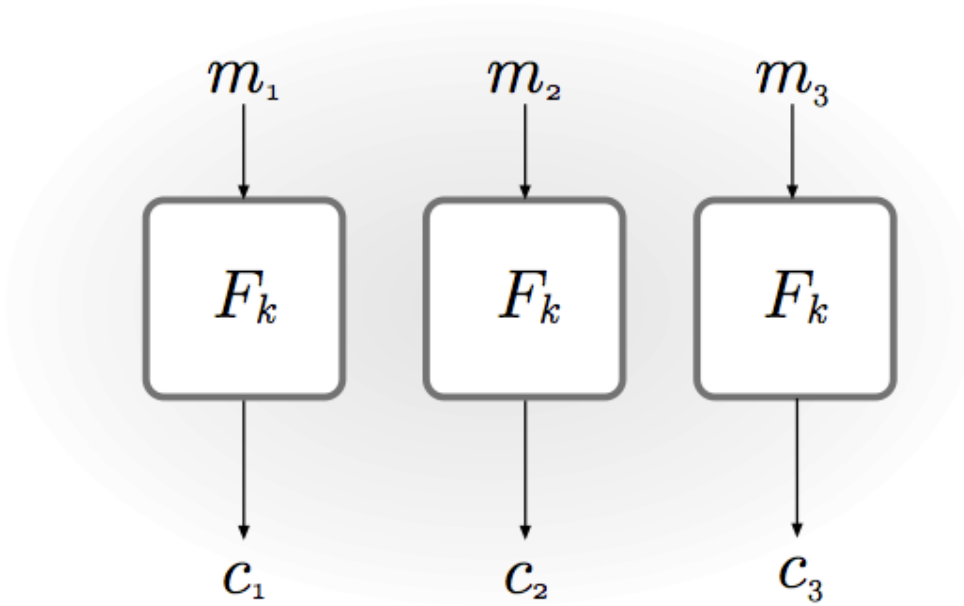


FIGURE 3.5: Electronic Code Book (ECB) mode.

x	00	01	10	11
k=00,F(x)	11	00	01	10
k=01,F(x)	10	11	00	01
k=10,F(x)	01	10	11	00
k=11,F(x)	00	01	10	11

$$c_i = F_k^{-1}(m_i)$$

C = 11 01 00 & k = 10

- $m_1 = F_k^{-1}(11) = 10$
- $m_2 = F_k^{-1}(01) = 00$
- $m_3 = F_k^{-1}(00) = 11$
- M = 10 00 11

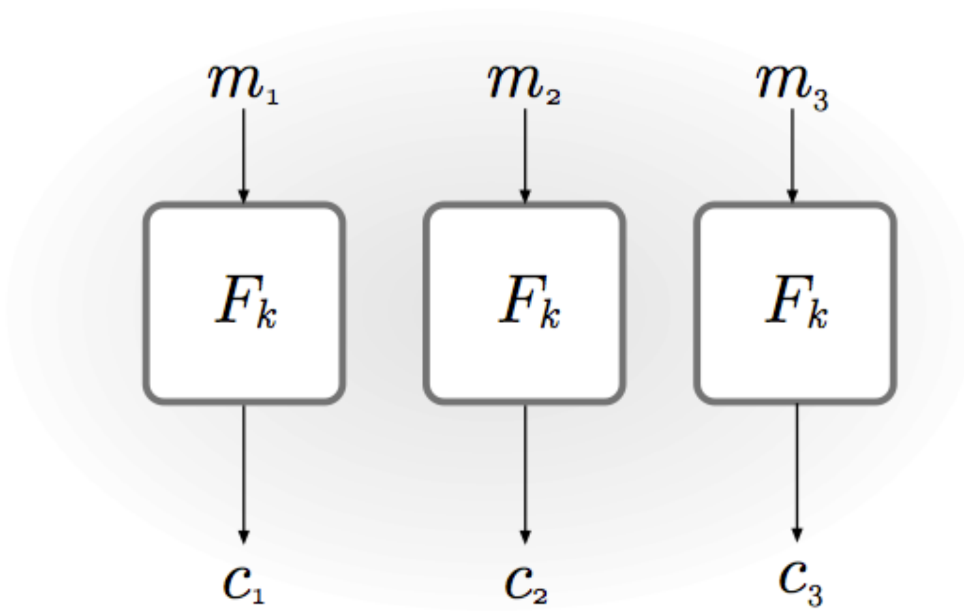


FIGURE 3.5: Electronic Code Book (ECB) mode.

CBC Mode

- Cipher Block Chaining (CBC)
  - Probabilistic, is CPA-secure if F is a PRP
  - IV (initialization vector) chosen uniformly from $\{0,1\}^n$

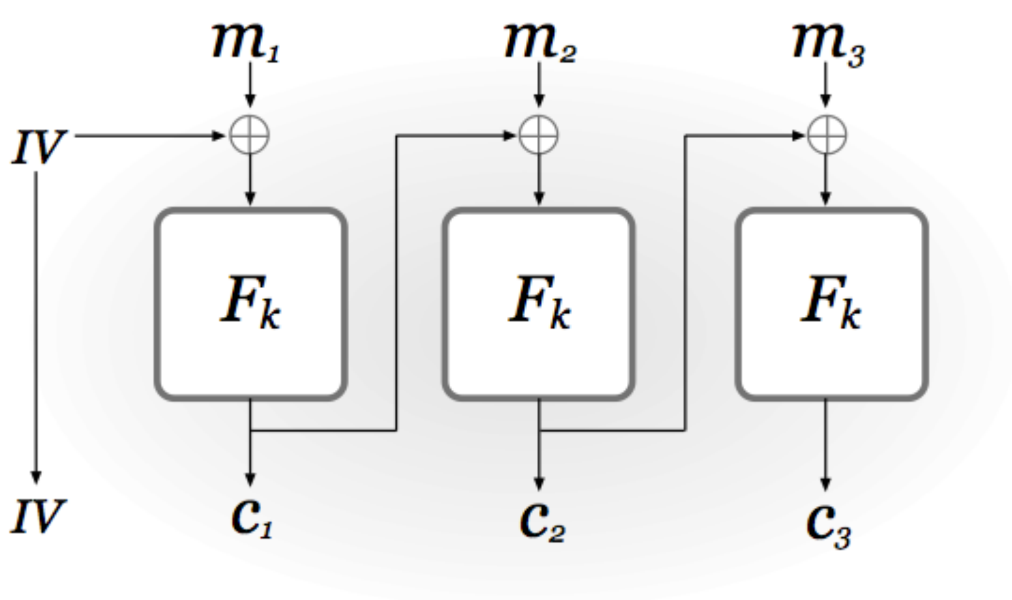


FIGURE 3.7: Cipher Block Chaining (CBC) mode.

$$c_0 = IV,$$
$$c_i = F_k(m_i \oplus c_{i-1})$$

$$c_0 = IV,$$
$$m_i = F_k^{-1}(c_i) \oplus c_{i-1}$$

x	00	01	10	11
k=00,F(x)	11	00	01	10
k=01,F(x)	10	11	00	01
k=10,F(x)	01	10	11	00
k=11,F(x)	00	01	10	11

- Example
- CBC Mode Encryption:
  - M = 1001
  - k = 01, IV = 10
  - each block has 2 bits
  - C = ?? ??

$$c_0 = IV, c_i = F_k(m_i \oplus c_{i-1})$$

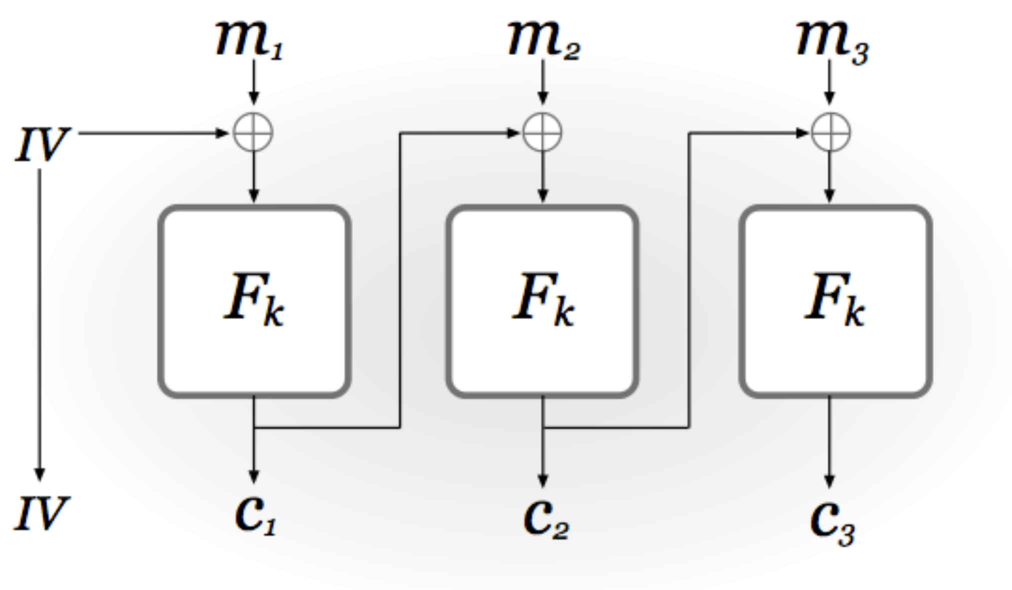


FIGURE 3.7: Cipher Block Chaining (CBC) mode.

x	00	01	10	11
k=00,F(x)	11	00	01	10
k=01,F(x)	10	11	00	01
k=10,F(x)	01	10	11	00
k=11,F(x)	00	01	10	11

M = 1001, k = 01, IV = 10

$$c_0 = IV, c_i = F_k(m_i \oplus c_{i-1})$$

- $IV \oplus m_1 = 10 \oplus 10 = 00$
- $c_1 = F_k(00) = 10$
- $c_1 \oplus m_2 = 10 \oplus 01 = 11$
- $c_2 = F_k(11) = 01$
- C = (IV, 10 01)

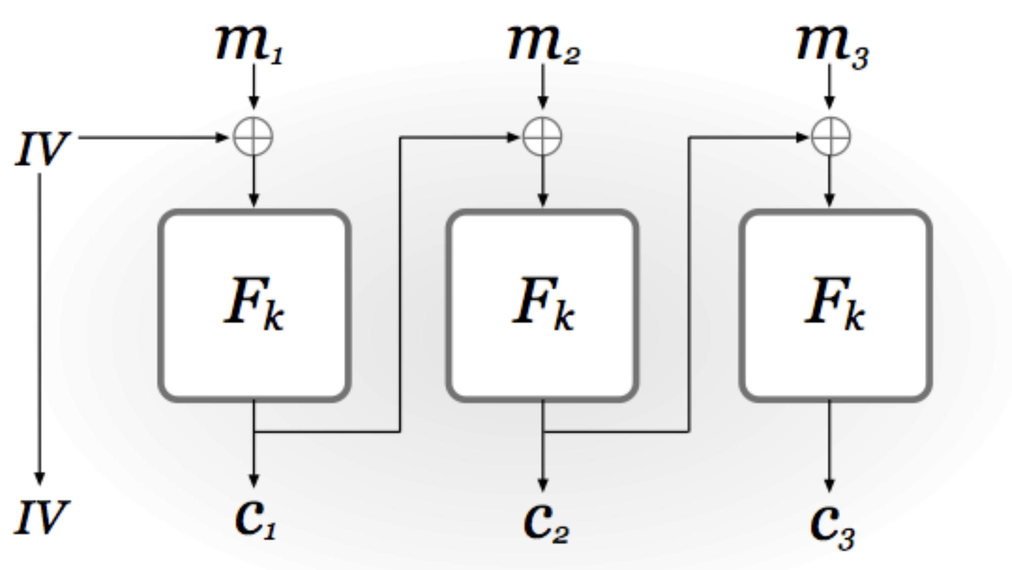


FIGURE 3.7: Cipher Block Chaining (CBC) mode.

x	00	01	10	11
k=00,F(x)	11	00	01	10
k=01,F(x)	10	11	00	01
k=10,F(x)	01	10	11	00
k=11,F(x)	00	01	10	11

- Practice:
- CBC Mode Encryption:
  - M = 110100
  - k = 10, IV = 11
  - each block has 2 bits
  - C = ??????

$$c_0 = IV, c_i = F_k(m_i \oplus c_{i-1})$$

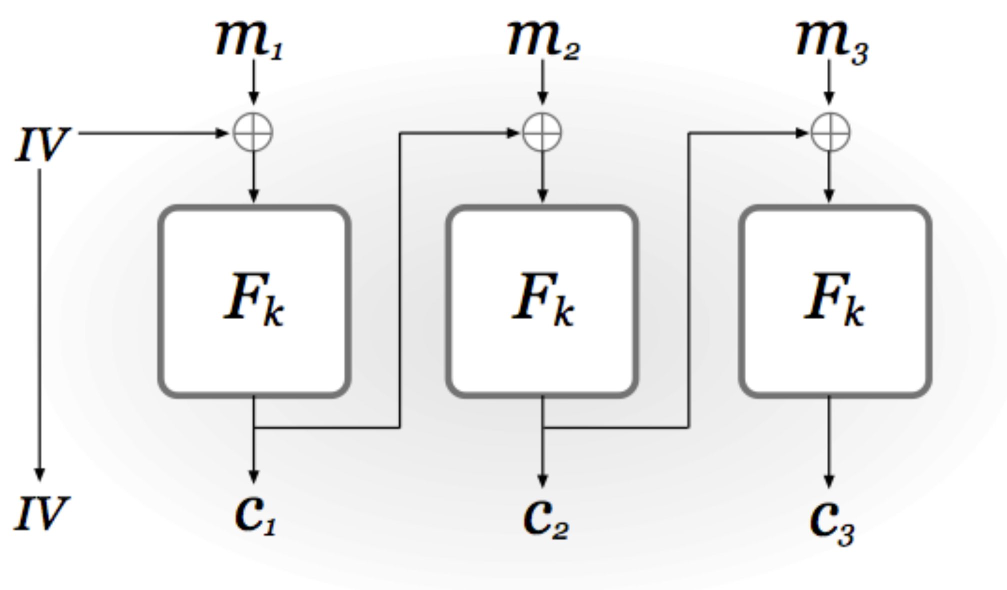


FIGURE 3.7: Cipher Block Chaining (CBC) mode.

x	00	01	10	11
k=00,F(x)	11	00	01	10
k=01,F(x)	10	11	00	01
k=10,F(x)	01	10	11	00
k=11,F(x)	00	01	10	11

M =110100, k = 10, IV = 11 $c_0 = IV, c_i = F_k(m_i \oplus c_{i-1})$

- c_0=IV=11
- $c_1=F_k(00)$= 01
- $c_2=F_k(00)$= 01
- $c_3=F_k(01)$= 10
- C = (IV, 01 01 10)

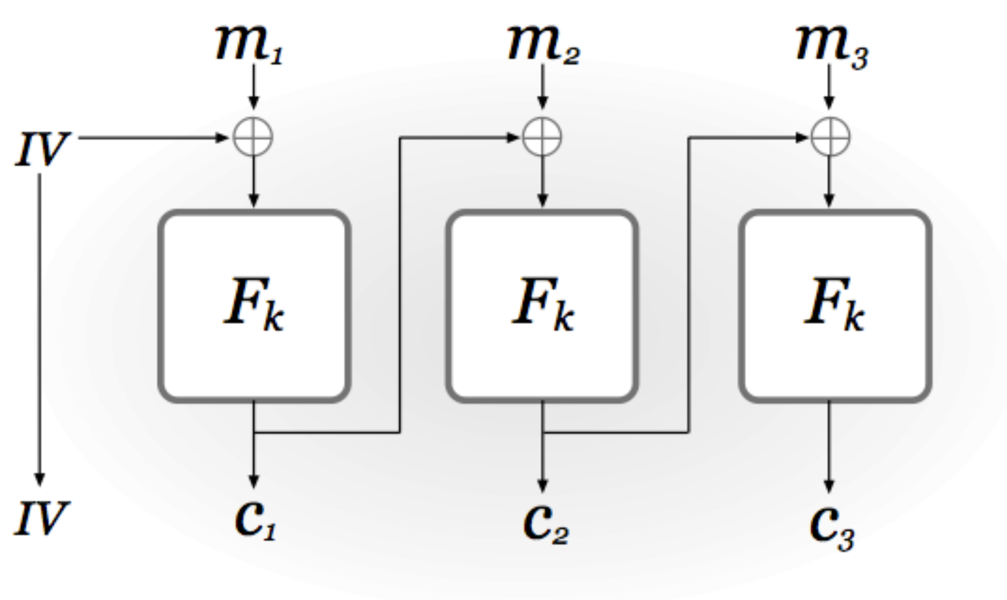


FIGURE 3.7: Cipher Block Chaining (CBC) mode.

x	00	01	10	11
k=00,F(x)	11	00	01	10
k=01,F(x)	10	11	00	01
k=10,F(x)	01	10	11	00
k=11,F(x)	00	01	10	11

- Practice:
- CBC Mode Decryption:
  - C = (IV, 100110)
  - k = 11, IV = 00
  - each block has 2 bits
  - M = ??????

$$c_0 = IV, m_i = F_k^{-1}(c_i) \oplus c_{i-1}$$

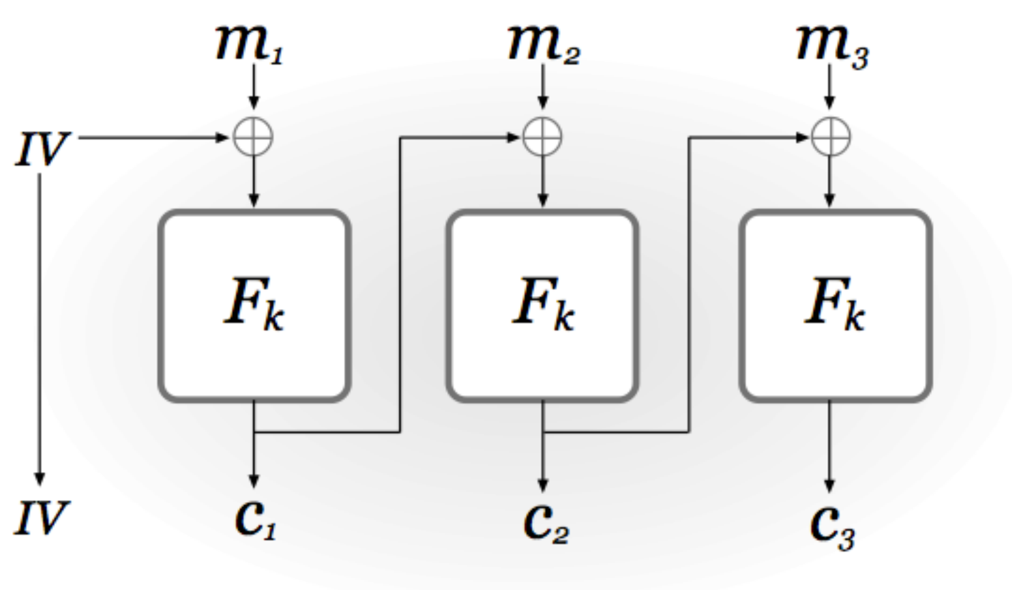


FIGURE 3.7: Cipher Block Chaining (CBC) mode.

x	00	01	10	11
k=00,F(x)	11	00	01	10
k=01,F(x)	10	11	00	01
k=10,F(x)	01	10	11	00
k=11,F(x)	00	01	10	11

$$c_0 = IV, m_i = F_k^{-1}(c_i) \oplus c_{i-1}$$

C = (00, 100110) & k = 11

- $F_k^{-1}(10) = 10$, $m_1 = F_k^{-1}(10) \oplus IV = 10 \oplus 00 = 10$
- $F_k^{-1}(01) = 01$, $m_2 = F_k^{-1}(01) \oplus c_1 = 01 \oplus 10 = 11$
- $F_k^{-1}(10) = 10$, $m_3 = F_k^{-1}(10) \oplus c_2 = 10 \oplus 01 = 11$
- M = 10 11 11

CBC Mode

- Cipher Block Chaining (CBC)
  - Probabilistic, is CPA-secure if F is a PRP
  - IV (initialization vector) chosen uniformly from $\{0,1\}^n$

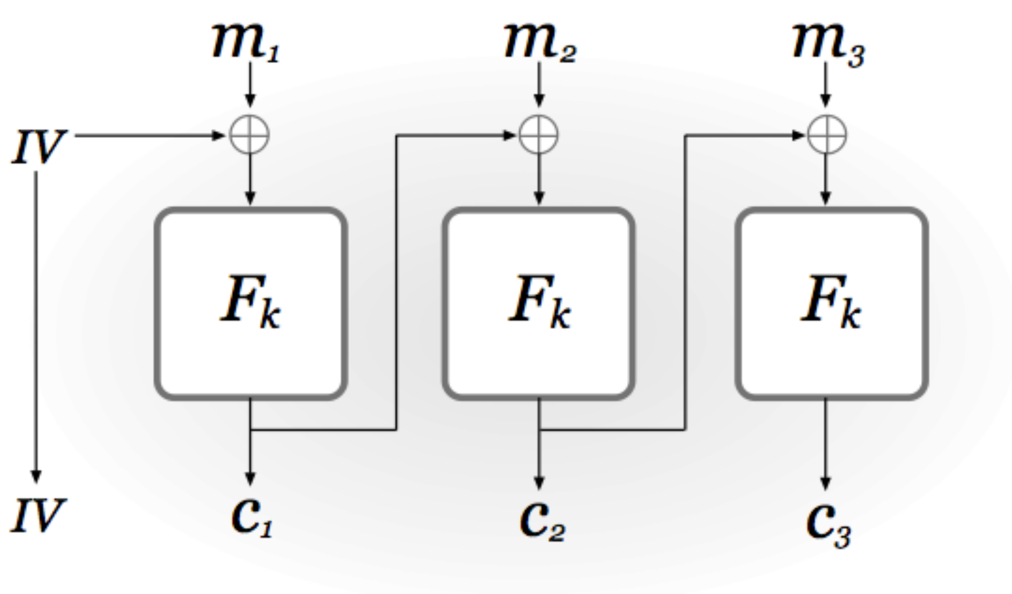


FIGURE 3.7: Cipher Block Chaining (CBC) mode.

$$c_0 = IV,$$
$$c_i = F_k(m_i \oplus c_{i-1})$$

$$c_0 = IV,$$
$$m_i = F_k^{-1}(c_i) \oplus c_{i-1}$$

OFB Mode

- Output Feedback (OFB)
  - Probabilistic,CPA-secure if F is a PRF, IV is random
  - Can <u>pre-compute</u> all the outputs of PRF

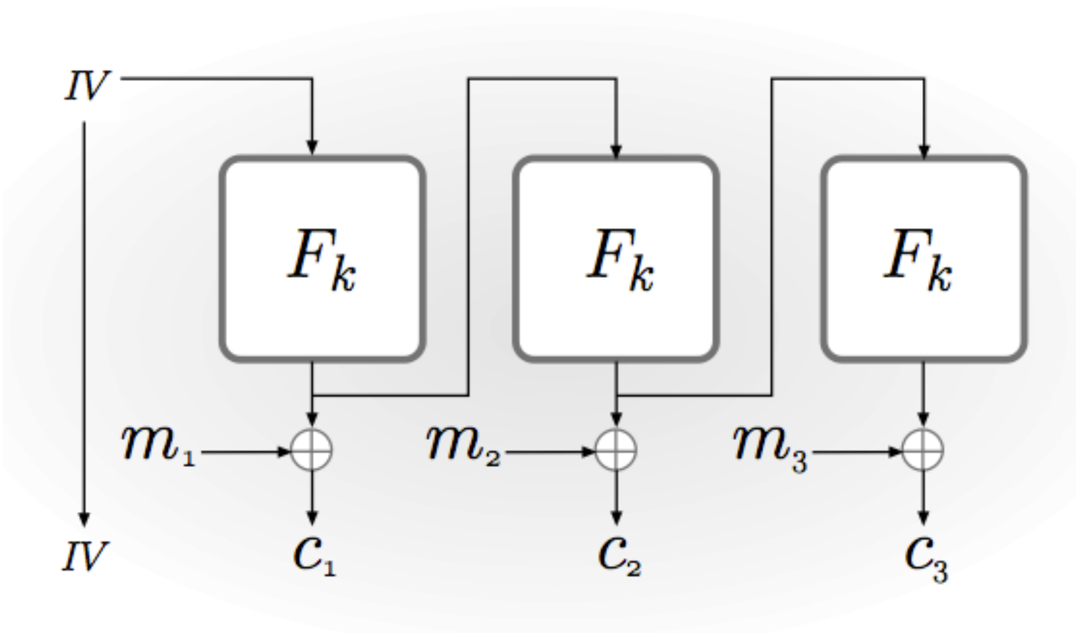


FIGURE 3.9: Output Feedback (OFB) mode.

$$x_0 = IV$$
$$x_i = F_k(x_{i-1})$$
$$c_i = x_i \oplus m_i$$

$$x_0 = IV$$
$$x_i = F_k(x_{i-1})$$
$$m_i = c_i \oplus x_i$$

x	00	01	10	11
k=00,F(x)	11	00	01	10
k=01,F(x)	10	11	00	01
k=10,F(x)	01	10	11	00
k=11,F(x)	00	01	10	11

- <u>Practice:</u>

$$x_0 = IV, x_i = F_k(x_{i-1}), c_i = x_i \oplus m_i$$

- OFB Mode Encryption:
  - M = 110100
  - k = 10, IV = 11
  - each block has 2 bits
  - C = ??????

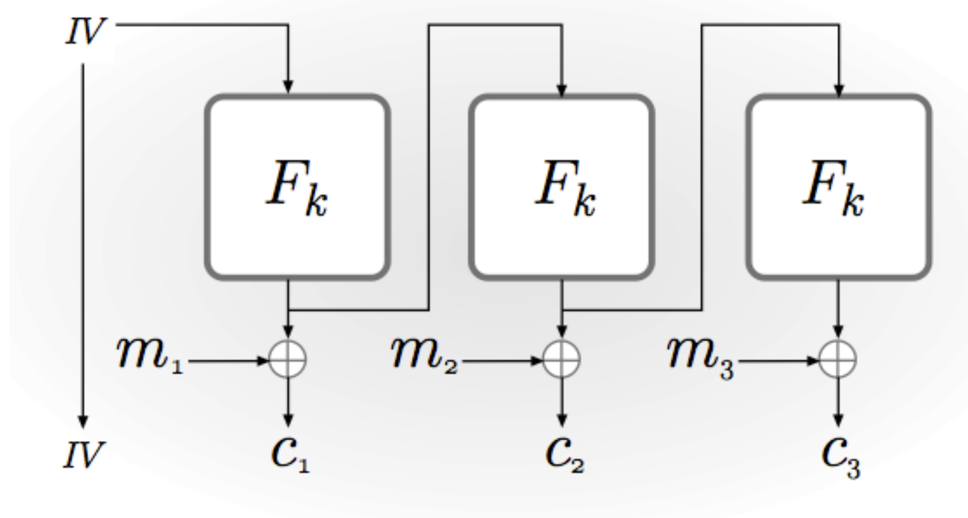


FIGURE 3.9: Output Feedback (OFB) mode.

x	00	01	10	11
k=00,F(x)	11	00	01	10
k=01,F(x)	10	11	00	01
k=10,F(x)	01	10	11	00
k=11,F(x)	00	01	10	11

M =110100

$$x_0 = IV, x_i = F_k(x_{i-1}), c_i = x_i \oplus m_i$$

k = 10, IV = 11

$x_1=F_k(IV)=00$, $c_1=x_1 \oplus m_1=11$

$x_2=F_k(x_1)=01$, $c_2=x_2 \oplus m_2=00$

$x_3=F_k(x_2)=10$, $c_3=x_3 \oplus m_3=10$

C = (IV, 11 00 10)

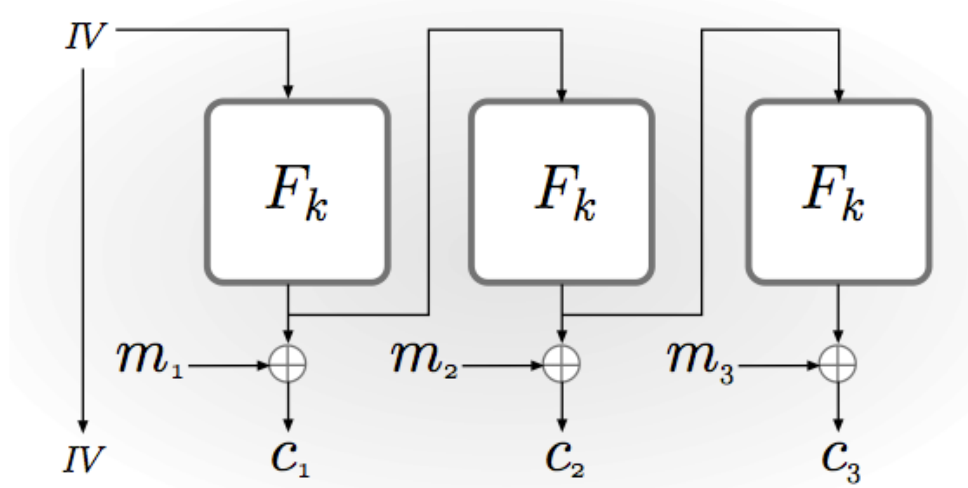


FIGURE 3.9: Output Feedback (OFB) mode.

Counter Mode

- Counter (CTR)
  - Probabilistic,CPA-secure if F is a PRF, IV is random
  - Compute <u>in parallel</u> (each block are independent)

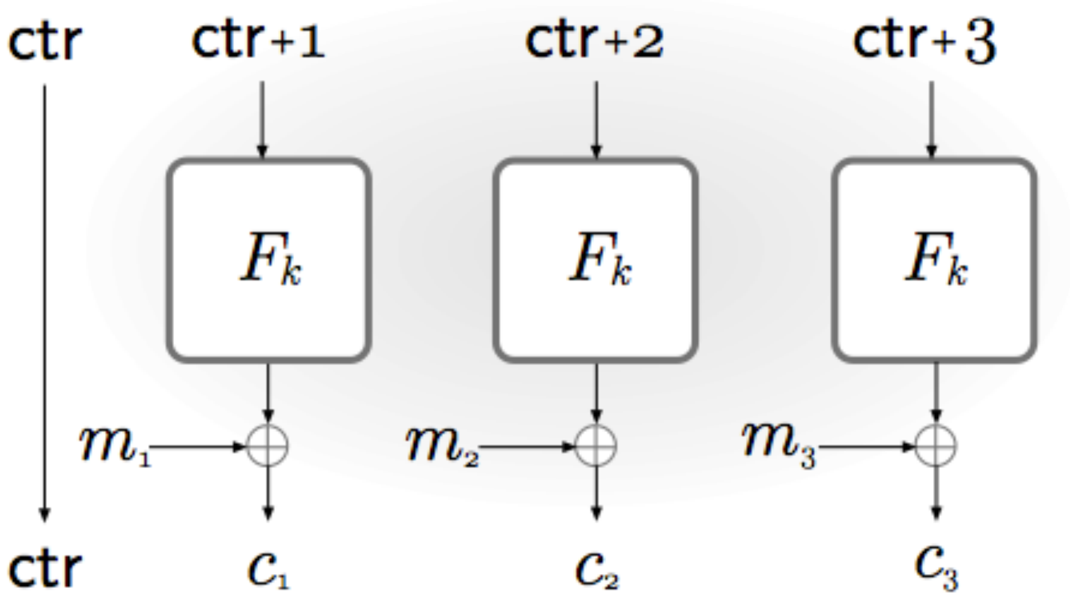


FIGURE 3.10: Counter (CTR) mode.

$$\texttt{ctr} = IV$$
$$x_i = F_k(\texttt{ctr} + 1)$$
$$c_i = x_i \oplus m_i$$

$$\texttt{ctr} = IV$$
$$x_i = F_k(\texttt{ctr} + 1)$$
$$m_i = c_i \oplus x_i$$

Block Ciphers

- Examples of Block Ciphers in Practice:
  - DES (Data Encryption Standard)
    - proposed 1977, no longer secure
  - AES (Advanced Encryption Standard)
    - proposed 2002, now almost everywhere
    - Message: 128 bits; Key: 128, 196, <u>256</u> bits
      - E.g., AES-CBC-256
      - Each block is a PRP $\{0,1\}^{128}$ —> $\{0,1\}^{128}$

Block Ciphers

- AES (Advanced Encryption Standard)
  - Message: 128 bits; Key: 128, 196, <u>256</u> bits
  - E.g., AES-CBC-256
  - Each block is a PRP $\{0,1\}^{128}$ —> $\{0,1\}^{128}$

  - How many permutations in PRP, if key is 256-bit?
  - How many permutations in Perm(n,n), if n=128?
  - $|F|$ in PRP is 2^l and $|Perm(n,n)| = (2^n)!$
  - $l = 256$, $n = 128$, therefore, 2^{256} v.s $(2^{128})!$

Key Idea in AES

- Each block is a PRP $\{0,1\}^{128} \longrightarrow \{0,1\}^{128}$
  - Each block uses Substitution-Permutation Network
    - Multiple rounds of substitution (S-boxes) and permutation (P-boxes)

  - The number of rounds depends on key length
    - 128-bit: 10 rounds
    - 192-bit: 12 rounds
    - 256-bit: 14 rounds

Key Idea in AES

- Initialize State (4 by 4 array of bytes) with message
- In each round
  - AddKey: get a 128-bit sub-key, XOR with State
  - S-Box: substitute each byte in State
  - P-Box: shift bytes in State
  - MixColumns: invertible transformation on each column; replace with AddKey in the final round
  - Use current State for the next round input

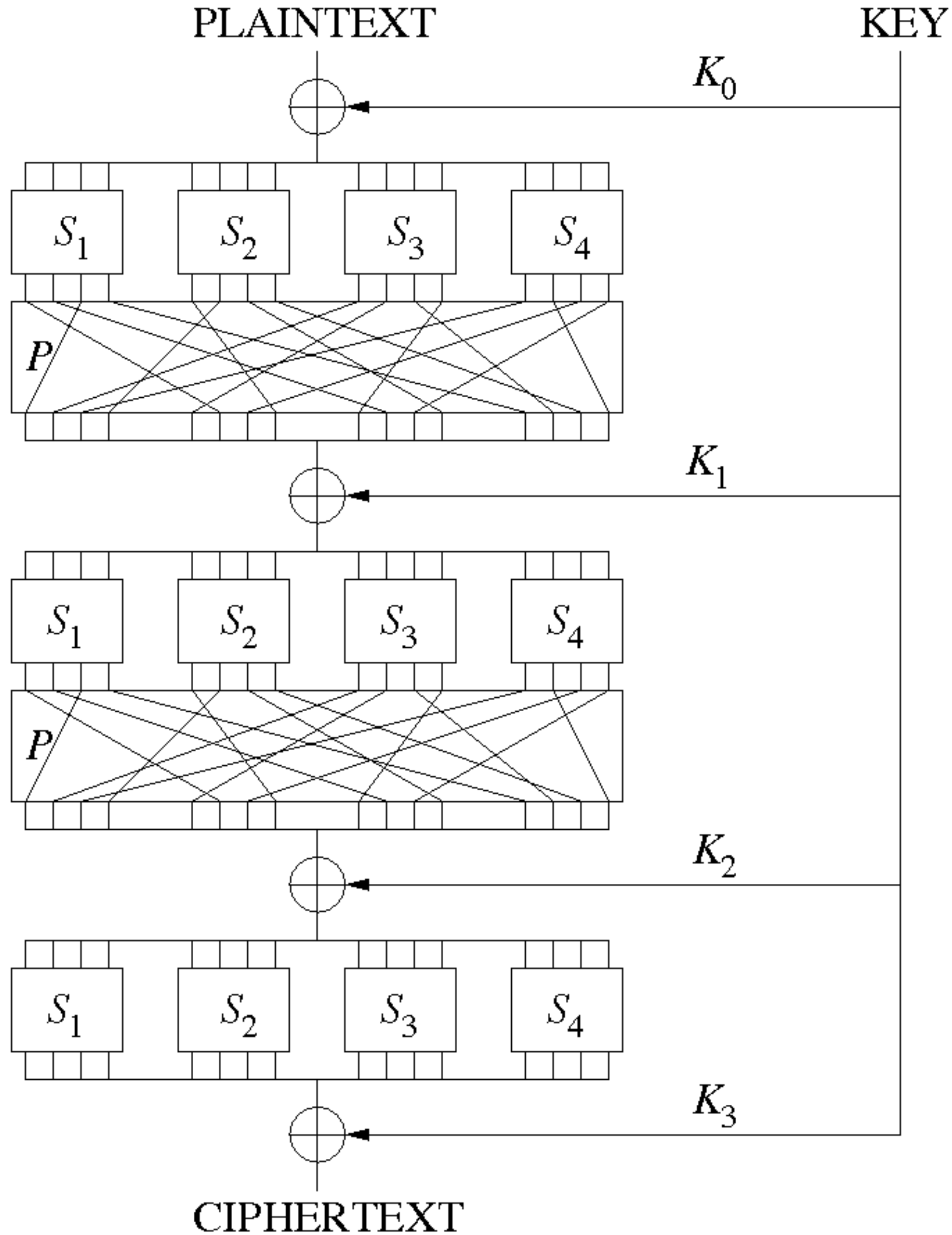
An example of SPN (Substitution-Permutation Network)

Input: 16 bits

3 rounds

This is a PRP

$\{0,1\}^{16} \longrightarrow \{0,1\}^{16}$



Roadmap for Encryption

- One-time Pad:
    - perfectly secure, impractical
- Fixed-length encryption (based on PRG)
    - deterministic, fixed-length messages only

- Fixed-length encryption (based on PRF)
    - probabilistic, fixed-length messages only
- Block Cipher
    - probabilistic, arbitrary-length messages

Additional Reading

Chapter 3 & 6, *Introduction to Modern Cryptography, Drs. J. Katz and Y. Lindell, 2nd edition*