UNIT-II

Fundamentals
Block ciphers

Prepared By:
Asst.Prof. Hiral Shastri

Outline

- Multiple encryption and triple DES
- Electronic Code Book Mode
- Cipher Block Chaining Mode
- Cipher Feedback Mode
- Output Feedback Mode
- Counter Mode

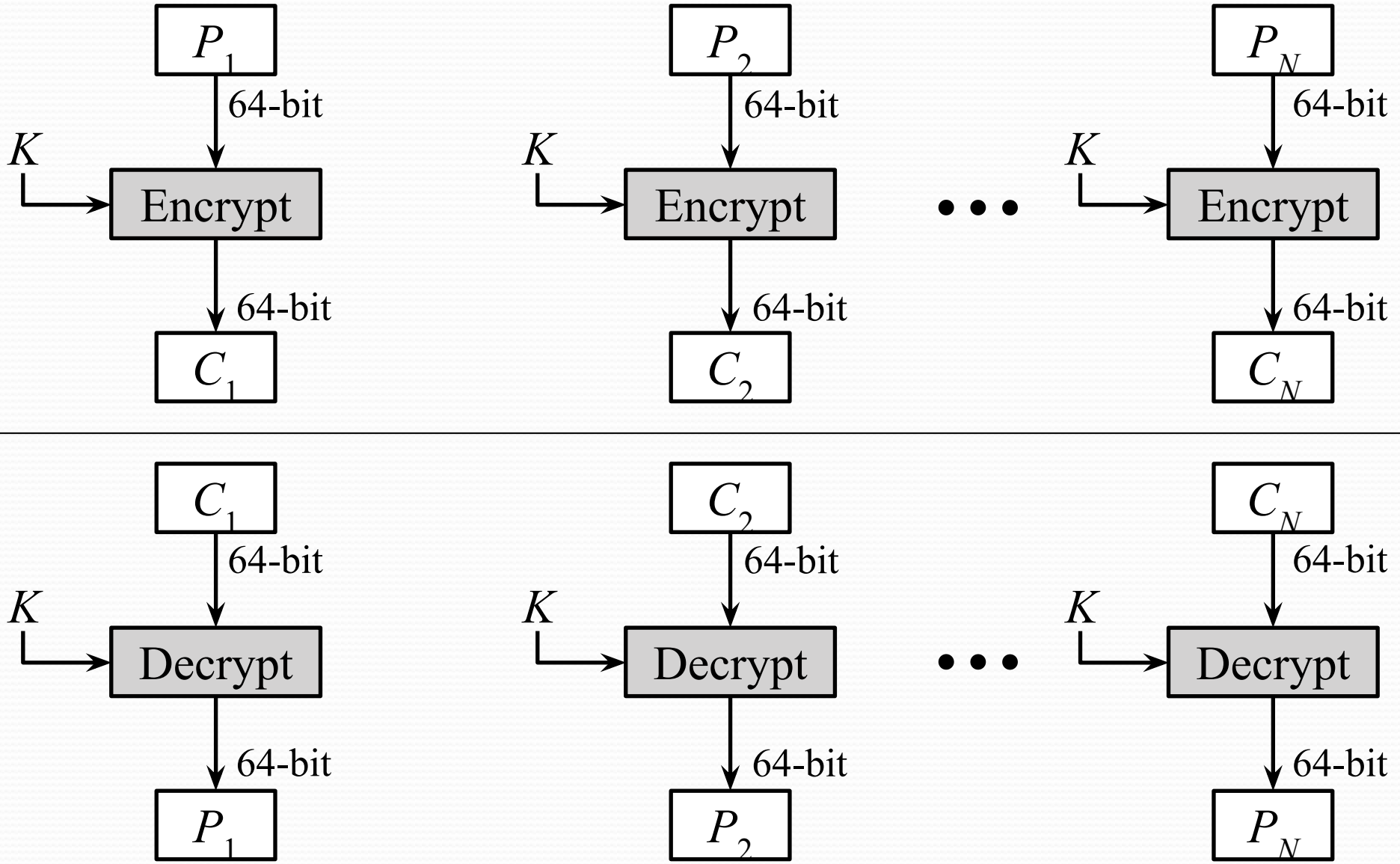
Block Cipher Modes of Operations

- To apply a block cipher in a variety of applications, five "modes of operation" have been defined.
  1. Electronic Code Book (ECB)
  2. Cipher Block Chaining (CBC)
  3. Cipher Feedback (CFB)
  4. Output Feedback (OFB)
  5. Counter (CTR)
- The five modes are intended to cover a wide variety of applications of encryption for which a block cipher could be used.
- These modes are intended for use with any symmetric block cipher, including triple DES and AES.

Block Cipher Modes of Operations

- **Block cipher:** operates on fixed length b-bit input to produce b-bit ciphertext.
- What about encrypting plaintext longer than b bits?
- Break plaintext into b-bit blocks (padding if necessary) and apply cipher on each block.

1. ECB Encryption & Decryption



Electronic Code Book (ECB) (cont....)

- In ECB Mode Plaintext handled one block at a time and each block of plaintext is encrypted using the same key.
- The term codebook is used because, for a given key, there is a unique ciphertext for every b-bit block of plaintext.

$$C_j = E(K, P_j) \qquad j = 1, .., N$$

$$P_j = D(K, C_j) \qquad j = 1, .., N$$

Electronic Code Book (ECB) (cont…)

- **ECB Advantages:**
  - No block synchronization between sender and receiver is required.
    - OK if some blocks are lost in transit.
  - Bit errors caused by noisy channels only affect the corresponding block but not succeeding blocks.
  - Block cipher operating can be parallelized.

Electronic Code Book (ECB) (cont....)

- **ECB Disadvantages:**
  - Identical plaintexts result in identical cipher texts.
  - An attacker recognizes if the same message has been sent twice simply by looking at the ciphertext.
  - Plaintext blocks are encrypted independently of previous blocks.
    - An attacker may reorder ciphertext blocks which results in valid plaintext.

Substitution Attack on ECB

- Consider an electronic bank transfer

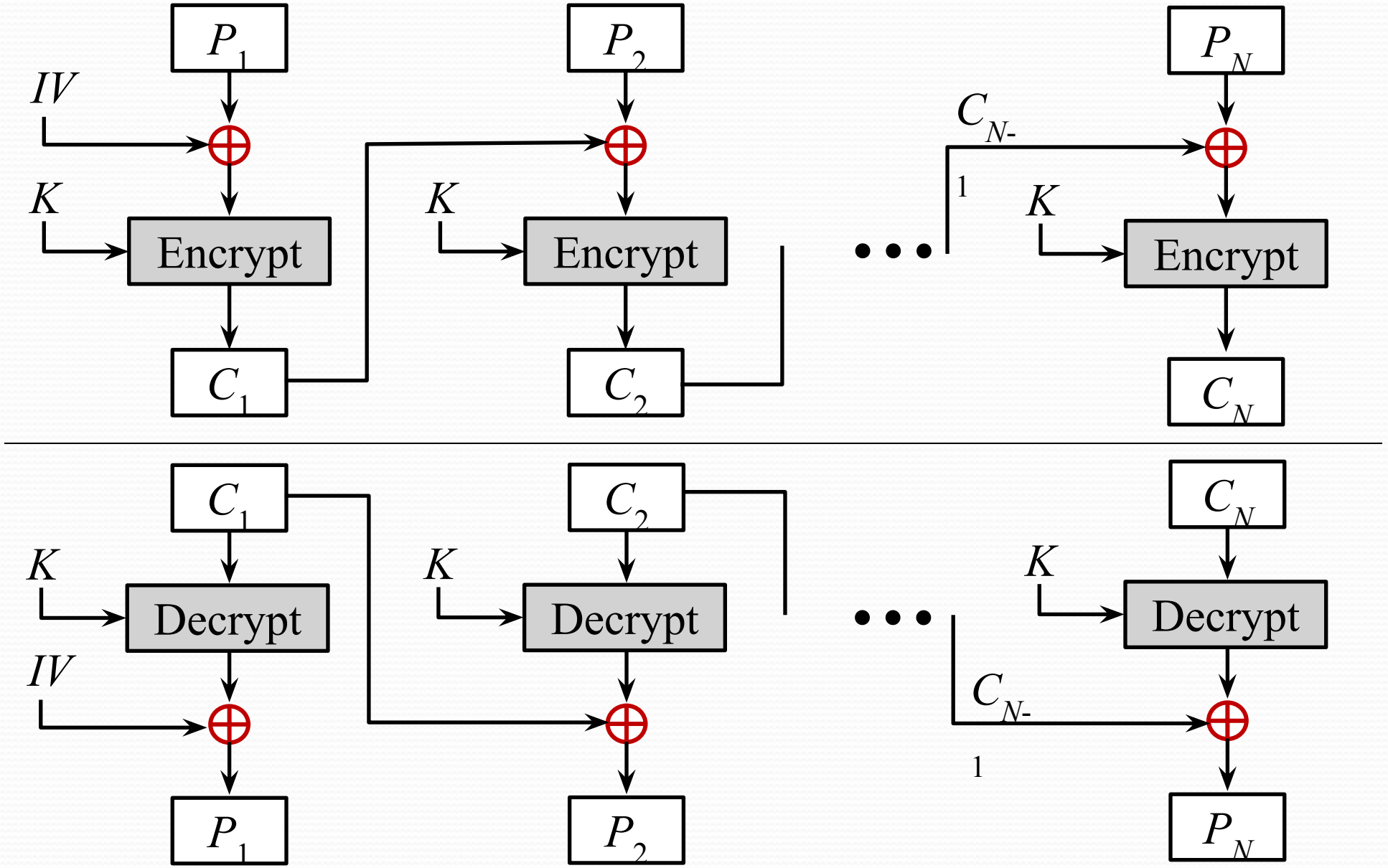
1	2	3	4	5
Sending Bank A	Sending Account #	Receiving Bank B	Receiving Account #	Amount $

- The attacker sends $1.00 transfers from his account at bank A to his account at bank B repeatedly.
- He can check for ciphertext blocks that repeat, and he stores blocks 1,3 and 4 of these transfers.
- He now simply replaces block 4 of other transfers with the block 4 that he stored before.
- All transfers from some account of bank A to some account of bank B are redirected to go into the attacker's B account.

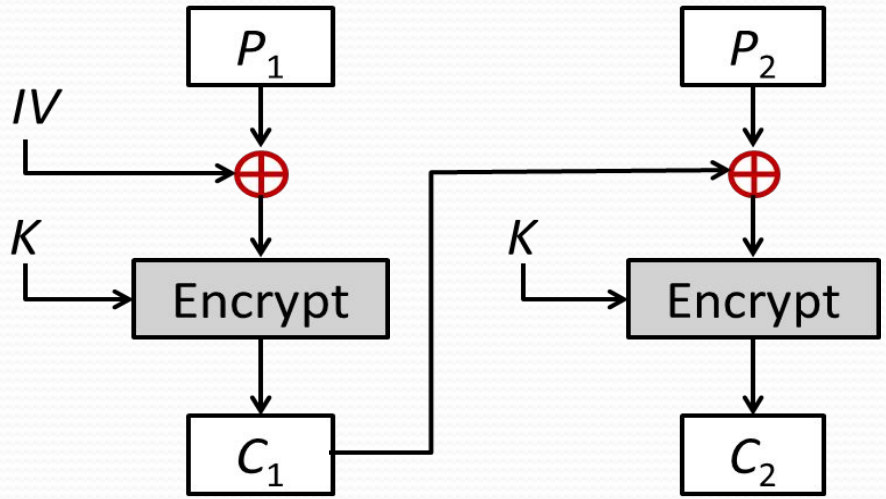
Electronic Code Book (cont.…)

- **Strength:** it's simple.
- **Weakness:**
  - Problem: with long message, repetition in plaintext may cause repetition in ciphertext.
- **Typical application:**
  - Secure transmission of short pieces of information (e.g. a temporary encryption key).

2. CBC - Encryption & Decryption

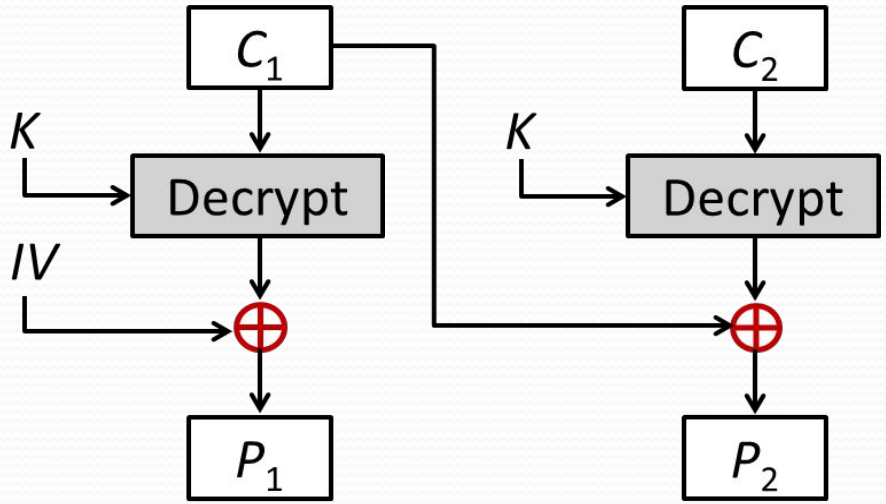


Cipher Block Chaining (CBC) (cont…)



$$C_1 = E(K, (P_1 \oplus IV)$$

$$C_j = E(K, (P_j \oplus C_{j-1})$$
$$j = 2, .., N$$



$$P_1 = D(K, C_1) \oplus IV$$

$$P_j = E(K, (C_j) \oplus C_{j-1}$$
$$j = 2, .., N$$

Cipher Block Chaining (CBC) (cont...)

- CBC is a technique in which the same plaintext block, if repeated, produces different ciphertext blocks.
- In this scheme, the input to the encryption algorithm is the XOR of the current plaintext block and the preceding ciphertext block and the same key is used for each block.
- To produce the first block of ciphertext, an initialization vector (IV) is XORed with the first block of plaintext.

Cipher Block Chaining (CBC) (cont....)

- Initialisation Vector (IV) must be known by sender/receiver, but it should be kept secret from attacker.
- On decryption, the IV is XORed with the output of the decryption algorithm to recover the first block of plaintext.

Substitution Attack on CBC

- Consider the last example (electronic bank transfer).
- If the IV is properly chosen for every wire transfer, the attack will not work at all.
- If the IV is kept the same for several transfers, the attacker would recognize the transfers from his account at bank A to back B.

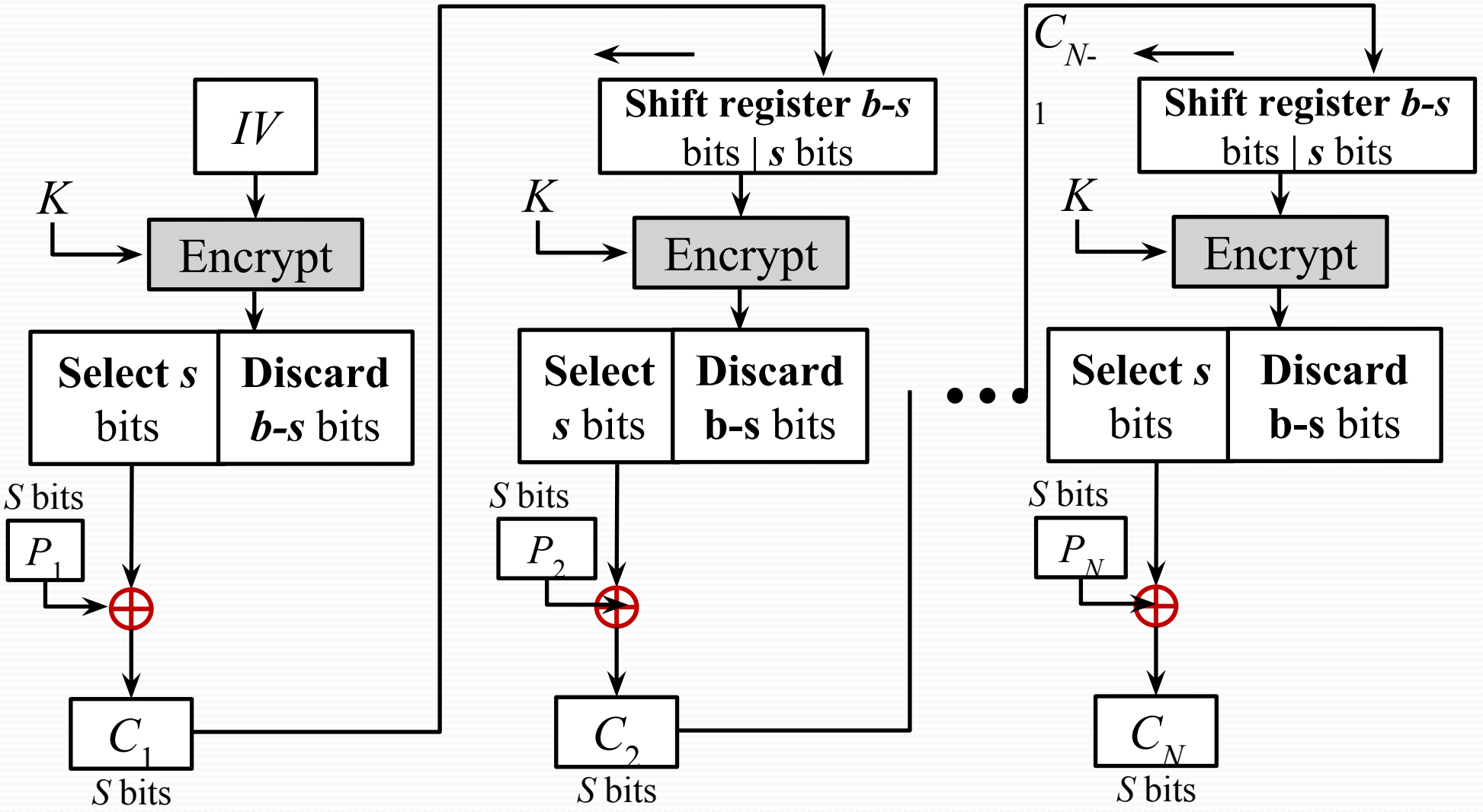
Cipher Block Chaining (CBC) (cont....)

- **Strength:** because of the chaining mechanism of CBC, it is an appropriate mode for encrypting messages of length greater than b bits.
- **Typical application:**
  - General-purpose block oriented transmission
  - Authentication

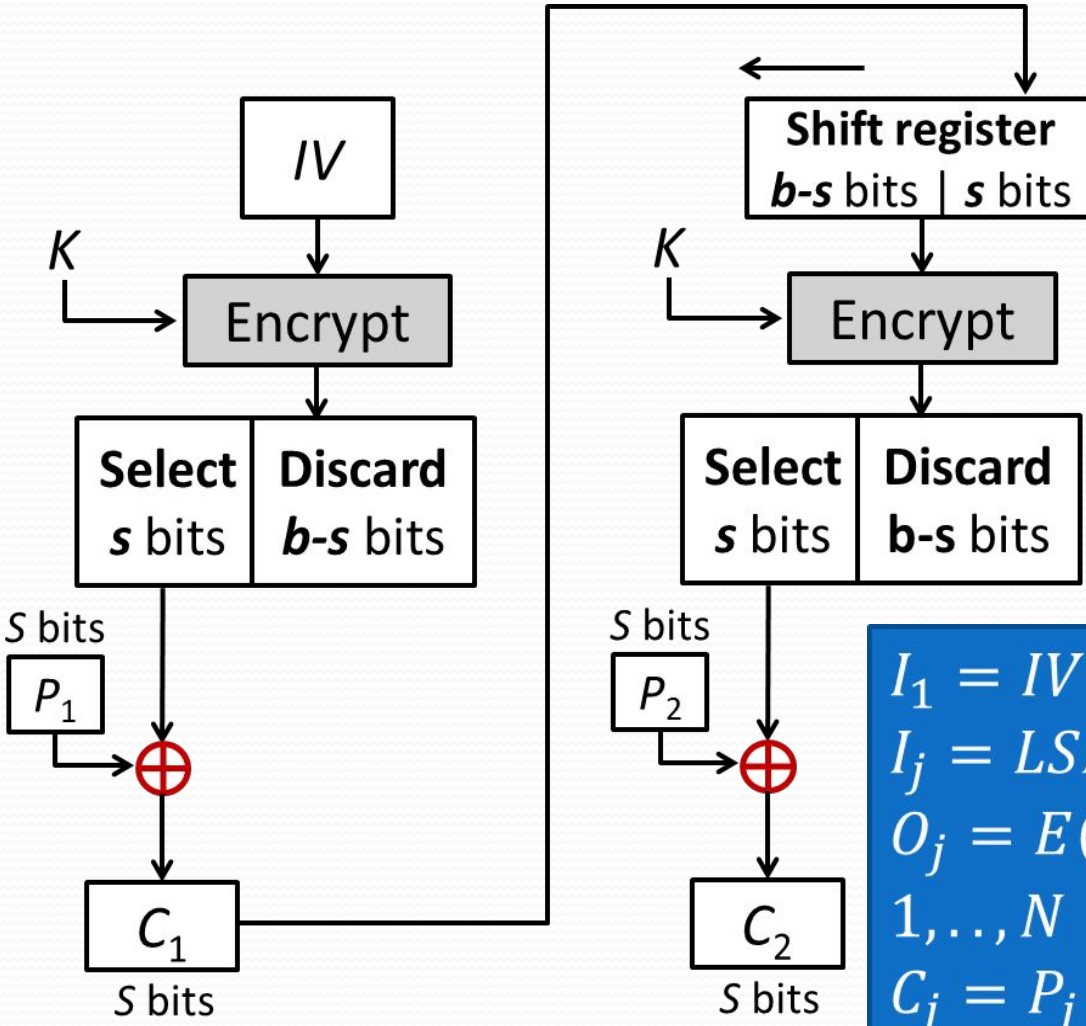
3. Cipher Feedback Mode (CFB)

- For AES, DES, or any block cipher, encryption is performed on a block of b bits. In DES, b = 64 and in AES, b = 128.
- However, it is possible to convert a block cipher into a stream cipher, using cipher feedback (CFB) mode, output feedback (OFB) mode, and counter (CTR) mode.
- A stream cipher eliminates the need to pad a message to be an integral number of blocks.

CFB Encryption

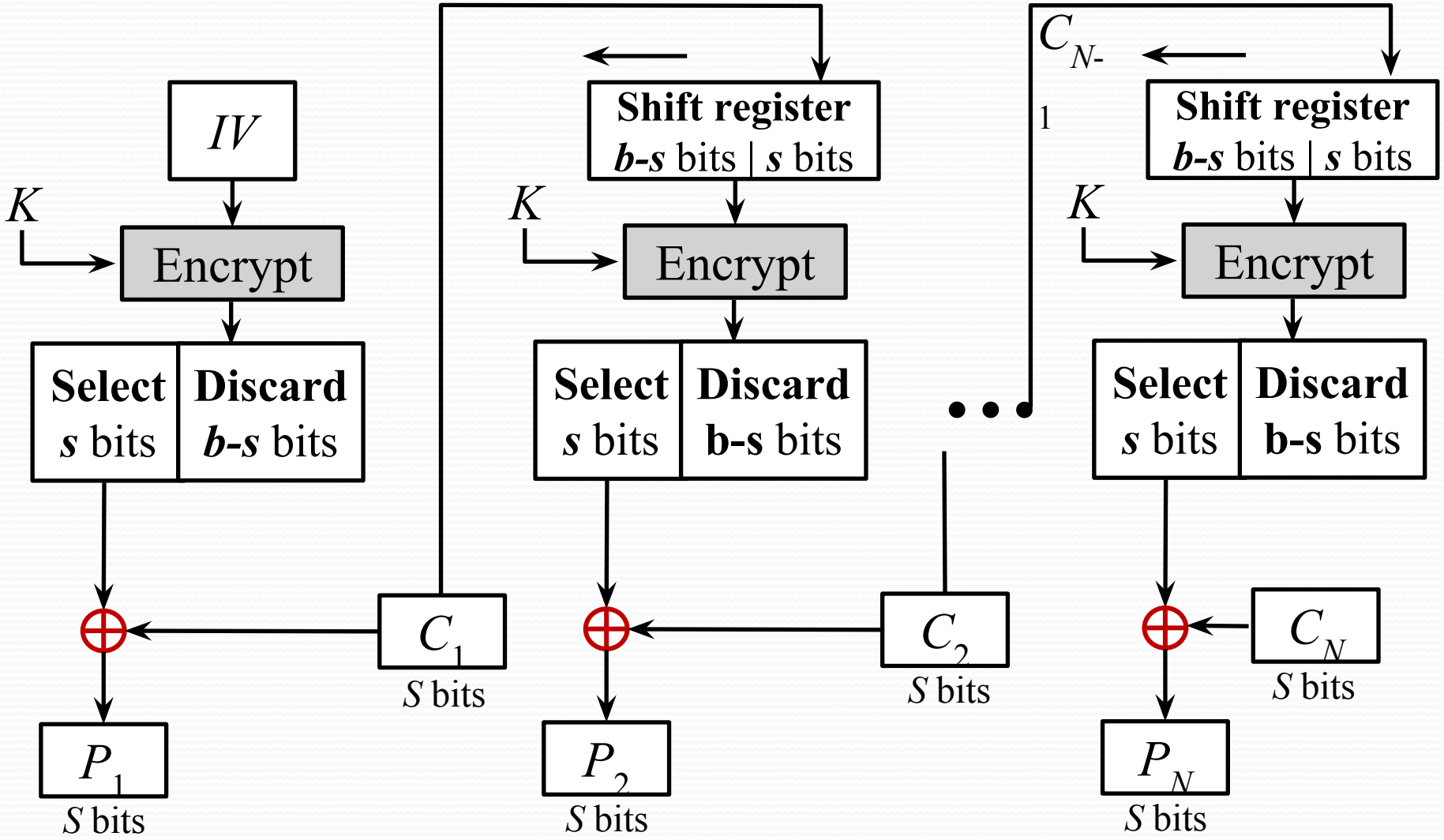


CFB Encryption (cont…)



$$I_1 = IV$$
$$I_j = LSB_{b-s}(I_{j-1}) || C_{j-1} \quad j = 2, .., N$$
$$O_j = E(K, I_j) \quad j = 1, .., N$$
$$C_j = P_j \oplus MSB_s(O_j) \quad j = 1, .., N$$

CFB Decryption



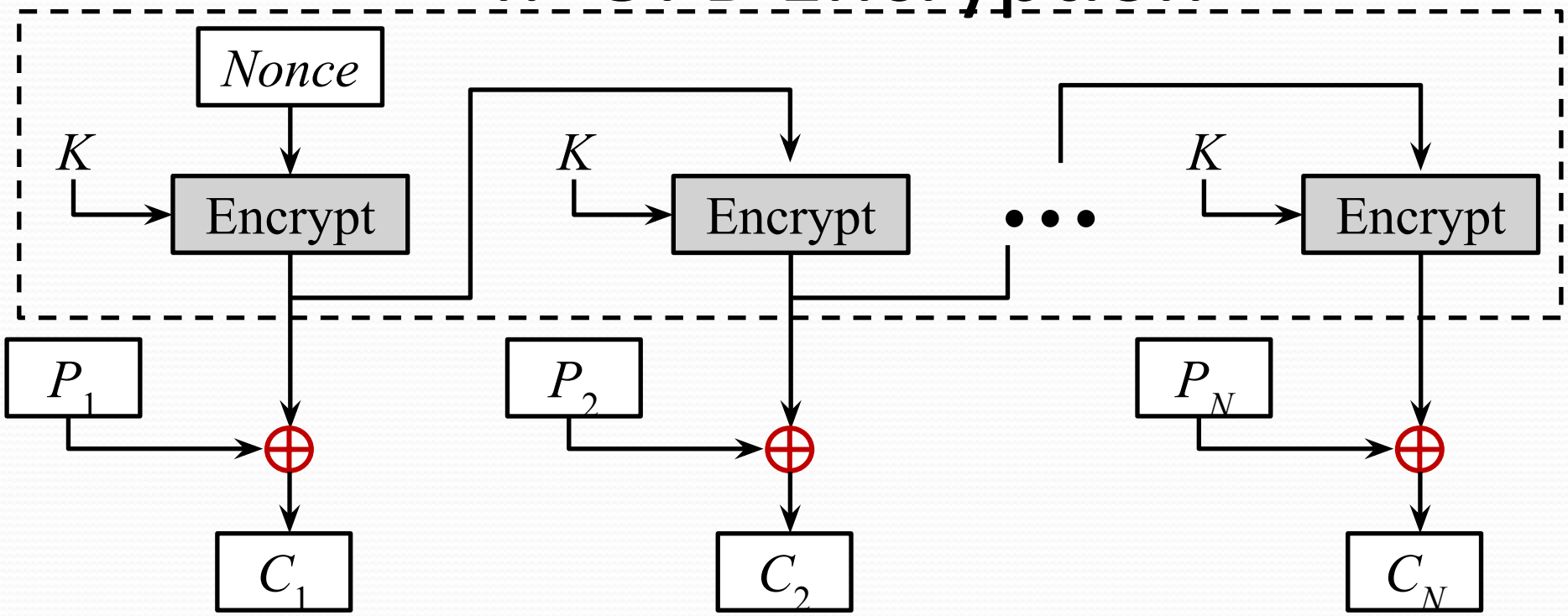
CFB Decryption (Cont…)

$$I_1 = IV$$
$$I_j = LSB_{b-s}\,(I_{j-1}) || C_{j-1} \qquad j = 2,..,N$$
$$O_j = E(K, I_j) \qquad j = 1,..,N$$
$$P_j = C_j \oplus MSB_s(O_j) \qquad j = 1,..,N$$

Cipher Feedback Mode (CFB) (cont….)

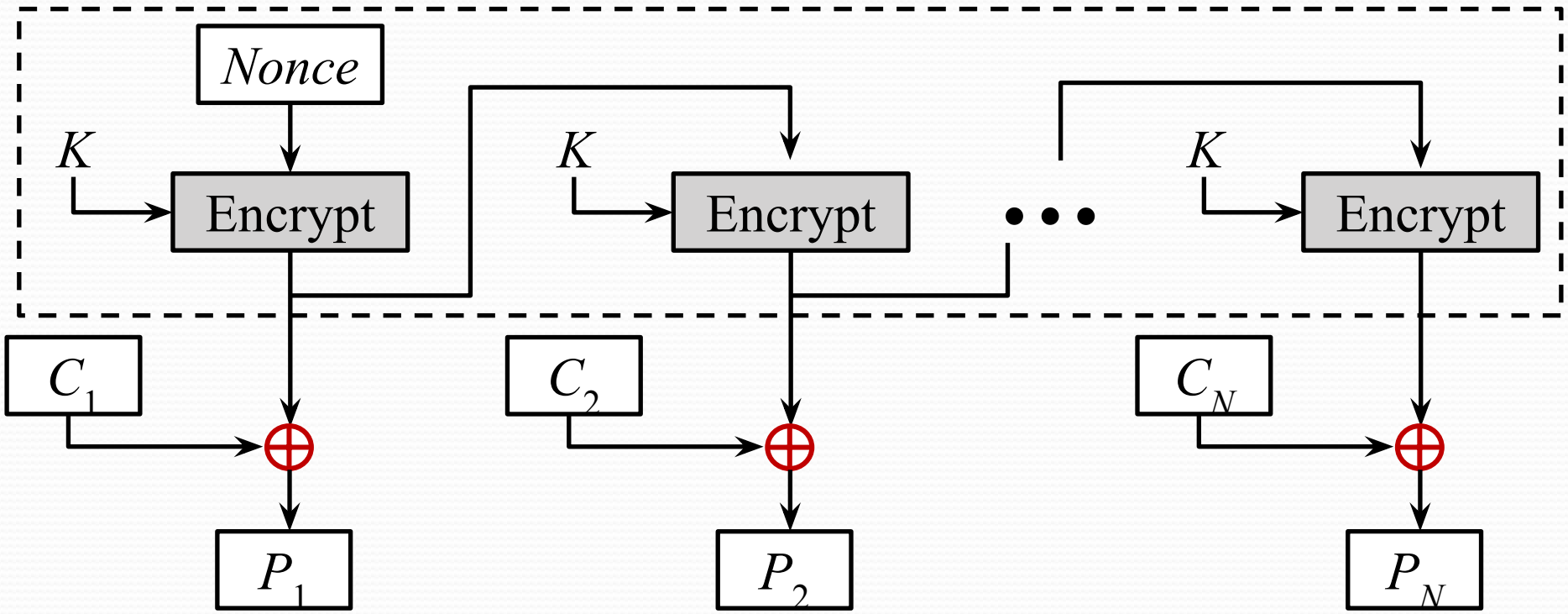
- The input to the encryption function is a b-bit shift register that is initially set to some initialization vector (IV).
- The leftmost (most significant) s bits of the output of the encryption function are XORed with the first segment of plaintext P1 to produce the first unit of ciphertext C1 , which is then transmitted.
- In addition, the contents of the shift register are shifted left by s bits, and C1 is placed in the rightmost (least significant) s bits of the shift register.
- For decryption, the same scheme is used, except that the received ciphertext unit is XORed with the output of the encryption function to produce the plaintext unit.

4. OFB Encryption



$$I_1 = Nonce$$
$$I_j = O_{j-1} \qquad j = 2,..,N$$
$$O_j = E(K, I_j) \qquad j = 1,..,N$$
$$C_j = P_j \oplus O_j \qquad j = 1,..,N-1$$

OFB Decryption



$$I_1 = Nonce$$
$$I_j = O_{j-1} \qquad j = 2,..,N$$
$$O_j = E(K, I_j) \qquad j = 1,..,N$$
$$P_j = C_j \oplus O_j \qquad j = 1,..,N-1$$

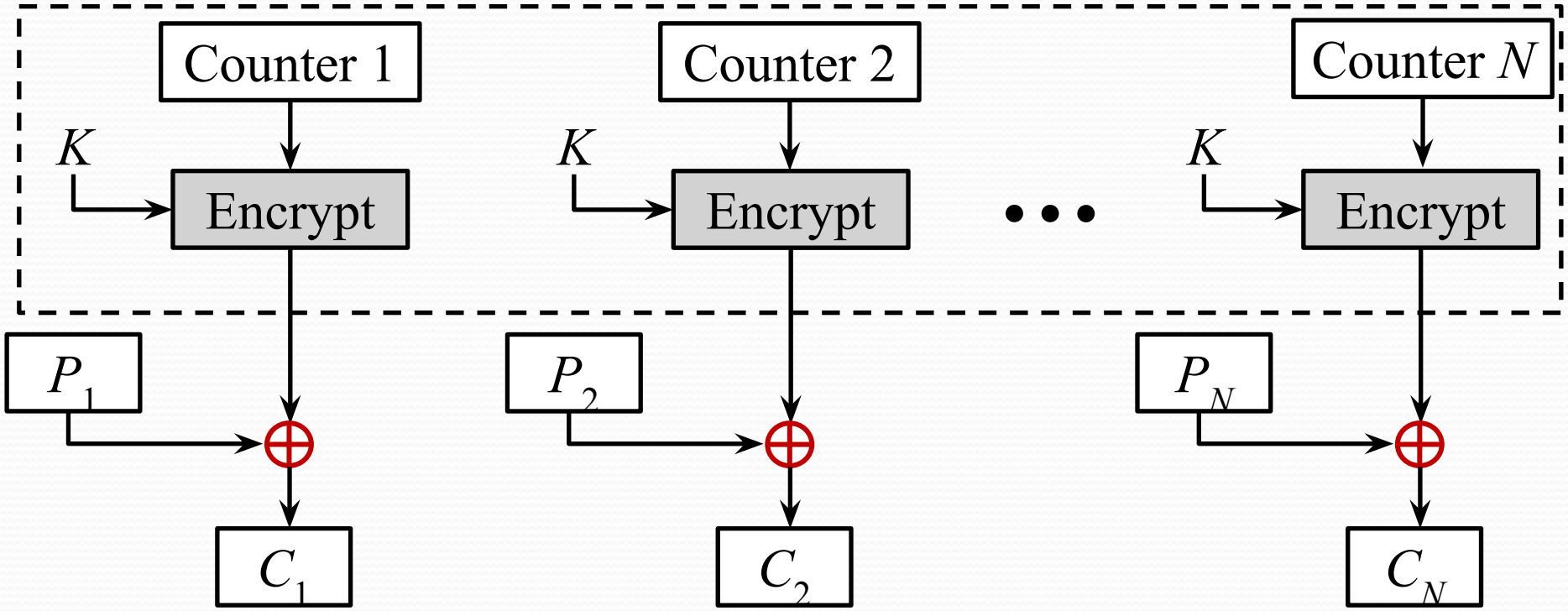
Output Feedback Mode(OFB) (cont..)

- The output feedback (OFB) mode is similar in structure to that of CFB.
- For OFB, the output of the encryption function is fed back to become the input for encrypting the next block of plaintext.
- In CFB, the output of the XOR unit is fed back to become input for encrypting the next block.
- The other difference is that the OFB mode operates on full blocks of plaintext and ciphertext, whereas CFB operates on an s-bit subset.

OFB Mode (cont..)

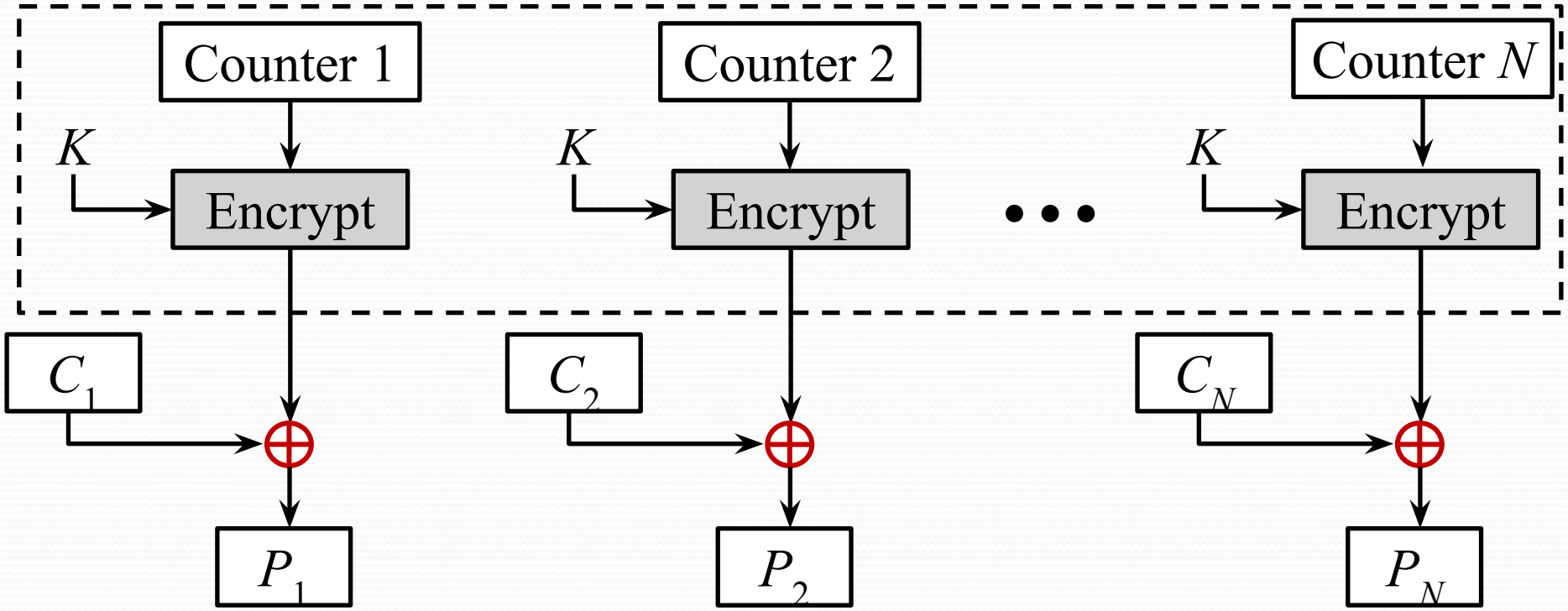
- **Nonce:** A time-varying value that has at most a negligible chance of repeating, for example, a random value that is generated anew for each use, a timestamp, a sequence number, or some combination of these.
- Each bit in the ciphertext is independent of the previous bit or bits.
- This avoids error propagation.
- Pre-compute of forward cipher is possible.

5. CTR Encryption



$$C_j = P_j \oplus E(K, T_j) \qquad j = 1, .., N$$

CTR Decryption



$$P_j = C_j \oplus E(K, T_j) \qquad j = 1, .., N$$

Counter Mode (CTR) (cont.…)

- Counter (CTR) mode has increased recently with applications to ATM (asynchronous transfer mode) network security and IP sec (IP security).
- A counter equal to the plaintext block size is used.
- The counter value must be different for each plaintext block that is encrypted.
- Typically, the counter is initialized to some value and then incremented by 1 for each subsequent block.

Advantages of the CTR Mode

- **Strengths:**
  - Needs only the encryption algorithm.
  - Random access to encrypted data blocks.
  - blocks can be processed (encrypted or decrypted) in parallel.
  - Simple and fast encryption/decryption.
- **Counter must be**
  - Must be unknown and unpredictable.
  - pseudo-randomness in the key stream is a goal.

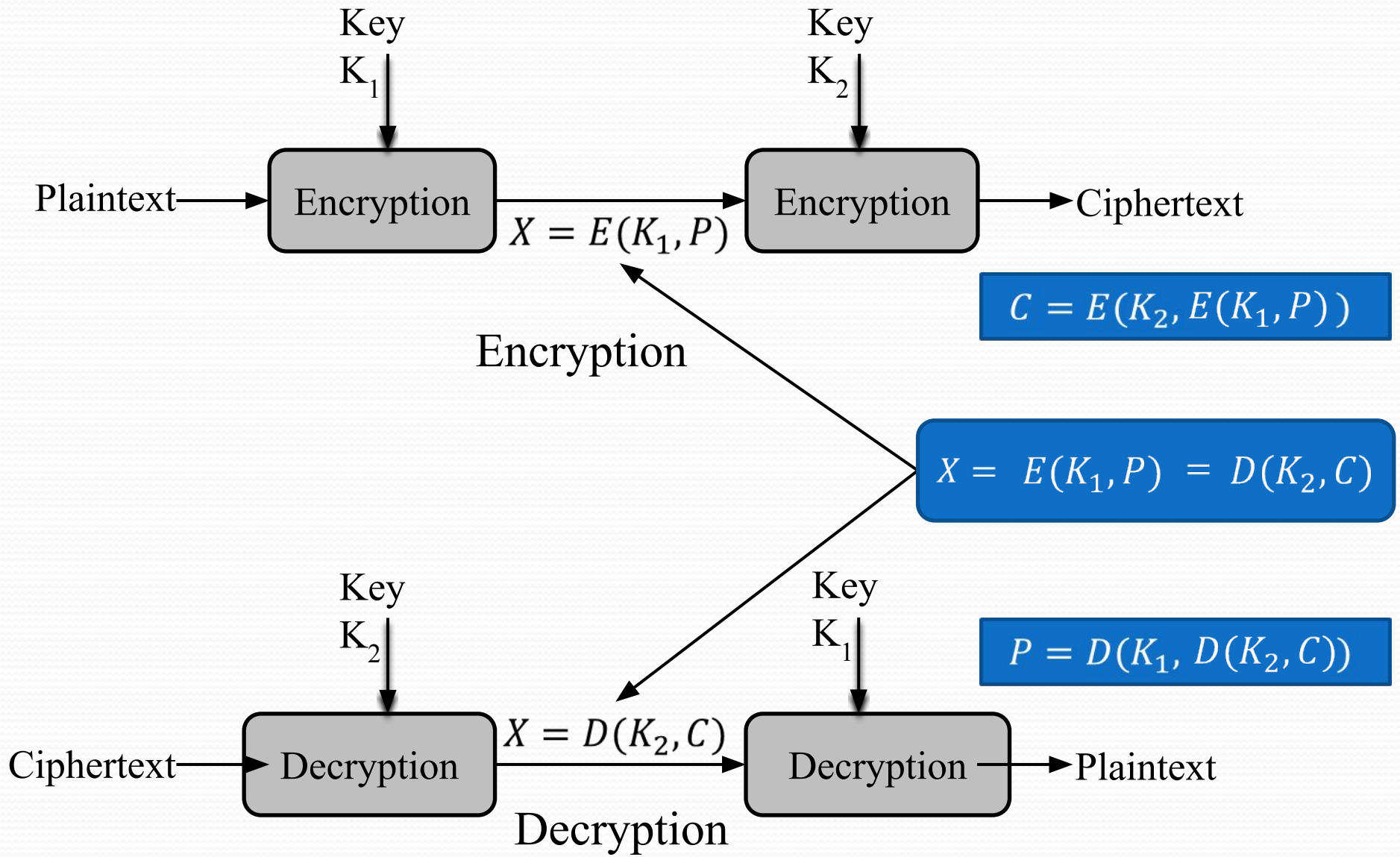
Summary of all modes

Operation Mode	Description	Type of Result
ECB	Each n-bit block is encrypted independently with same key.	Block Cipher
CBC	Same as ECB, but each block is XORed with previous cipher text.	Block Cipher
CFB	Each s-bit block is XORed with s-bit key which is part of previous cipher text.	Stream Cipher
OFB	Same as CFB, but input to the encryption is preceding encryption output.	Stream Cipher
CTR	Same as OFB, but a counter is used instead of nonce.	Stream Cipher

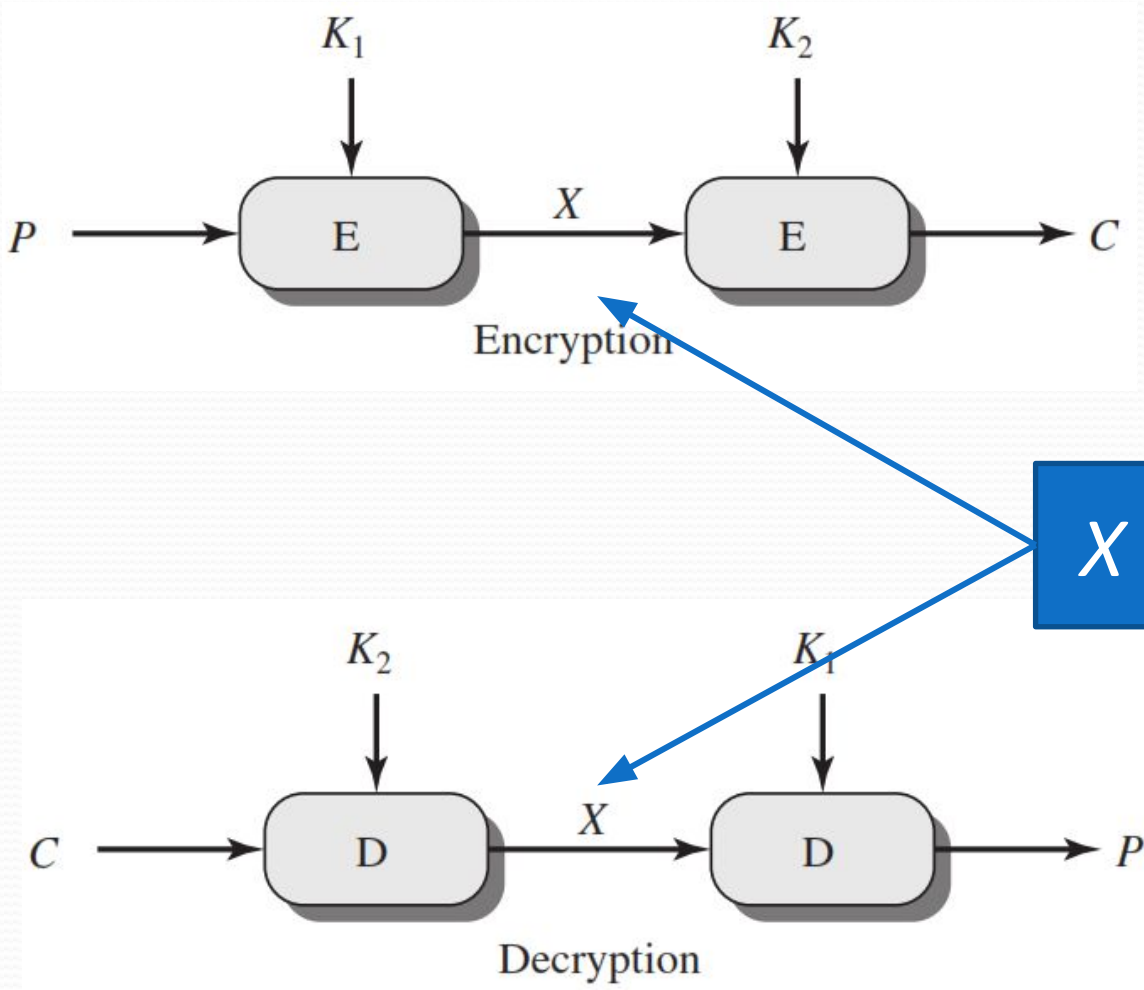
Multiple Encryption

- Given the potential vulnerability of DES to a brute-force attack, there has been considerable interest in finding an alternative.
- For DES requires 2^{56} operations for brute force attack.
- One approach is to design a completely new algorithm, of which AES is a prime example.
- Another alternative, which would preserve the existing investment in software and equipment, is to use multiple encryption with DES and multiple keys.

Double DES


Key
K_1
Key
K_2
Plaintext
Encryption
$X = E(K_1, P)$
Encryption
Ciphertext
$C = E(K_2, E(K_1, P))$
Encryption
$X = E(K_1, P) = D(K_2, C)$
Key
K_2
Key
K_1
$P = D(K_1, D(K_2, C))$
Ciphertext
Decryption
$X = D(K_2, C)$
Decryption
Plaintext
Decryption

Double DES



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

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

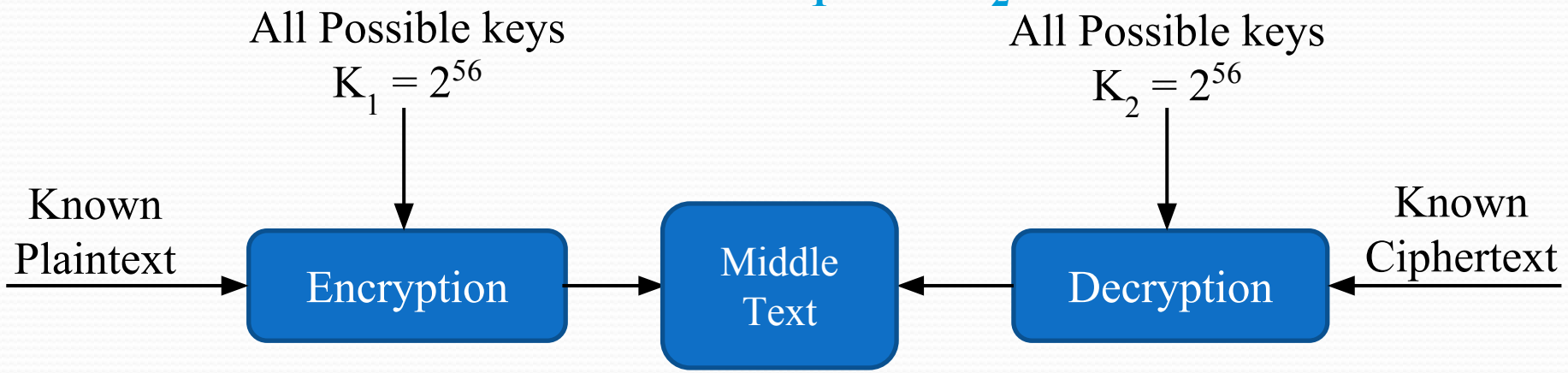
$P=D(K_1,D(K_2, C))$

Double DES

- For double DES, 2 × 56-bit keys, meaning 112-bit key length.
- Requires 2^{112} operations for brute force attack.
- Meet-in-the-middle attack makes it easier.

Meet in the Middle Attack

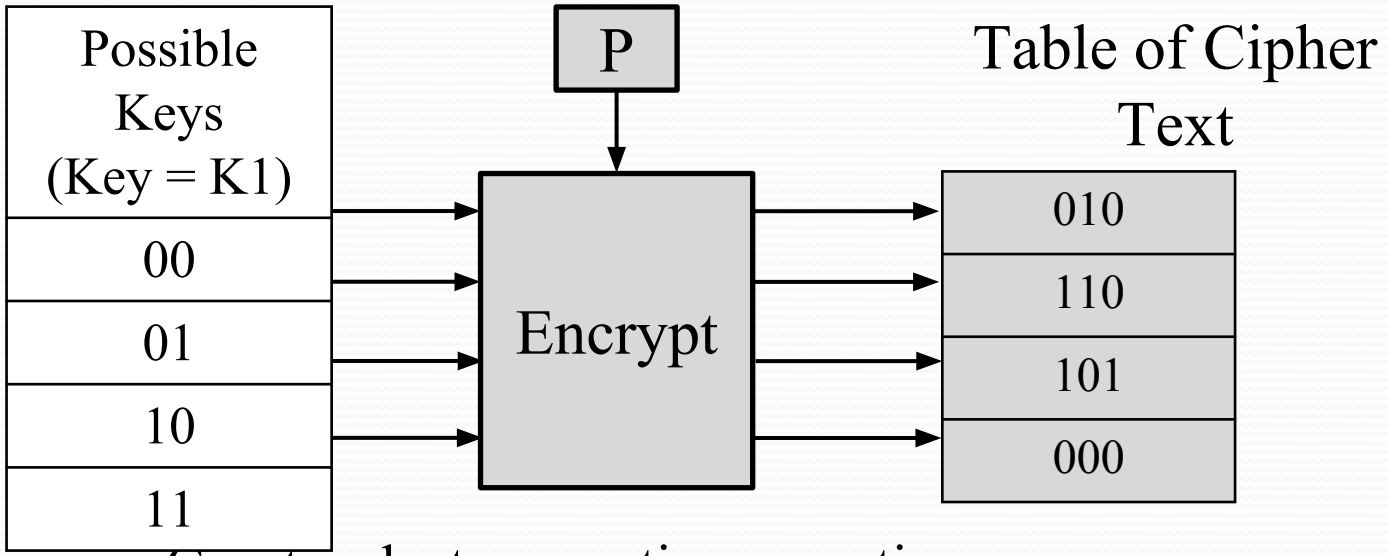
- This attack involves encryption from one end, decryption from the other and matching the results in the middle.
- Suppose cryptanalyst knows P_i and corresponding C_i.
- Now, the aim is to obtain the values of K_1 and K_2.



- No. of Encryptions and Decryptions: $2^{56} + 2^{56} = 2^{57}$
- For Double DES requires 2^{57} operations for brute force attack.

Meet in the Middle Attack Step-1

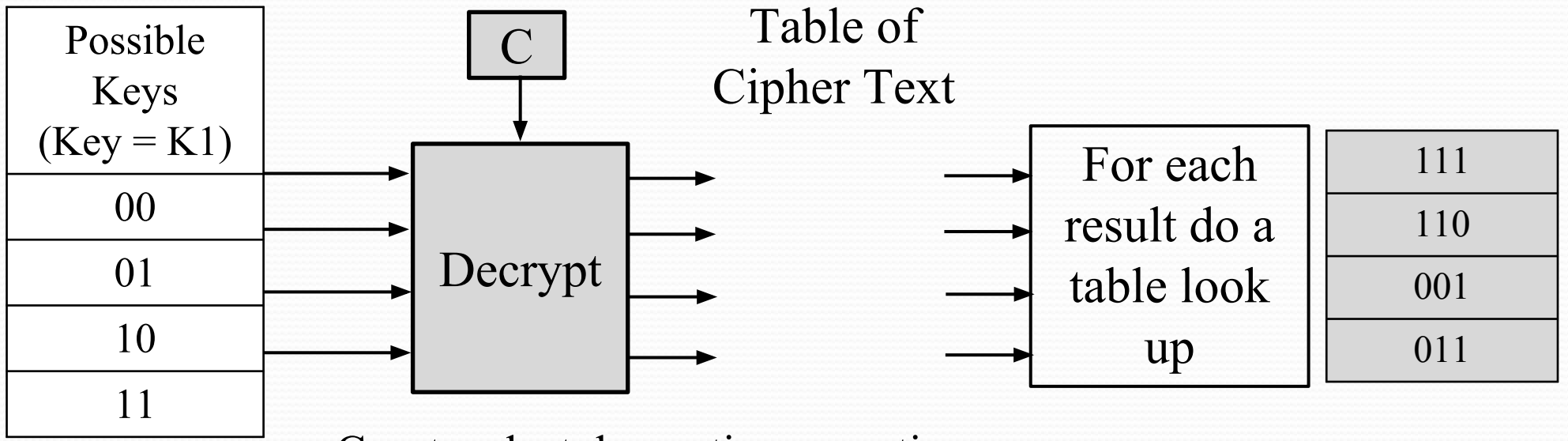
- For all possible values (2^{56}) of key K1, the cryptanalyst would encrypt the known plaintext by performing E(K1,P).
- The cryptanalyst would store output in a table.



Cryptanalyst encryption operation

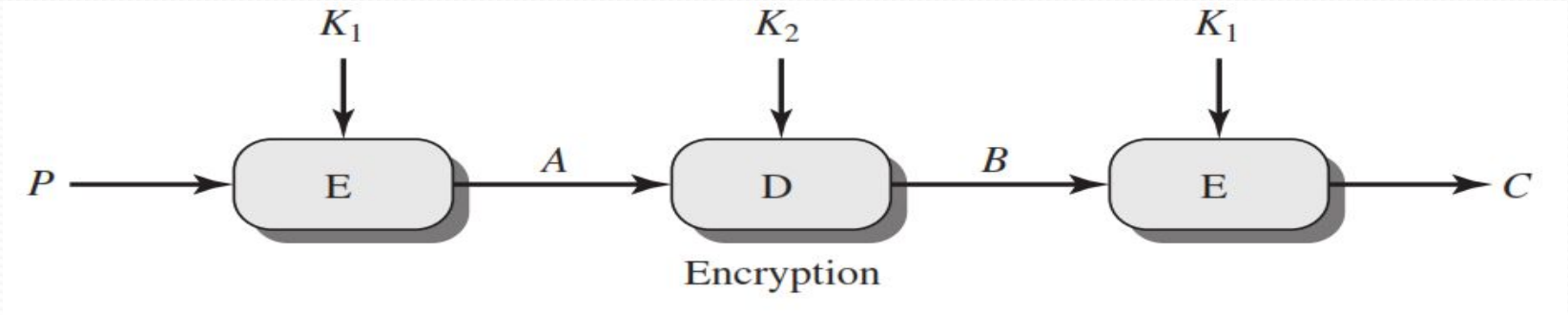
Meet in the Middle Attack Step-2

- Cryptanalyst decrypt the known ciphertext with all possible values of K2.
- In each case cryptanalyst will compare the resulting value with the all values in the table of ciphertext.

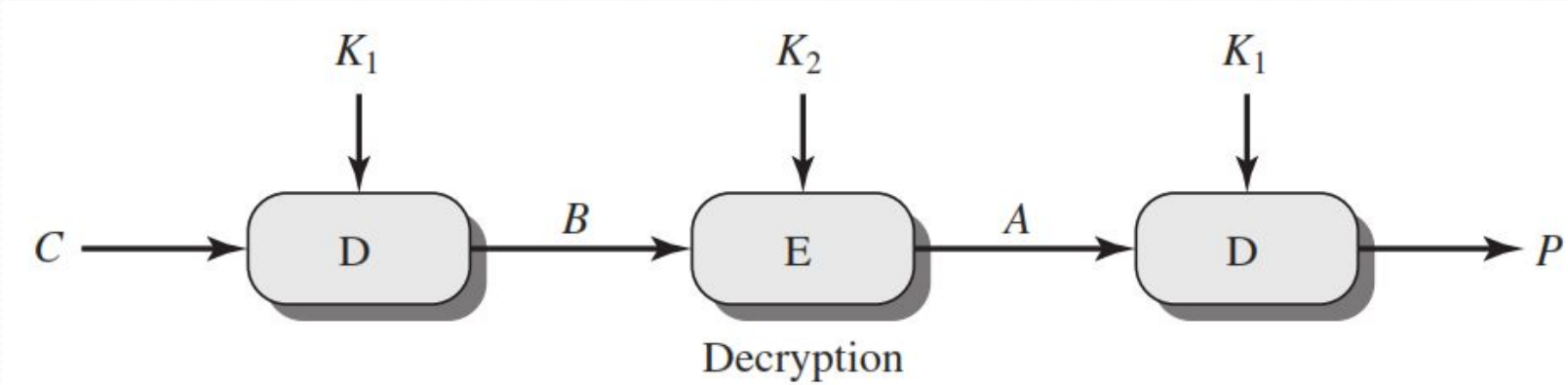


Cryptanalyst decryption operation

Triple DES

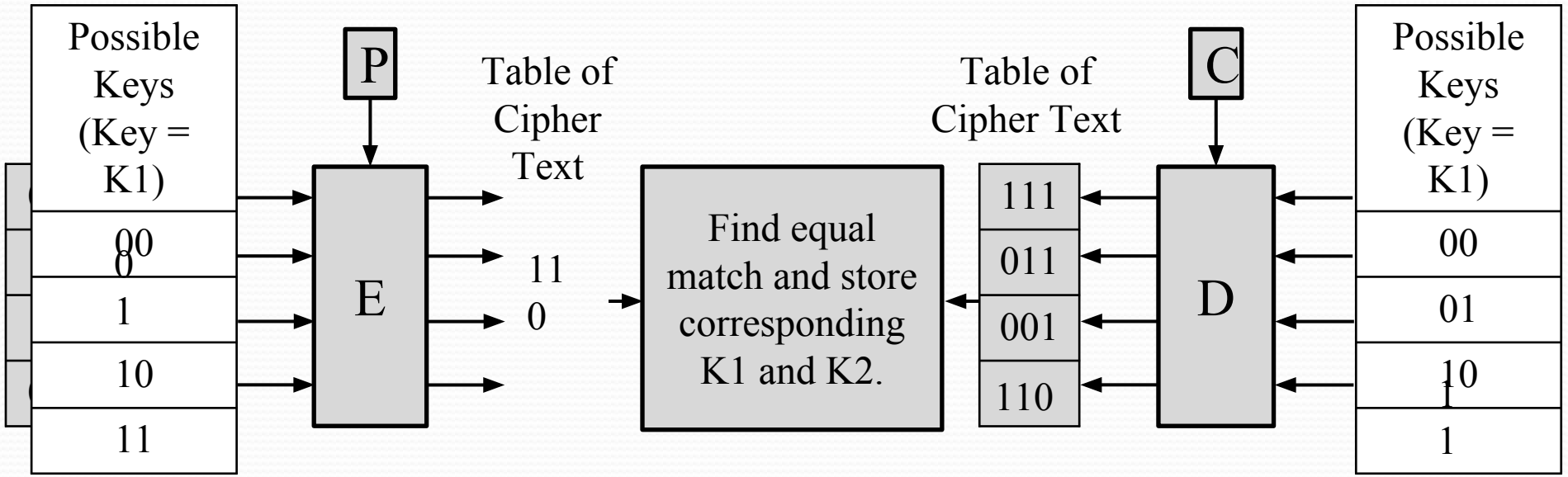


$$C=E(K_1,D(K_2,E(K_1,P)))$$



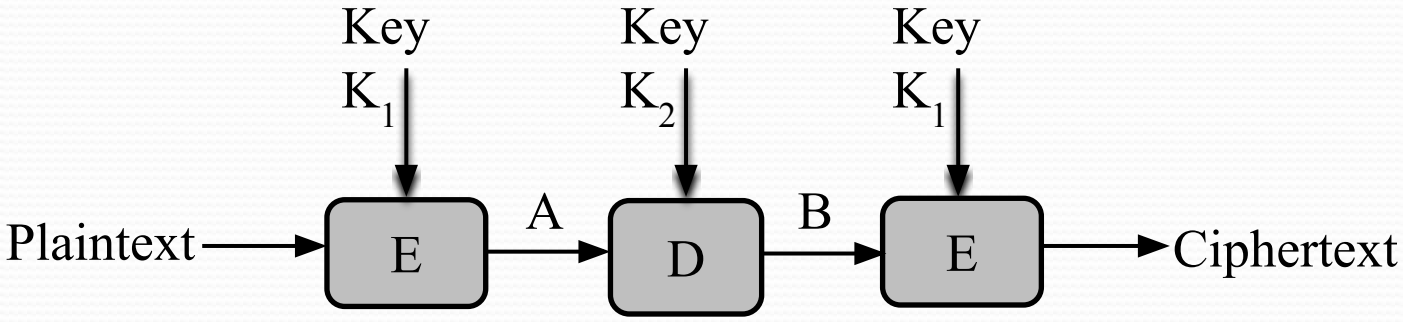
$$P=D(K_1,E(K_2,D(K_1,C)))$$

Meet in the Middle Attack

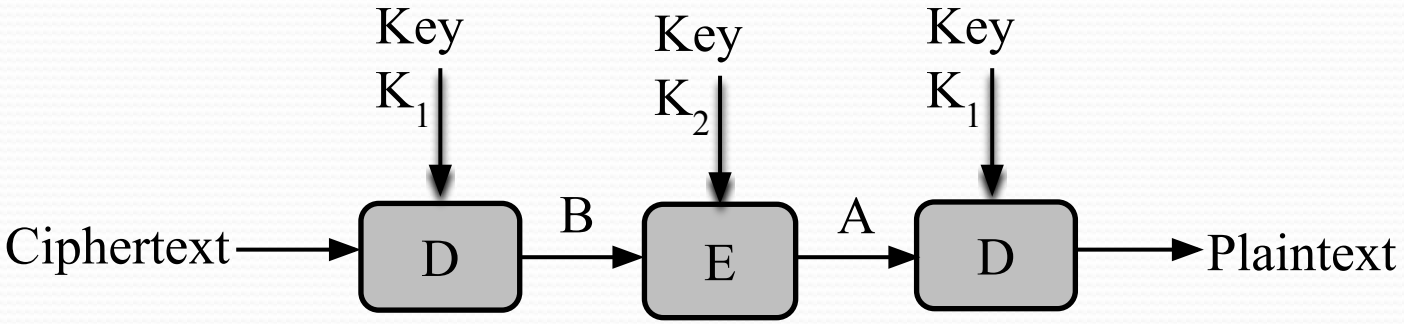


Values of K1=01 and K2=11

Triple DES



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



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