More on Symmetric Cipher

Lecture 6

Hazem Said

Reference: Chapter 6,7 Cryptography and Network Security, William Stallings

Agenda

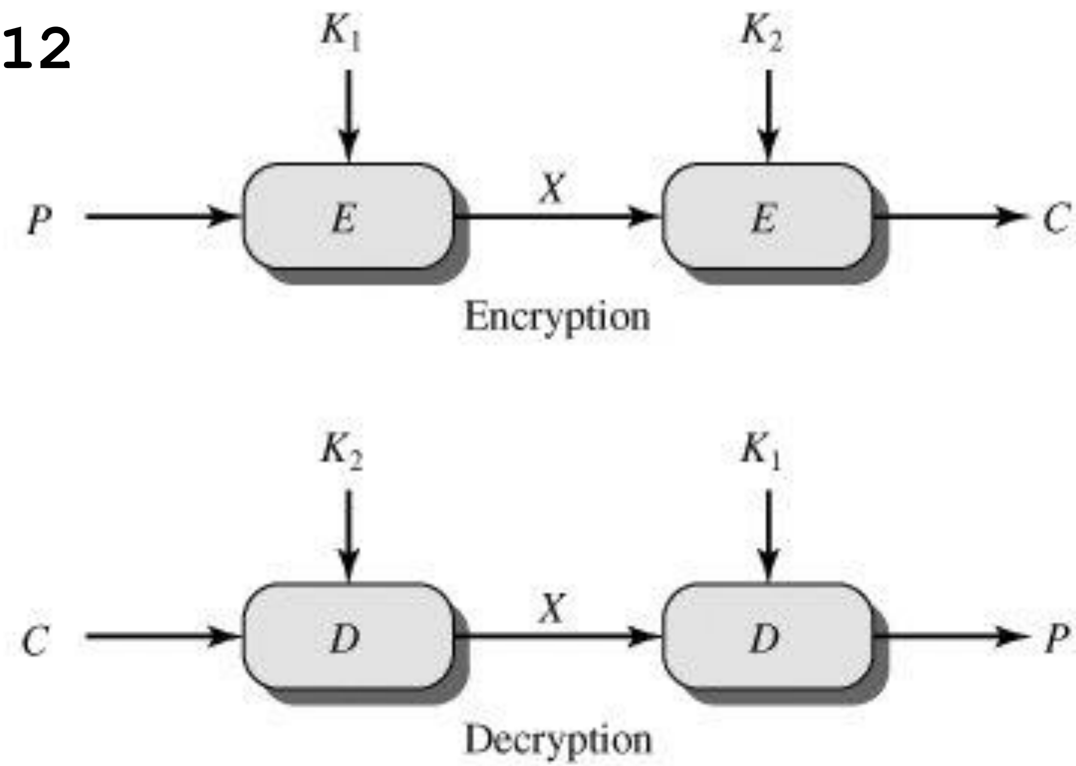
- Multiple Encryption and Triple DES
- Block Cipher Modes
- Other Topics

Multiple Encryption and Triple DES

Double DES

$$C = E(K_2, E(K_1, P)) \qquad\qquad P = D(K_1, D(K_2, C))$$

Key Size 112



(a) Double encryption

Double DES Brute force Attack

- For known plaintext attack with P and C
- Each P needs 2^{64} key alternatives to produce 2^{64} Unique C value.
- The reset $2^{(112-64)} = 2^{48}$ key alternatives will produce a redundant values.
- This means, more than one key map the same P and C. This will lead to false cryptanalysis results.

Double DES Brute force Attack

- Example, there is:
  - $C = E(K_2, E(K_1,P))$
  - $C = E(K_4, E(K_3,P))$
  - and more
  - If cryptanalyst find K_1, K_2 this does not mean that the key is found
- For pair $\{P_1,C_1\}$, $\{P_2,C_2\}$
- The number of false keys is reduced to
  - $2^{(112-2x64)} = 2^{-16}$.

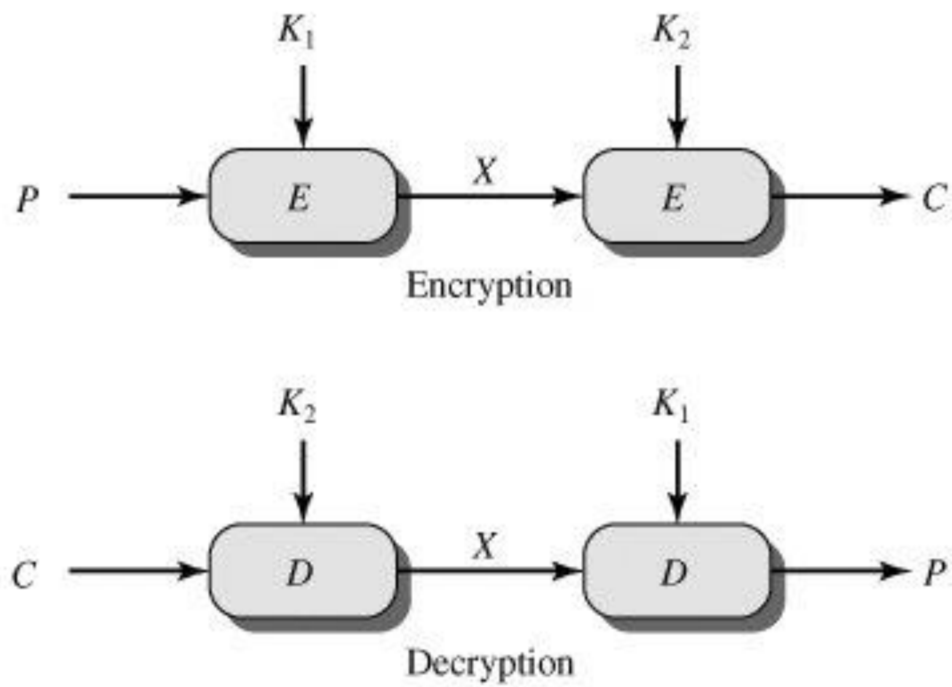
Double DES Brute force Attack

- What is the number of required pairs P,C to apply Brute force Attack?

- What is the complexity of Brute force Attack?

Double DES MIM Attack

- MIM stands for Meet In the Middle
- $X = E(K_1, P)$ also $X = D(K2, C)$



(a) Double encryption

Double DES MIM Attack

- Generate $E(K_1, P)$ for all K1 alternatives 2^{56}.
- Store the result in a Table.
- Try $X = D(K_2, C)$ for all K2 alternatives 2^{56}.
- Search for X in the table.
- Repeat again for another pairs P`, C`.

- Why repeat?
- What is the complexity of MIM Attack?

Double DES MIM Attack

$X = E(K_1, P)$

K1	X

$X = D(K_2, C)$

X	K2

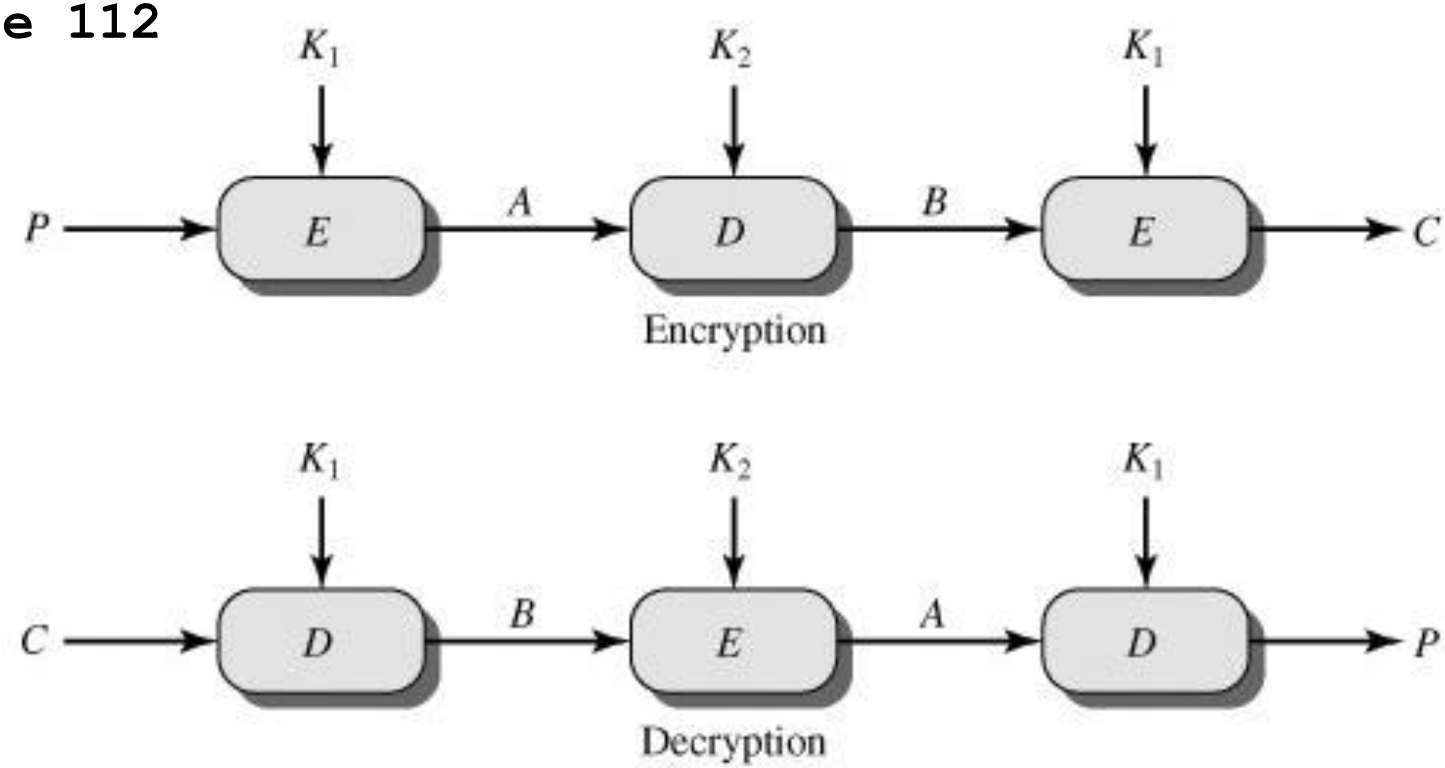
- What is the required storage?

Tipple DES with Two Keys

$$C = E(K_1, D(K_2, E(K_1, P)))$$

$$P = D(K_1, E(K_2, D(K_1, C)))$$

Key Size 112



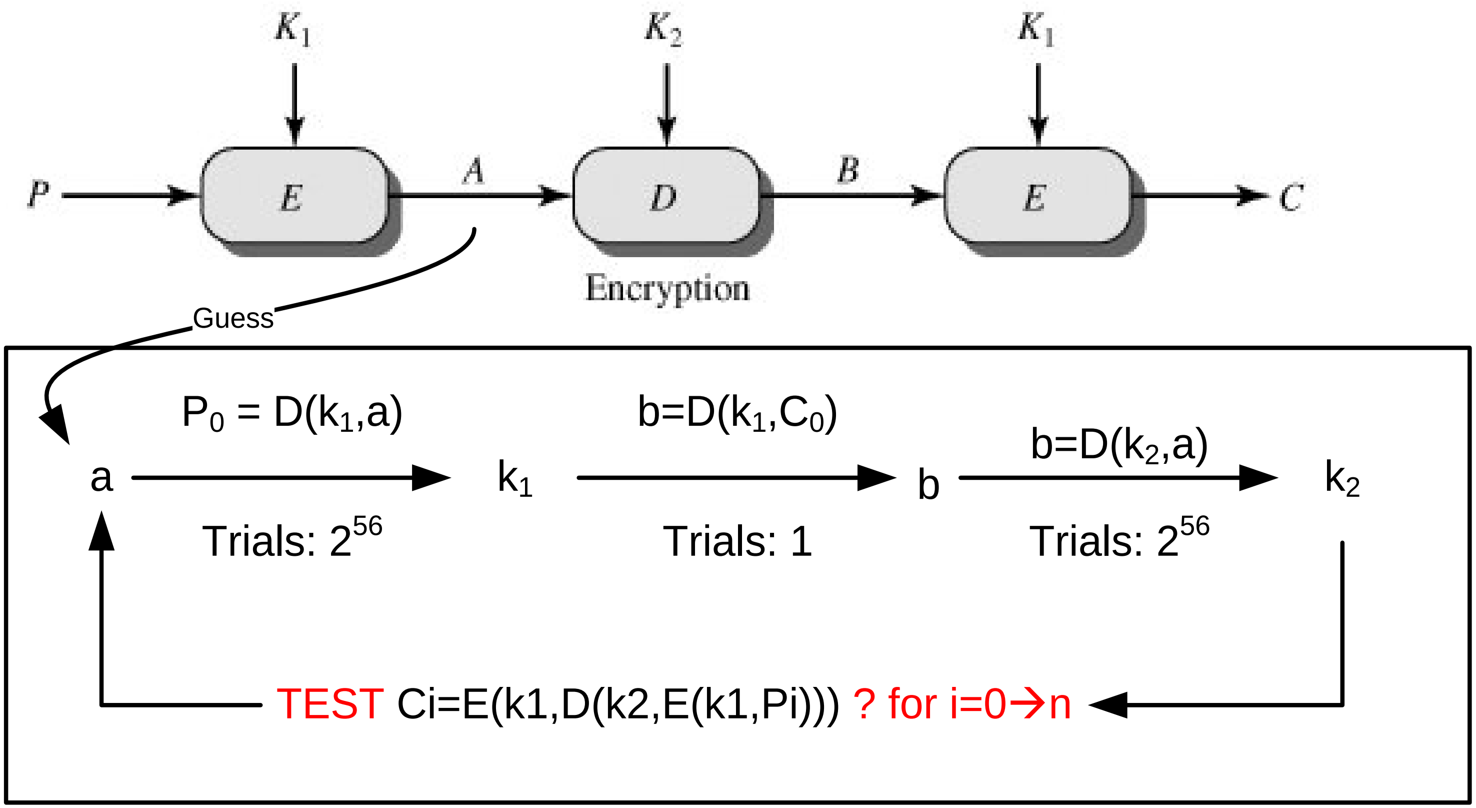
(b) Triple encryption

Single DES if K_1=K_2

Triple DES with Two Keys MIM Attack

Known Plain Text Pairs

	P	C
0		
n		



Trials: 2^{64}

What is the complexity of this Attack?

Tipple DES with Three Keys

$$C = E\left(K_3, D\left(K_2, E\left(K_1, P\right)\right)\right) \qquad P = D\left(K_1, E\left(K_2, D\left(K_3, C\right)\right)\right)$$

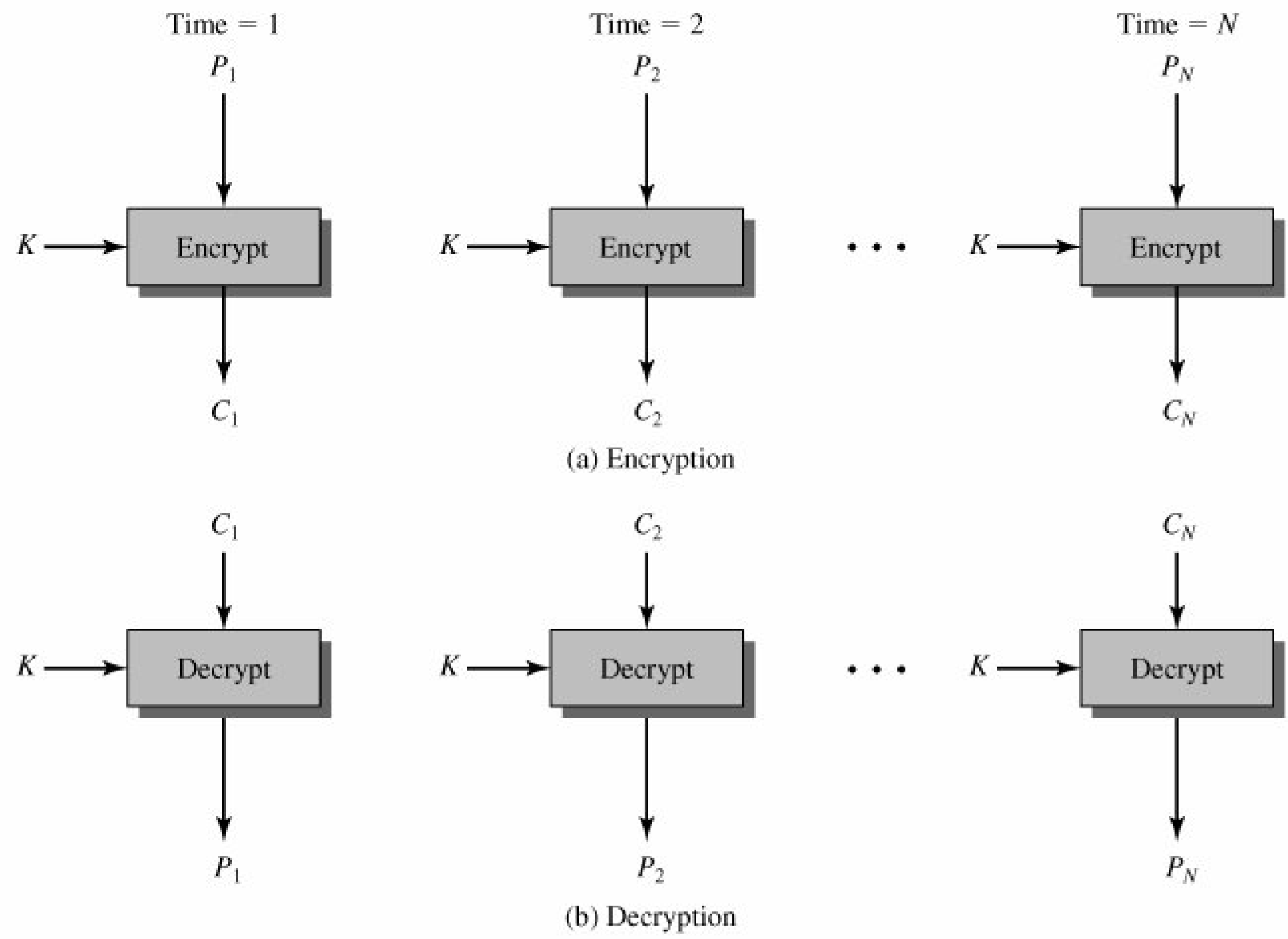
Key Size 168

Single DES if K_1=K_2 or K_2=K_3

Block Cipher Modes

ECB, CBC, CFB, OFB, CTR

ECB: Electronic Code Book Mode



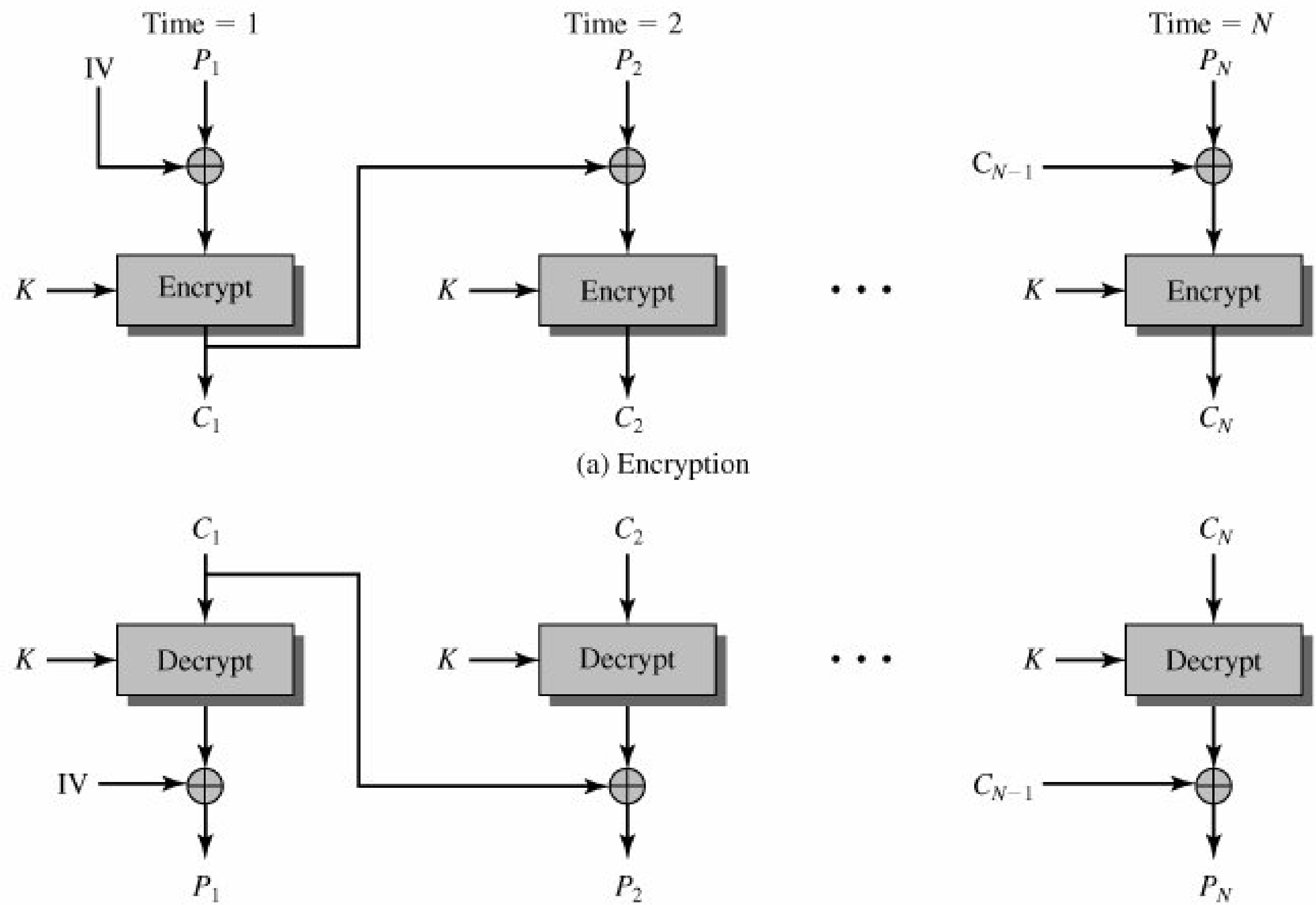
(a) Encryption

(b) Decryption

ECB

- Normal Block Encryption
- Not recommended for:
  - Structured data with repeated sections, Why?
- Recommended for:
  - Small data
  - Keys whiles secure key exchange
  - Single values (numeric, string, single structures)

CBC: Cipher Block Chaining Mode



(a) Encryption

(b) Decryption

CBC

- Recommended for long data

$$C_j = E\left(K, \left[C_{j-1} \oplus P_j\right]\right) \qquad (1)$$

$$P_j = D\left(K, C_j\right) \oplus C_{j-1} \qquad (2)$$

$$\text{where } C_0 = IV$$

Proof

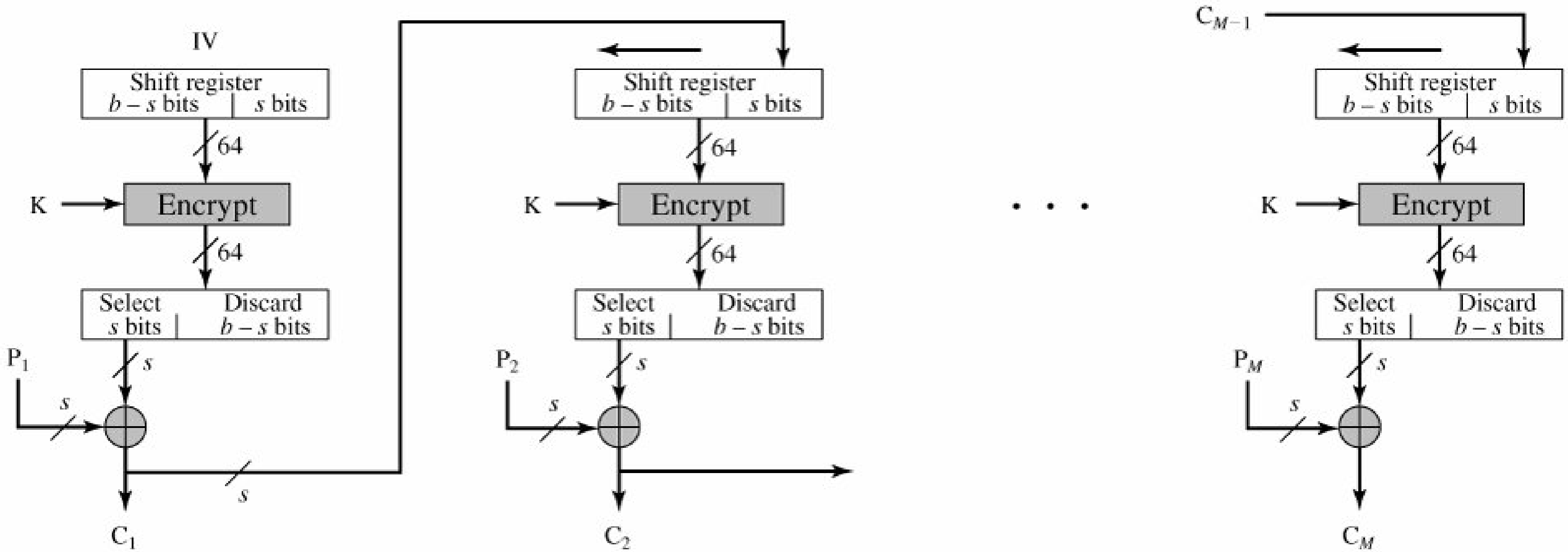
$$P_j = D\left(K, C_j\right) \oplus C_{j-1}$$

$$P_j = D\left(K, E\left(K, \left[C_{j-1} \oplus P_j\right]\right)\right) \oplus C_{j-1}$$

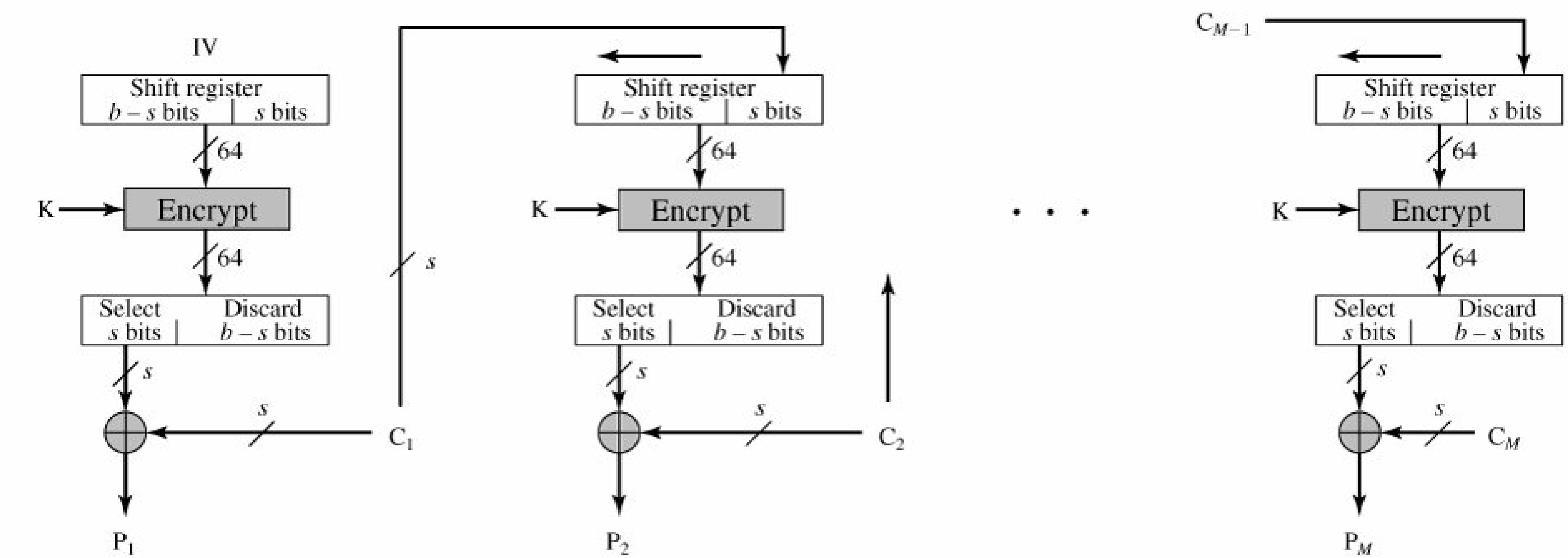
$$P_j = C_{j-1} \oplus P_j \oplus C_{j-1} = P_j$$

CFB: Cipher Feedback Mode

- Stream Cipher applied to s Bits



(a) Encryption



(b) Decryption

CFB

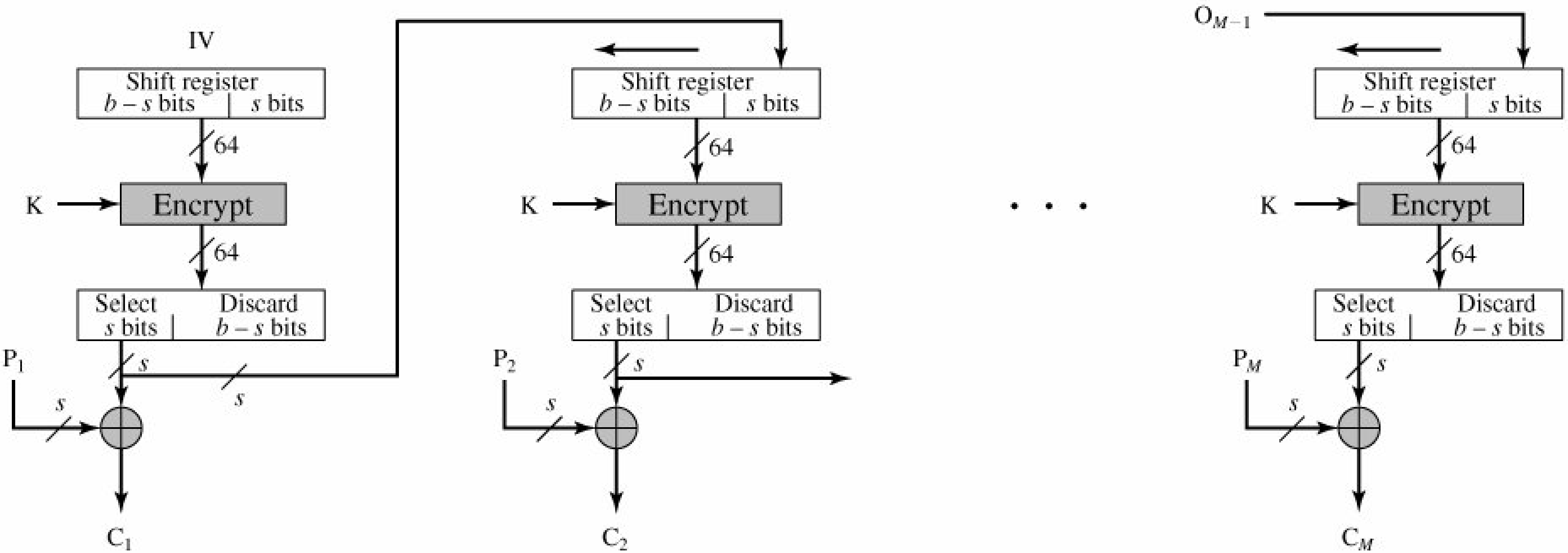
- Let $S_s(X)$ return the most significant x bits
- Let $Shl_s(X)$ return the x shifted to left s bits

$$C_j = P_j \oplus S_s\left(E\left(K, IV_{j-1}\right)\right)$$
$$P_j = C_j \oplus S_s\left(E\left(K, IV_{j-1}\right)\right)$$
$$\text{where } IV_0 = IV \qquad IV_j = \left[Shl_s\left(IV_{j-1}\right) \quad C_j\right]$$

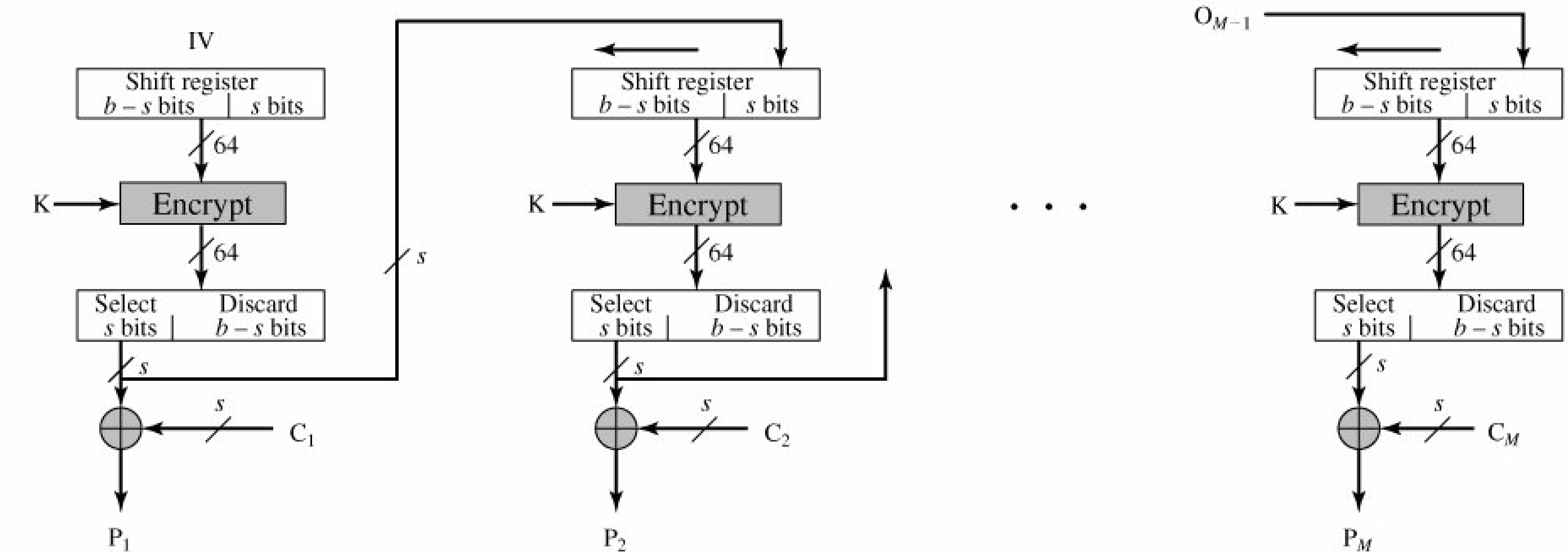
- Problem:
  – Transmission error lead to false construction

OFB: Output Feedback Mode

- Stream Cipher applied to b Bits
- Resolve error propagation while transmission



(a) Encryption

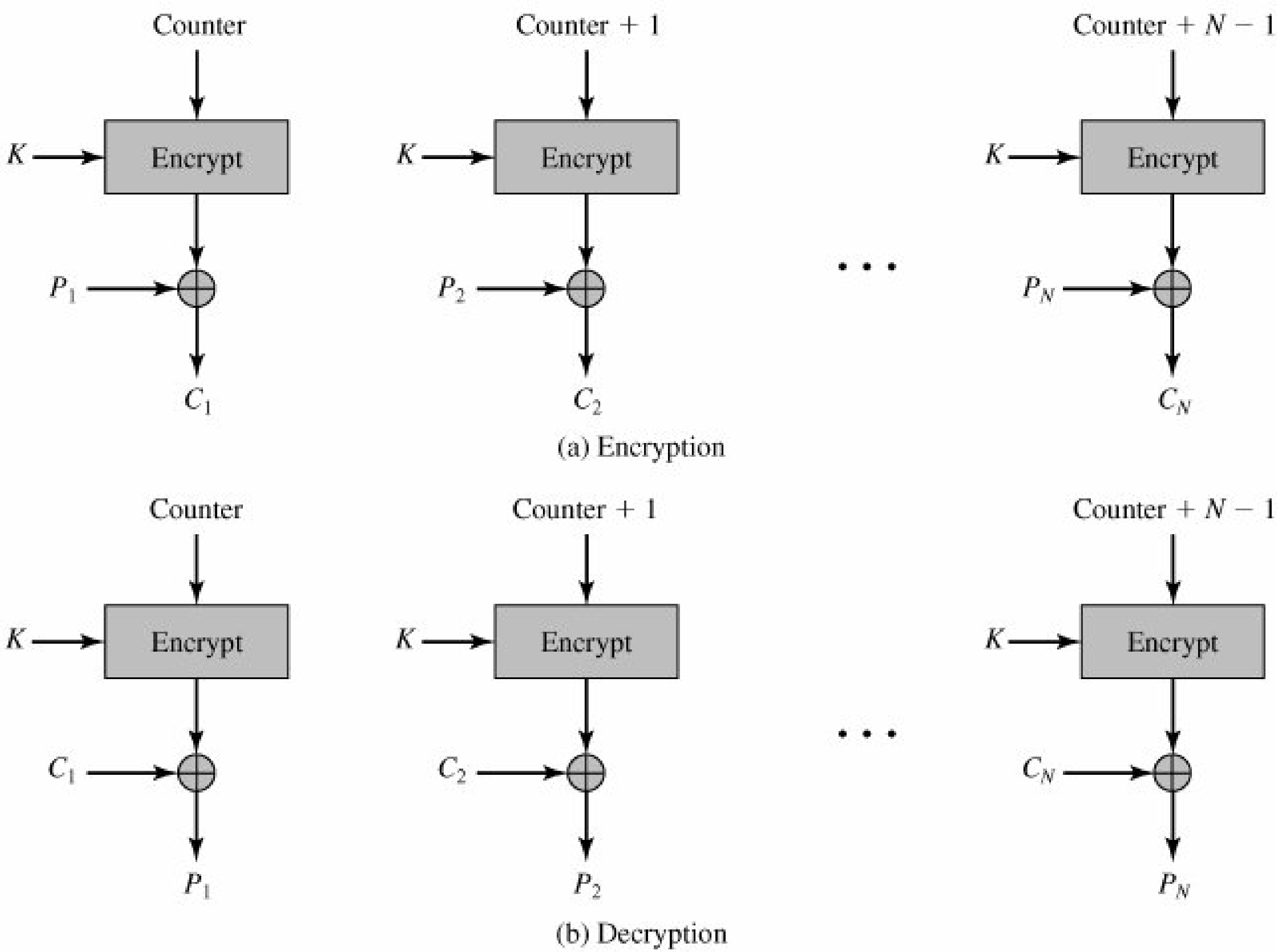


(b) Decryption

CFB vs.. OFB

- Which is more reliable?
- Which is more secure?

CTR: Counter Mode



CTR

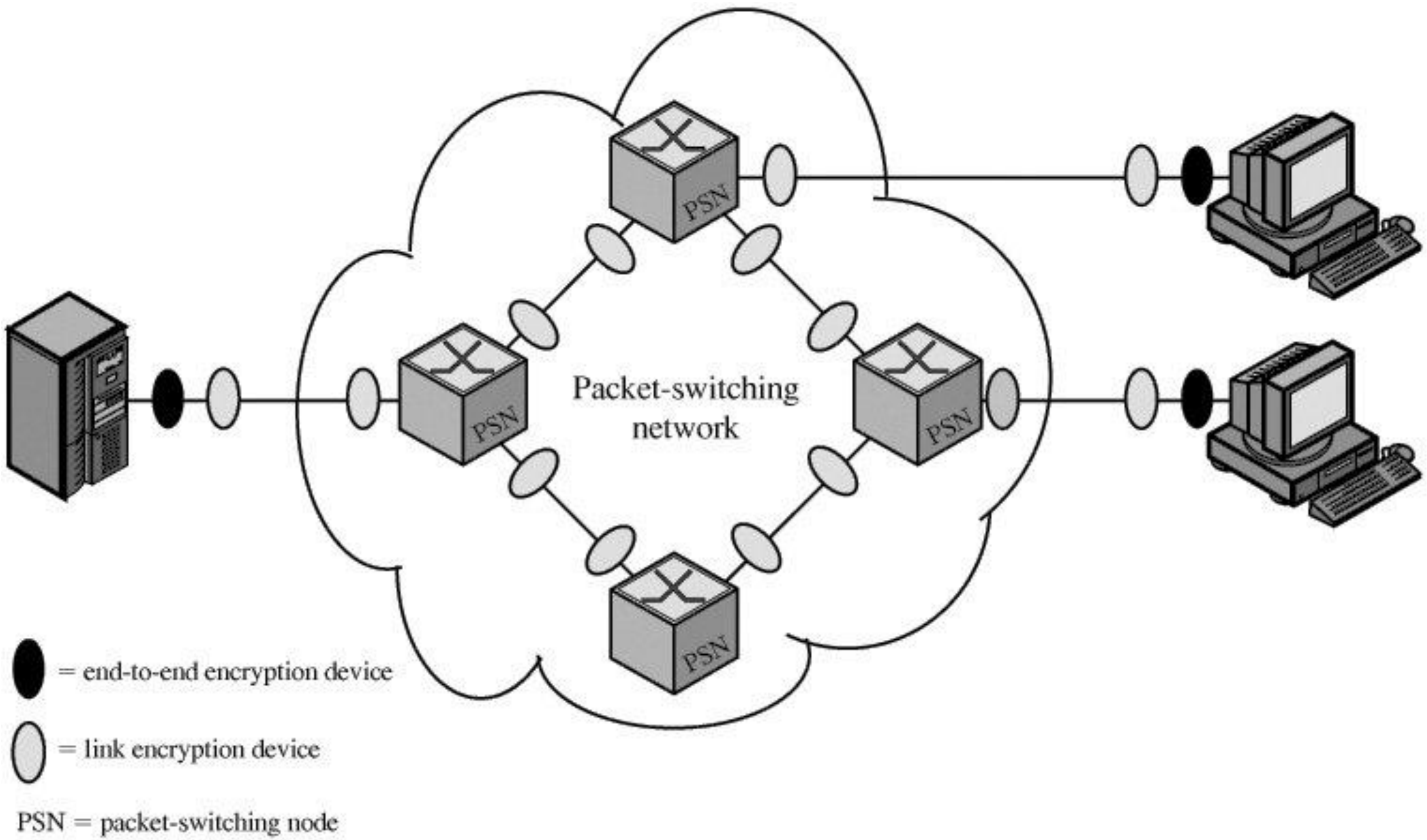
- Suitable for long data without error propagation
- No need for decryption
- Allow Parallel SW/HW Implementation
- Allow Preprocessing, Why?
- Allow Random Access
- Can be used for Blocks or Streams

Other Topics

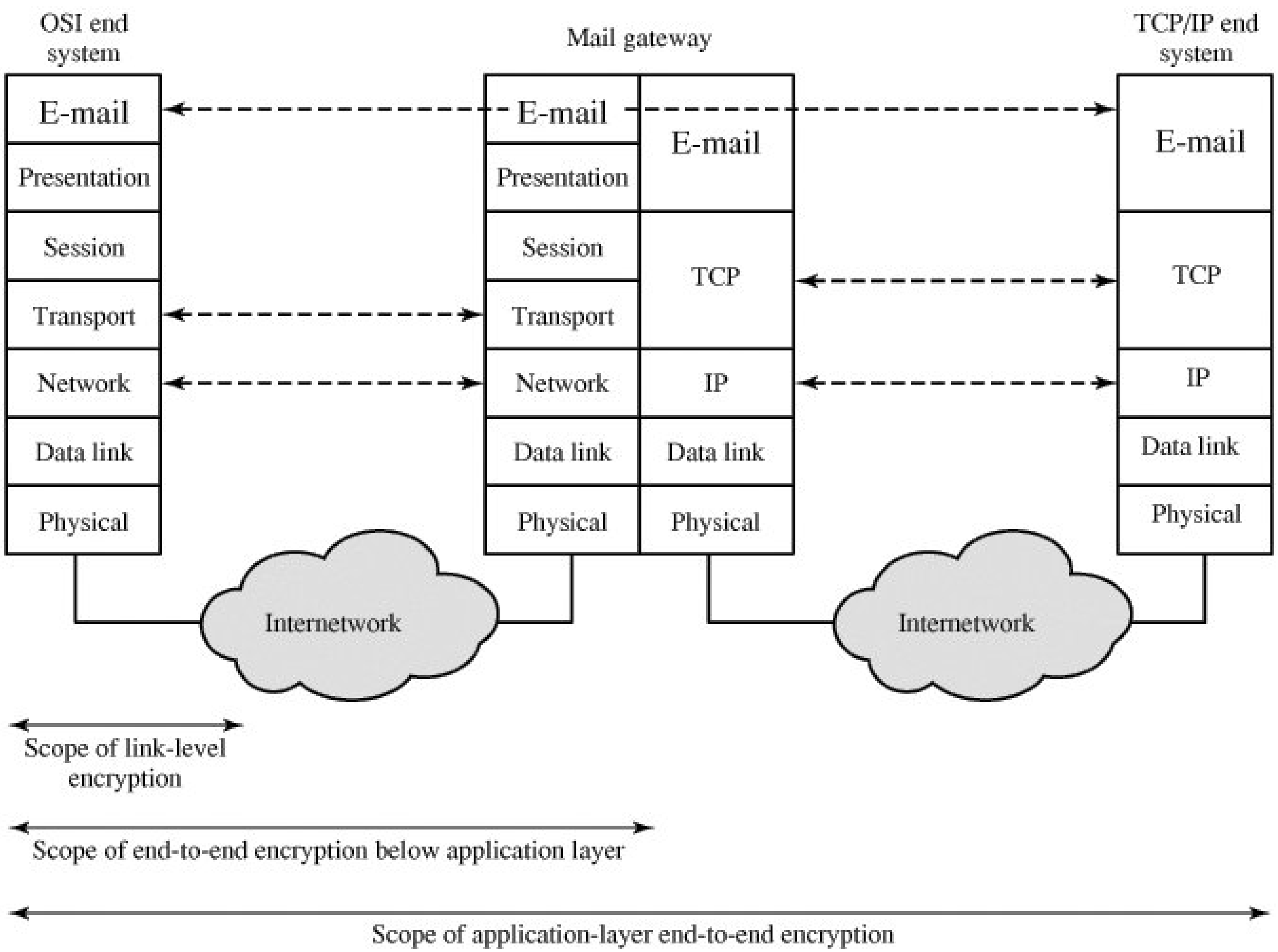
Where to Apply the Encryption

- When an application communicate with another application, example email system
- Email software send Email contents using TCP/IP protocol
- TCP/IP divide email contents into packets and add some headers for each
- Network card create network packet and add some hearers for each

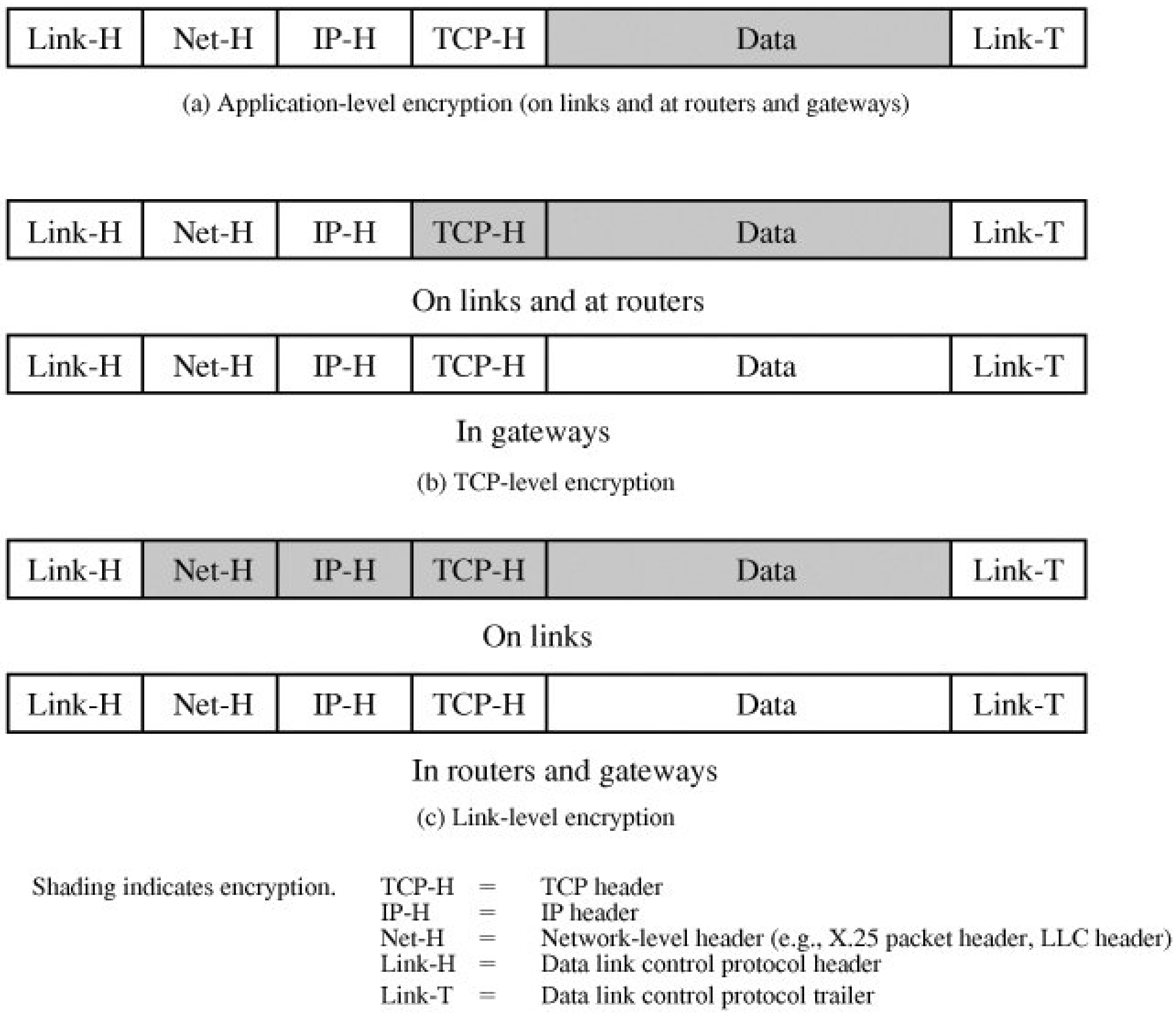
Where to Apply the Encryption



Where to Apply the Encryption



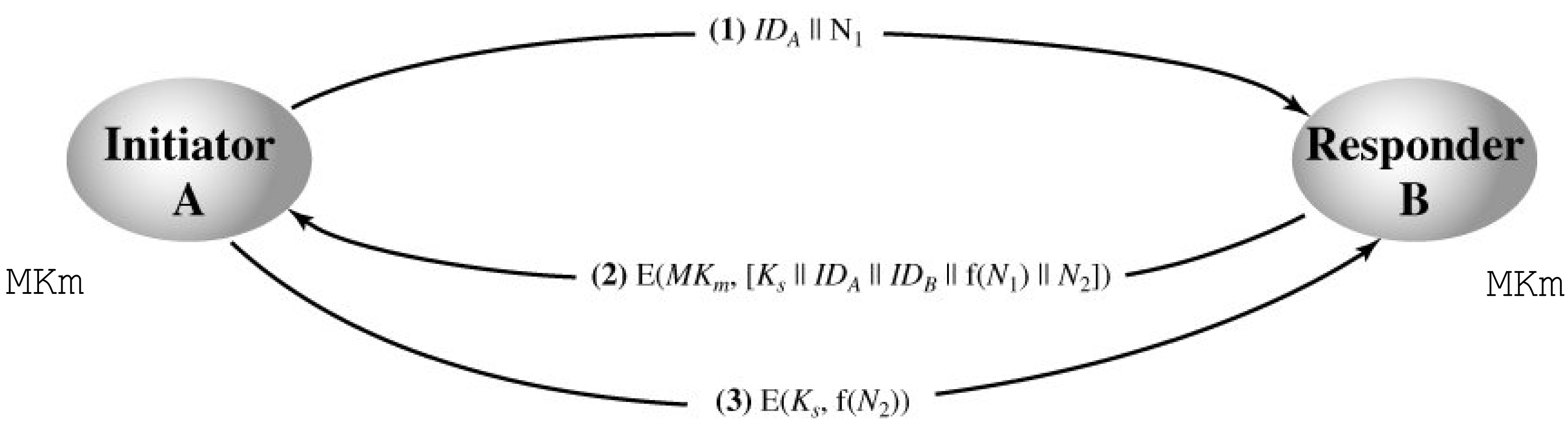
Where to Apply the Encryption



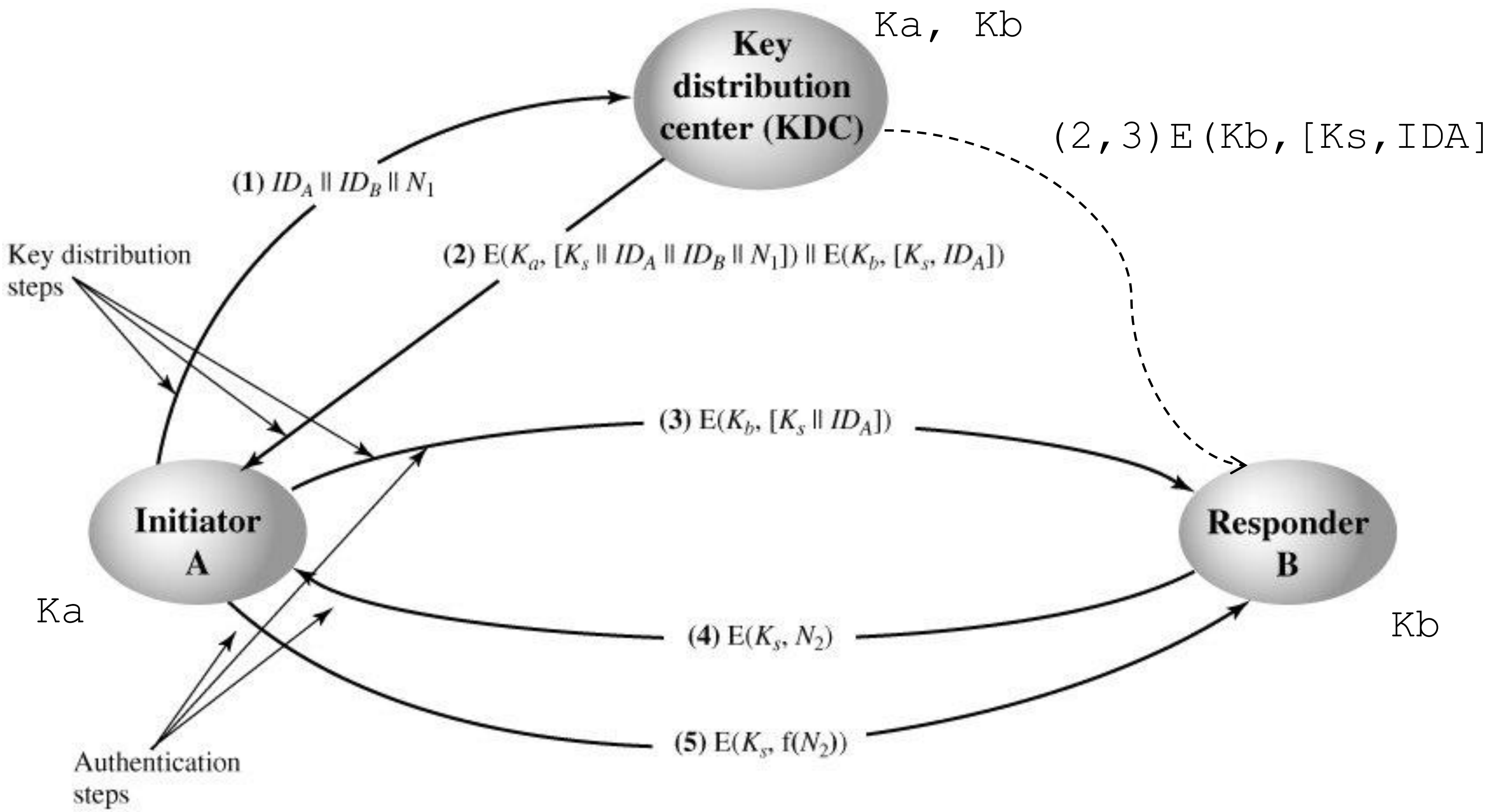
Key Distribution

- How to distribute the key to A and B
  - A generate a key then physically deliver it to B
  - Third party generate a key then physically deliver it to A and B
  - Using old key A and B can exchange the new key encrypted with old key
  - A and B has encrypted link with C, C can deliver the key to A and B

Decentralized Key Distribution



Centralized Key Distribution



Next Step

Next Step

- Key distribution is not safe
- For Decentralized Solution
  - Keys are distributed using previously shared keys
  - Shared keys is unsecure
- For Centralized Solution
  - Keys are distributed using KDC who use shared keys
  - Shared keys is unsecure
  - KDC is un-trusted

Next Step

- We need
- A can send the key to B without using any shared keys
- B must be the only one who can retrieve the key
- B can make sure that A is the sender of the key