Unit 2

Modes of Operations, Multiple encryptions and triple DES

Outline

- Block cipher modes of operations
  - Electronic Code Book Mode
  - Cipher Block Chaining Mode
  - Cipher Feedback Mode
  - Output Feedback Mode
  - Counter Mode
- Multiple encryptions
- Triple DES

Block Cipher Modes of Operations

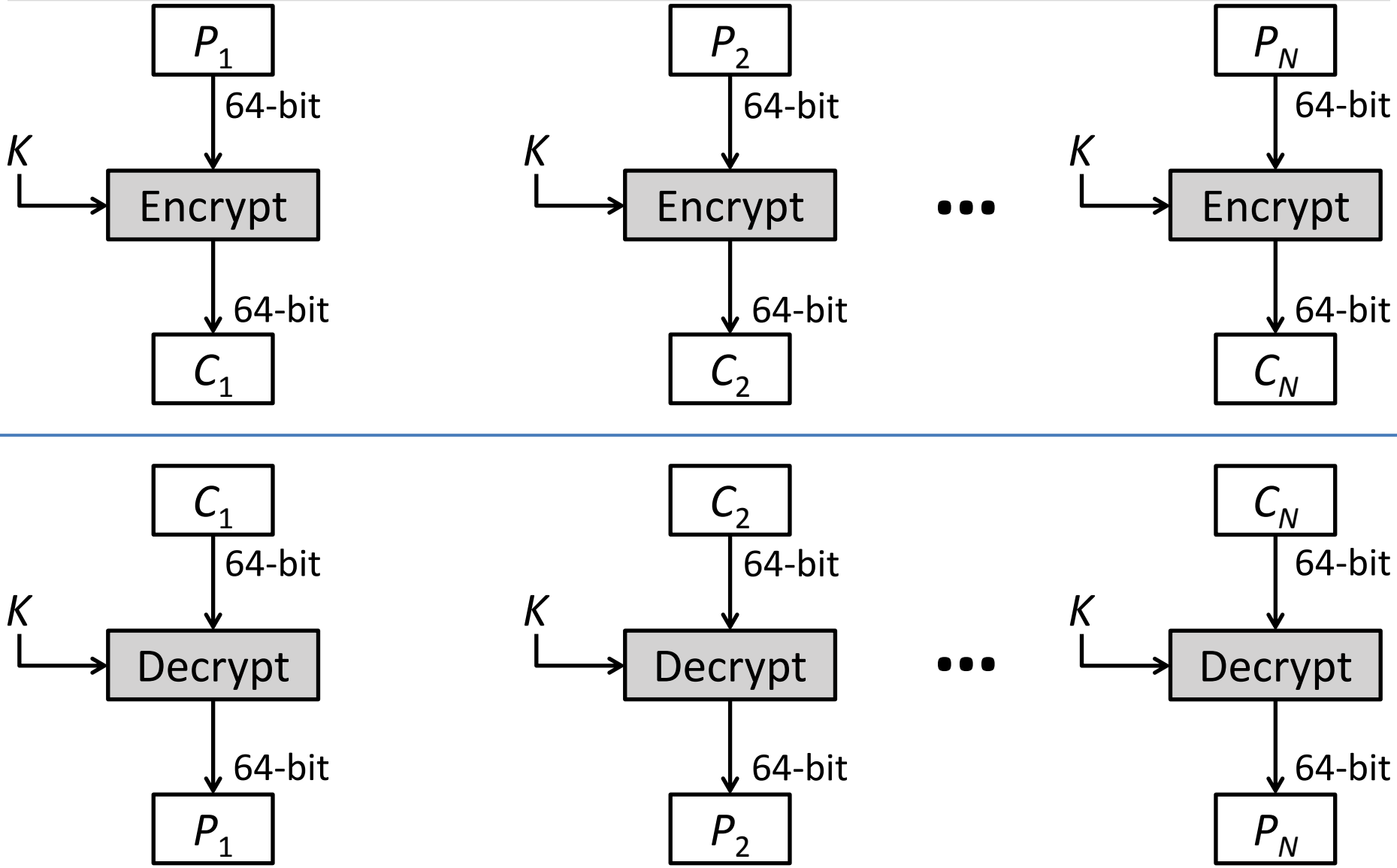
- To apply a block cipher in a **variety of applications**, five "modes of operation" have been defined.
- The **five modes** are intended to cover a wide variety of applications of encryption for which a block cipher could be used.
- These modes are intended for use with any symmetric block cipher, including triple DES and AES.

1. Electronic Code Book (ECB)
2. Cipher Block Chaining (CBC)
3. Cipher Feedback (CFB)
4. Output Feedback (OFB)
5. Counter (CTR)

1. Electronic Code Book (ECB)

- In **ECB** Mode Plaintext is 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 block of plaintext.

1. ECB Encryption & Decryption



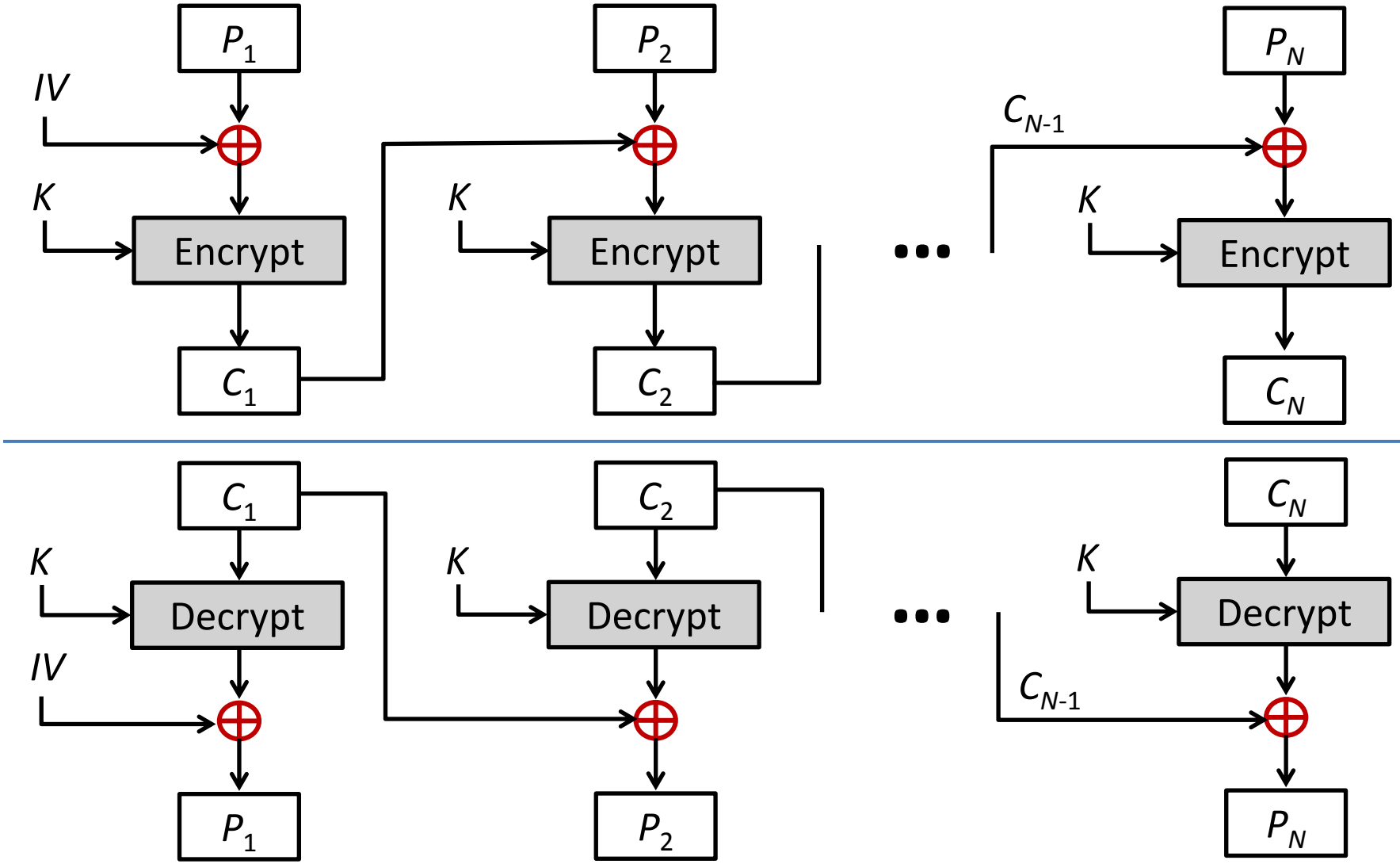
Electronic Code Book - Cont…

- **Strength:** it's simple.
- **Weakness:**
  - Repetitive information contained in the plaintext may show in the ciphertext also.
  - If the message has repetitive elements with a period of repetition a multiple of b bits, then these elements can be identified by the analyst.
- **Typical application:**
  - Secure transmission of short pieces of information (e.g. a temporary encryption key)

2. Cipher Block Chaining (CBC)

- **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; 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.
- On decryption, the **IV** is XORed with the output of the decryption algorithm to recover the first block of plaintext.

2. CBC - Encryption & Decryption



CBC	$C_1 = \mathrm{E}(K, [P_1 \oplus \mathrm{IV}])$ $C_j = \mathrm{E}(K, [P_j \oplus C_{j-1}])\ j = 2, \ldots, N$	$P_1 = \mathrm{D}(K, C_1) \oplus \mathrm{IV}$ $P_j = \mathrm{D}(K, C_j) \oplus C_{j-1}\ j = 2, \ldots, N$

2. 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

Cons:
No Parallelism

Pros:
Confidentiality + Availability

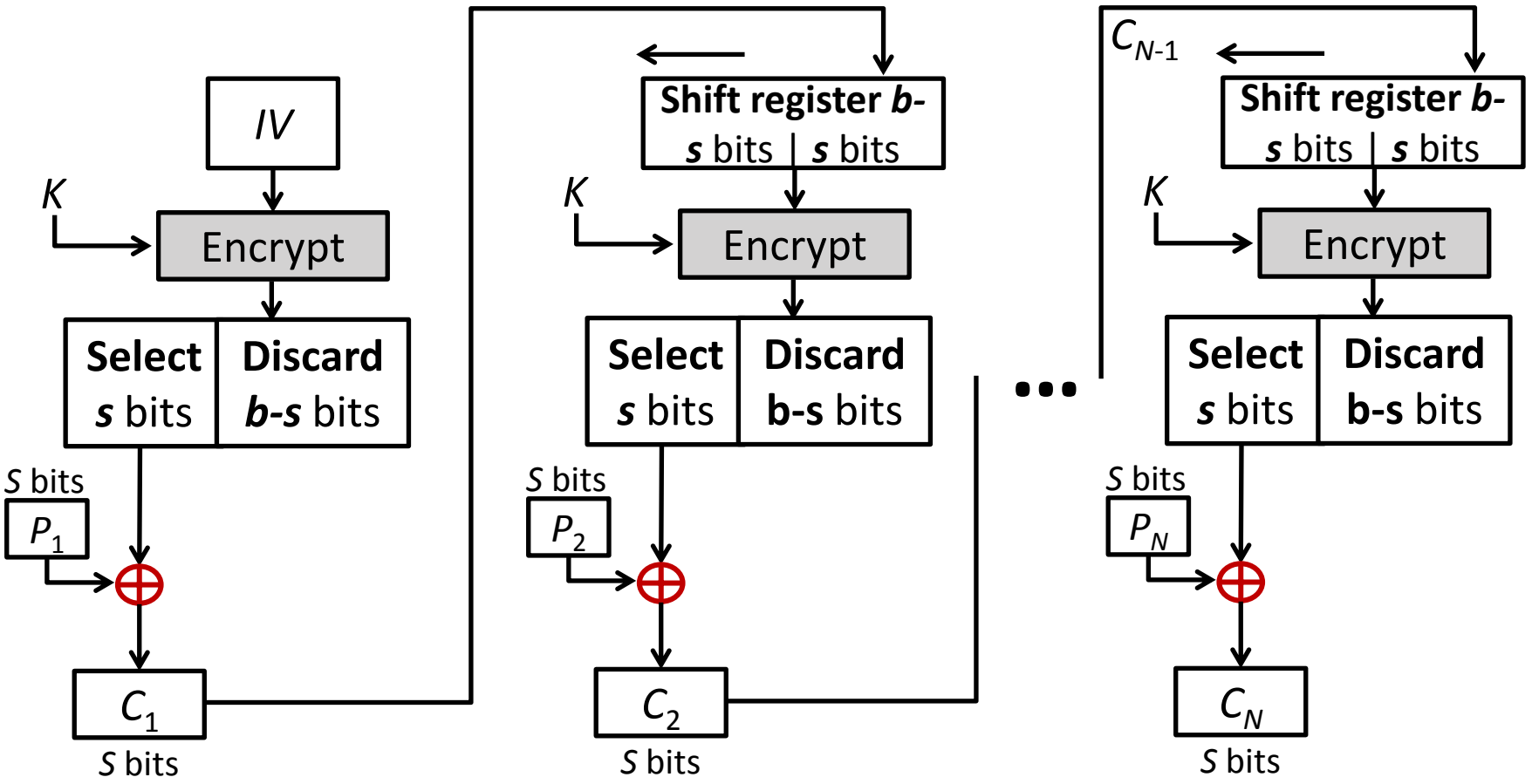
3. Cipher Feedback Mode (CFB)

- 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.

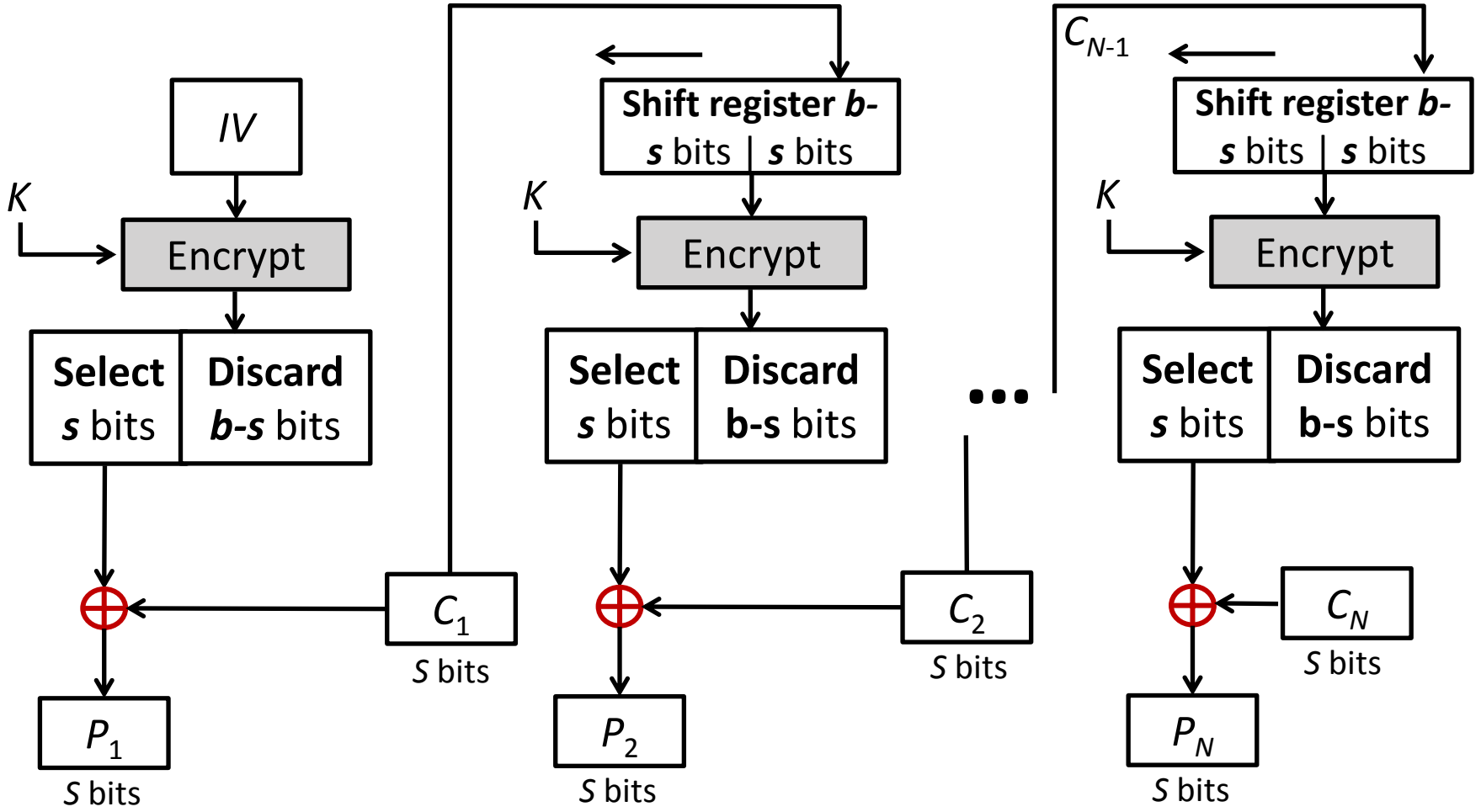
- A stream cipher eliminates the need to pad a message to be an integral number of blocks.

3. CFB Encryption



CFB	$I_1 = IV$ $I_j = \mathrm{LSB}_{b-s}(I_{j-1}) \| C_{j-1} \quad j = 2, \ldots, N$ $O_j = \mathrm{E}(K, I_j) \quad j = 1, \ldots, N$ $C_j = P_j \oplus \mathrm{MSB}_s(O_j) \quad j = 1, \ldots, N$

3. CFB Decryption



$$
\begin{aligned}
I_1 &= IV \\
I_j &= \mathrm{LSB}_{b-s}(I_{j-1}) \| C_{j-1} \quad j = 2, \ldots, N \\
O_j &= \mathrm{E}(K, I_j) \quad j = 1, \ldots, N \\
P_j &= C_j \oplus \mathrm{MSB}_s(O_j) \quad j = 1, \ldots, N
\end{aligned}
$$

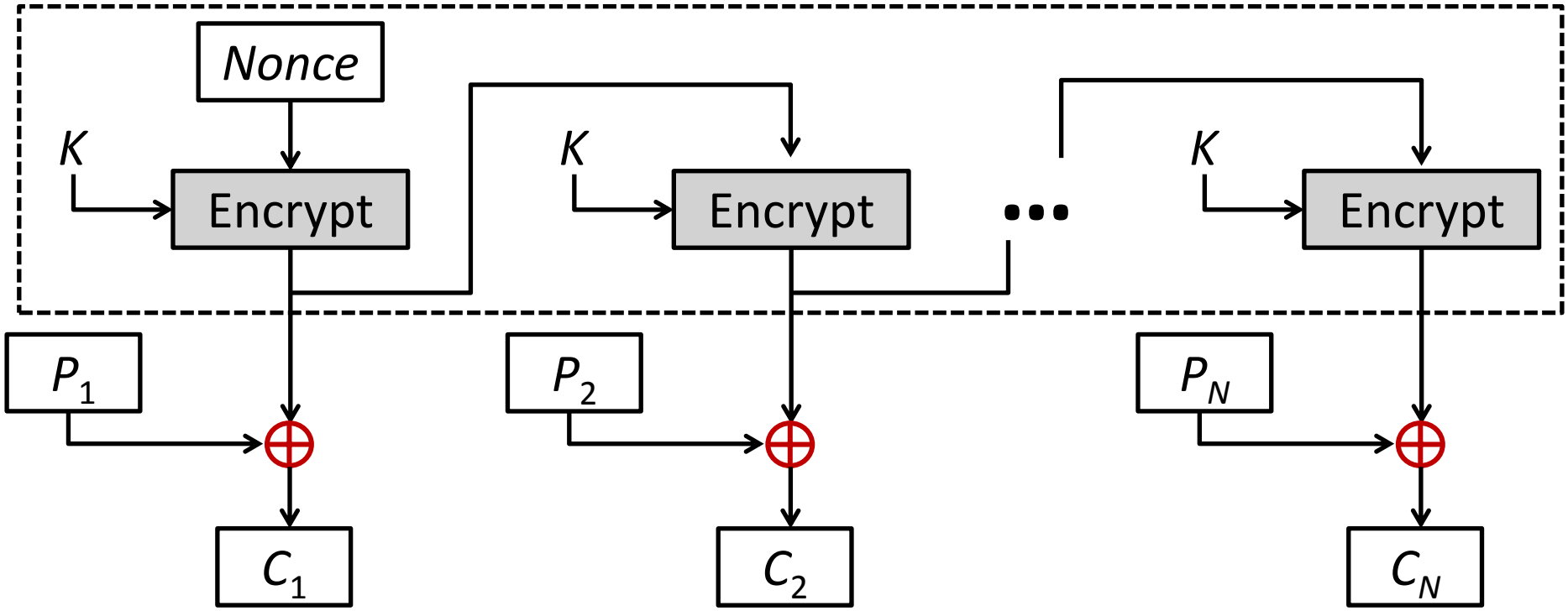
CFB Mode

- 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. Output Feedback Mode (OFB)

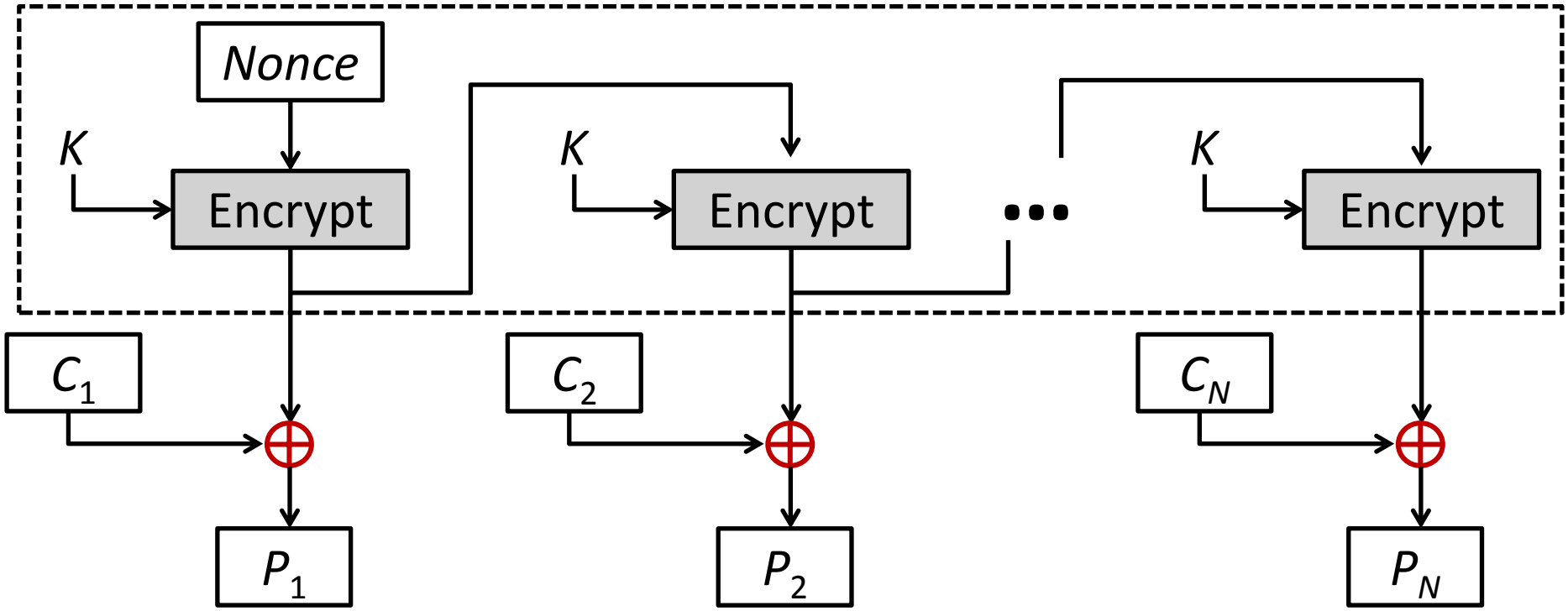
- The output feedback (**OFB**) mode is similar in structure to that of **CFB**.
- For **OFB**, the output of the encryption function is fed back to become the input for encrypting the next block of plaintext.
- In **CFB**, the output of the XOR unit is fed back to become input for encrypting the next 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.
- **Nonce:** A time-varying value that has at most a negligible chance of repeating, for example, a **random value** that is freshly generated for each use, a timestamp, a sequence number, or some combination of these.

4. OFB Encryption



OFB	$I_1 = Nonce$ $I_j = O_{j-1} \quad j = 2, \ldots, N$ $O_j = \mathrm{E}(K, I_j) \quad j = 1, \ldots, N$ $C_j = P_j \oplus O_j \quad j = 1, \ldots, N-1$ $C_N^* = P_N^* \oplus \mathrm{MSB}_u(O_N)$

4. OFB Decryption



$$
\begin{aligned}
I_1 &= Nonce \\
I_j &= O_{j-1} \qquad j = 2, \ldots, N \\
O_j &= \mathrm{E}(K, I_j) \qquad j = 1, \ldots, N \\
P_j &= C_j \oplus O_j \qquad j = 1, \ldots, N-1 \\
P_N^* &= C_N^* \oplus \mathrm{MSB}_u(O_N)
\end{aligned}
$$

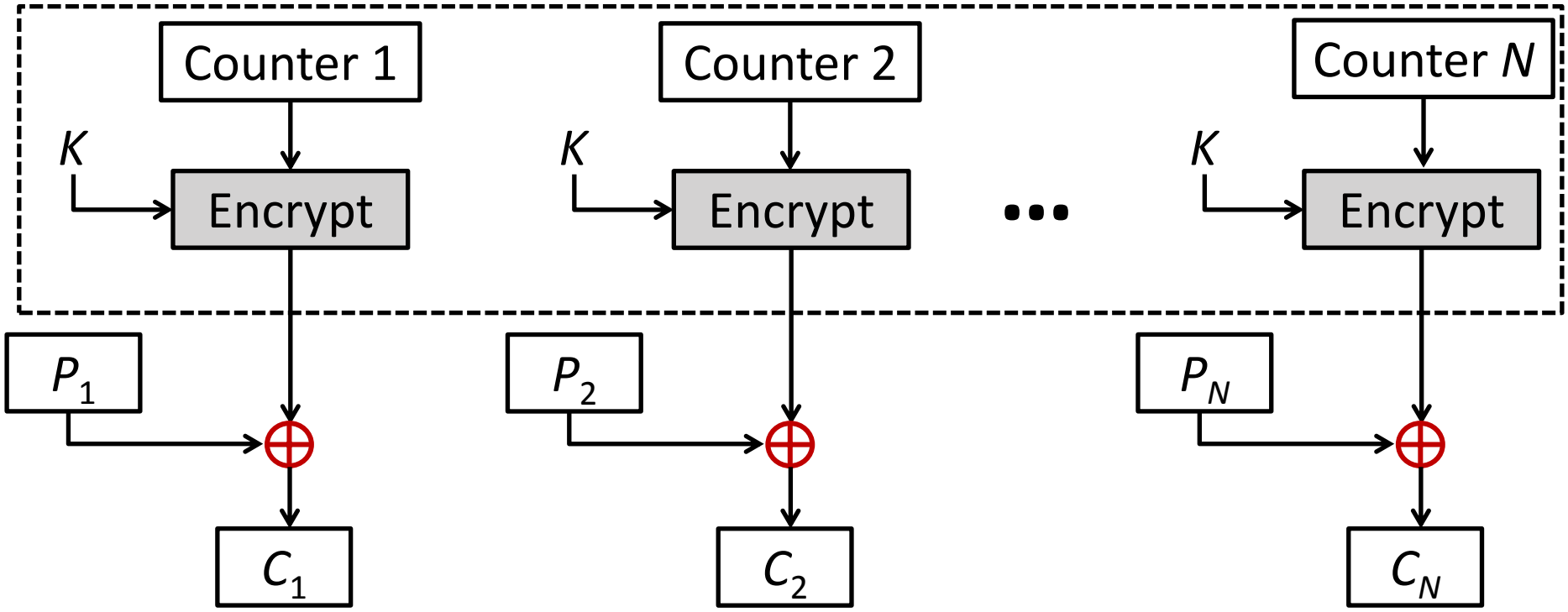
OFB Mode

- Each bit in the ciphertext is independent of the previous bit or bits. i.e. Feedback is independent of transmission
- This **avoids error propagation which**
- It allows many error correcting codes to function normally even when applied before encryption
- It helps recover from ciphertext bit errors, but cannot self-synchronize
- Pre-compute of forward cipher is possible
- Flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location

5. Counter Mode (CTR)

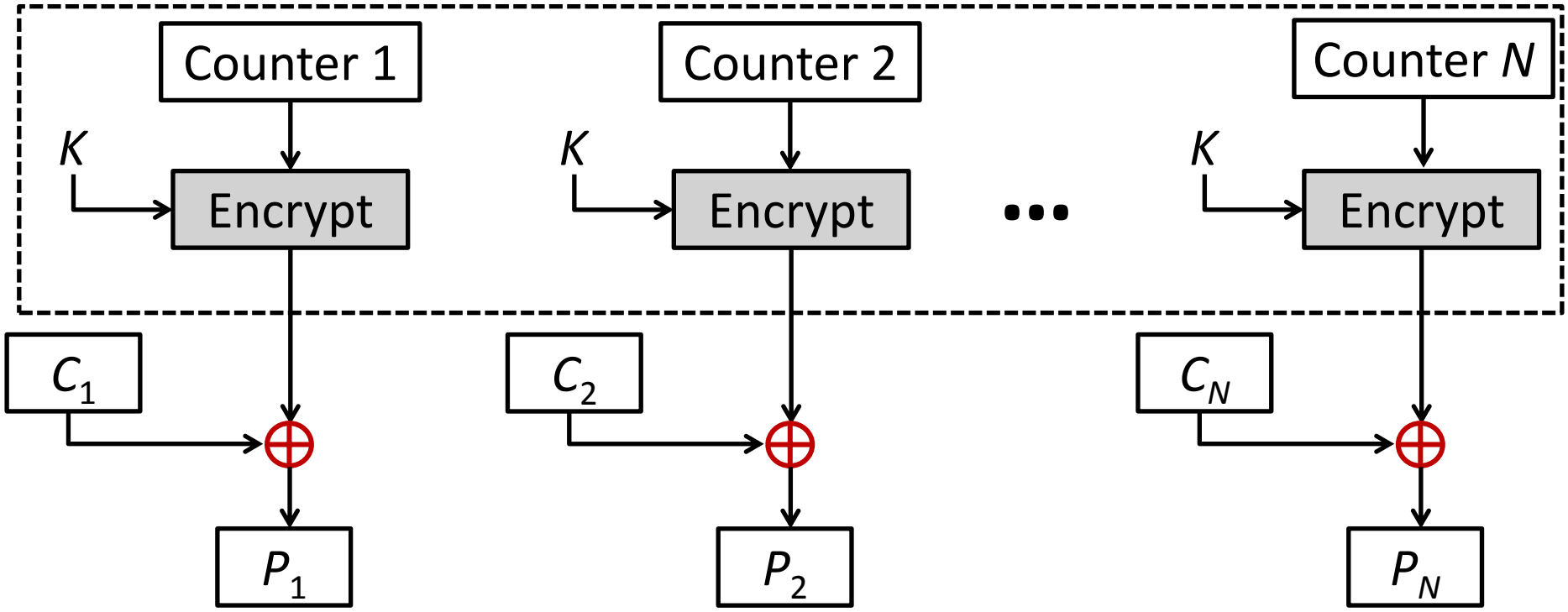
- Counter (**CTR**) mode has increased recently with applications to ATM (asynchronous transfer mode) network security and IP sec (IP security).
- A **counter** equal to the plaintext block size is used.
- The counter value must be different for each plaintext block that is encrypted.
- Typically, the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

5. CTR Encryption



CTR	$C_j = P_j \oplus \mathrm{E}(K, T_j) \qquad j = 1, \ldots, N-1$ $C_N^* = P_N^* \oplus \mathrm{MSB}_u[\mathrm{E}(K, T_N)]$

4. CTR Decryption



$$P_j = C_j \oplus \mathrm{E}(K, T_j) \qquad j = 1, \ldots, N-1$$
$$P_N^* = C_N^* \oplus \mathrm{MSB}_u[\mathrm{E}(K, T_N)]$$

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; fast encryption/decryption

- Counter
  - 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, except that the input to the encryption algorithm is the output of preceding encryption algorithm	Stream Cipher
CTR	Same as OFB, but a counter is used instead of nonce	Stream Cipher

Typical Applications of All Modes

Mode	Typical Application
Electronic Codebook (ECB)	• Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	•General-purpose block-oriented transmission •Authentication
Cipher Feedback (CFB)	•General-purpose stream-oriented transmission •Authentication
Output Feedback (OFB)	•Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	• General-purpose transmission •Useful for high-speed requirements

Use of Stream Ciphers

- Although the five modes of operations enable the use of block ciphers for encipherment of messages or files in large units (ECB, CBC, and CTR) and small units (CFB and OFB), sometimes pure streams are needed for enciphering small units of data such as characters or bits.
- Stream ciphers are more efficient for real-time processing.
- Several stream ciphers have been used in different protocols during the last few decades.
- Examples: RC4, A5/1

RC4

- RC4 means Rivest Cipher 4 invented by Ron Rivest in 1987 for RSA Security. It is a Stream Ciphers.
- Stream Ciphers operate on a stream of data byte by byte.
- RC4 stream cipher is one of the most widely used stream ciphers because of its simplicity and speed of operation.
- It is a variable key-size stream cipher with byte-oriented operations. It uses either 64 bit or 128-bit key sizes.
- It is generally used in applications such as Secure Socket Layer (SSL), Transport Layer Security (TLS), and also used in IEEE 802.11 wireless LAN std.

A5/1

- **A5/1** is a stream cipher used to provide over-the-air communication privacy in the GSM cellular telephone standard.
- It is one of several implementations of the A5 security protocol.

Synchronous & Asynchronous Stream Ciphers

- With **synchronous stream** ciphers, the bits of the key stream do not depend on the ciphertext bits.
- With **asynchronous stream** ciphers the key stream can be inferred (provided one knows the secret key) from previous bits of the cipher stream.
- CTR would be an example of a synchronous streaming mode and CFB would be an example of an asynchronous mode.

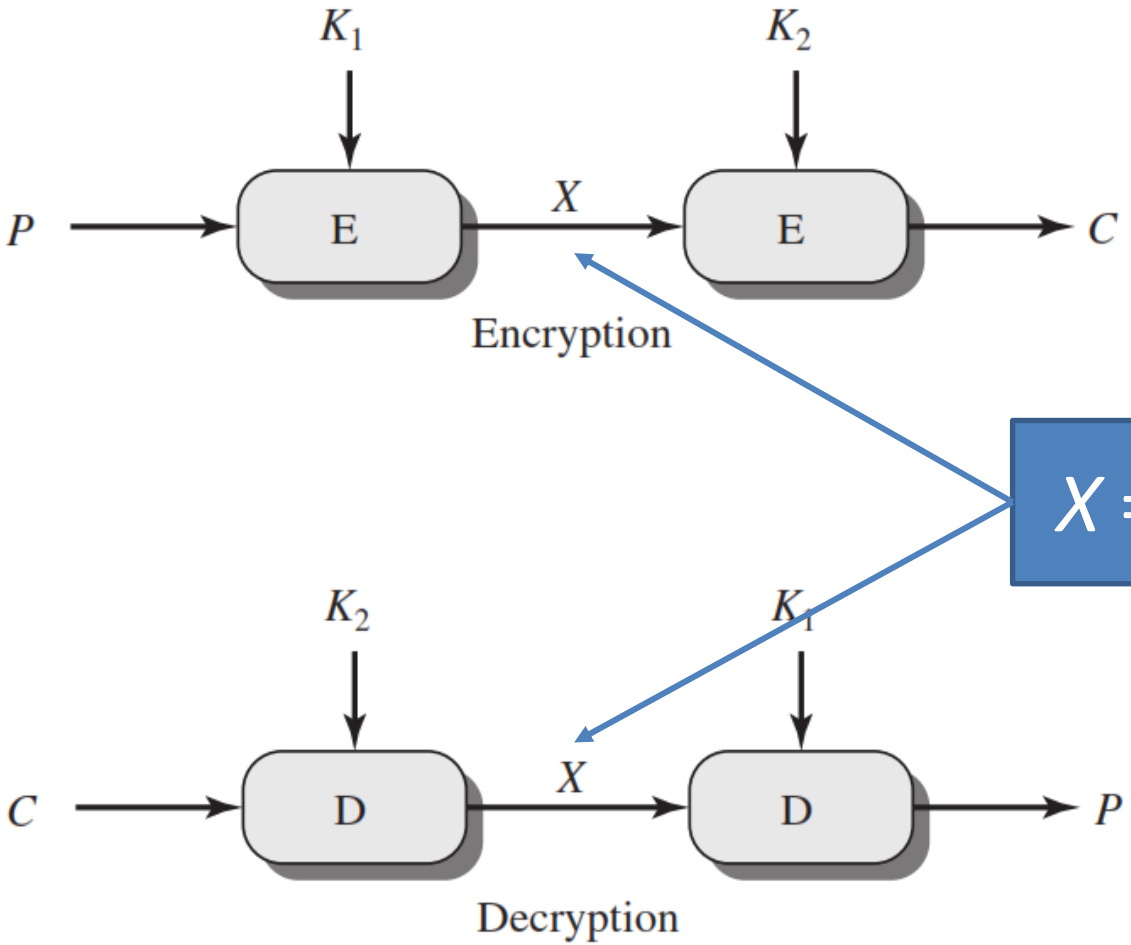
Synchronous & Asynchronous stream ciphers (Cont.)

- Synchronous ciphers have these advantages and disadvantages:
  - Key stream can be pre-computed before plaintext or ciphertext is provided, often with parallelism. typically faster and more efficient than block ciphers when encrypting large volumes of data in real-time
  - As the keystream is deterministic, they have the disadvantage of ciphertext malleability (a known change in ciphertext produces a known change in plaintext) and so will need to be combined with some form of message authentication.
- Asynchronous ciphers have these advantages and disadvantages:
  - The key stream can only be computed once the plaintext/ciphertext is provided. However, changing the ciphertext changes subsequent key stream and so there is considerably less malleability.
  - They also allow easy synchronization at any point in transmission.
  - They are more computationally intensive and slower than synchronous stream ciphers because of the additional complexity in generating the keystream

Multiple Encryption

- Given the **potential vulnerability of DES to a brute-force attack**, there has been considerable interest in finding an alternative.
- 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



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

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

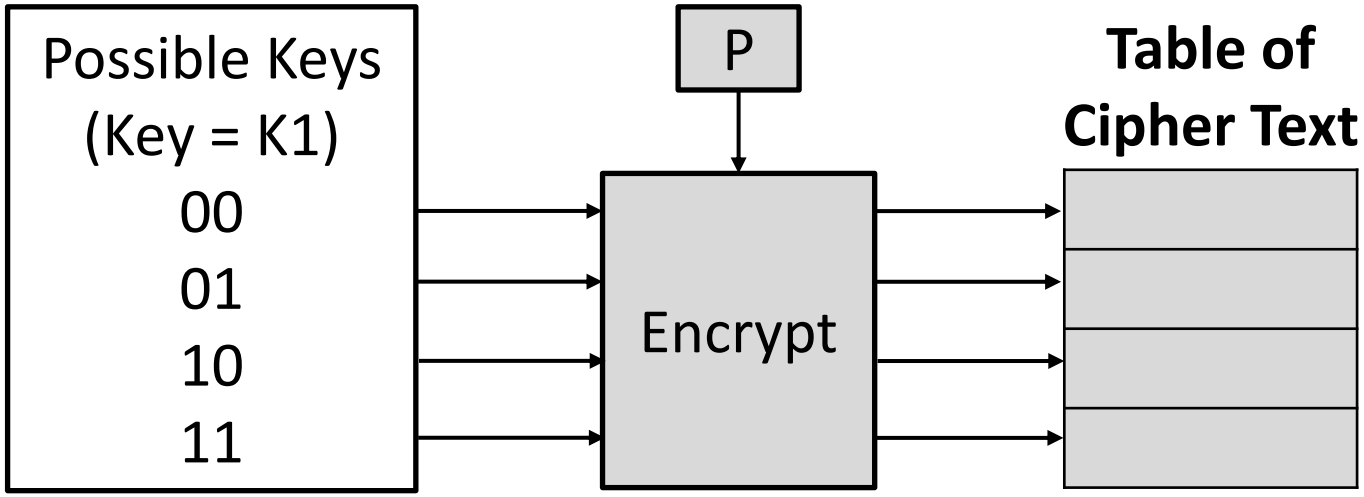
$P=D(K_1,D(K_2, C))$

Meet in the Middle Attack

- **Meet-in-the-middle (MITM) attacks** are often executed to decode multiple data encryption standard (DES) techniques.
- This attack involves encryption from one end, decryption from the other and matching the results in the middle.
- An attacker can use a MITM attack to bruteforce **Double DES**
  - an attacker encrypts the plaintext with all possible keys for the first encryption (2^56 operations) and then decrypts the ciphertext with each possible key for the second encryption (2^56 operations)

Meet in the Middle Attack Step-1

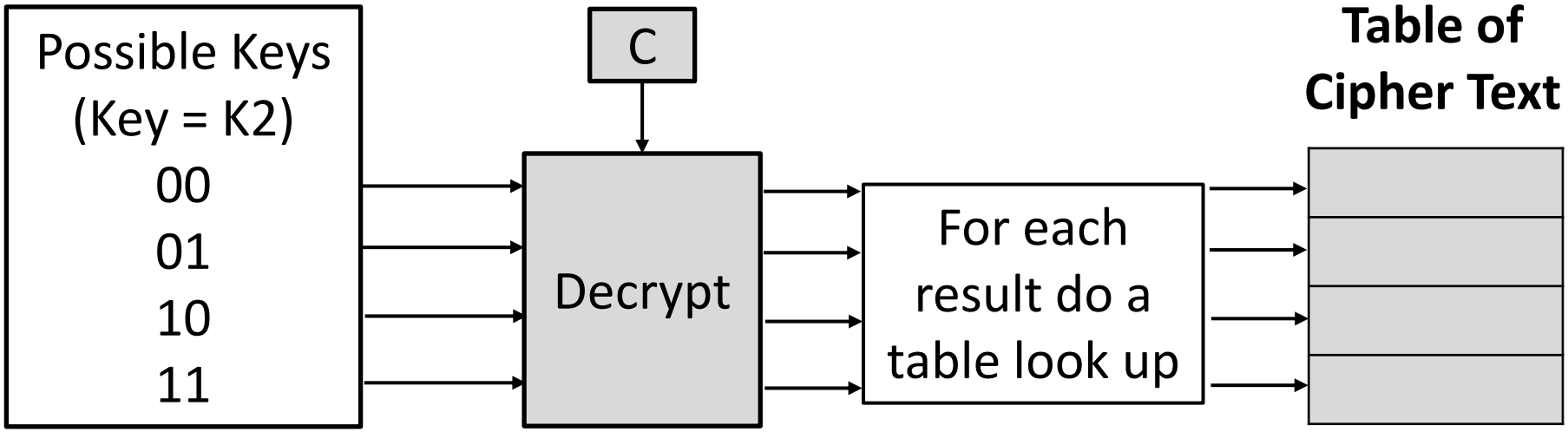
- Suppose cryptanalyst knows **P** and corresponding **C**.
- Now, the aim is to obtain the values of K_1 and K_2.
- For all possible values (2^{56}) of key K1, the cryptanalyst would encrypt the P by performing E(K1,P).
- The cryptanalyst would store output in a table.



Cryptanalyst encryption operation

Meet in the Middle Attack Step-2

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



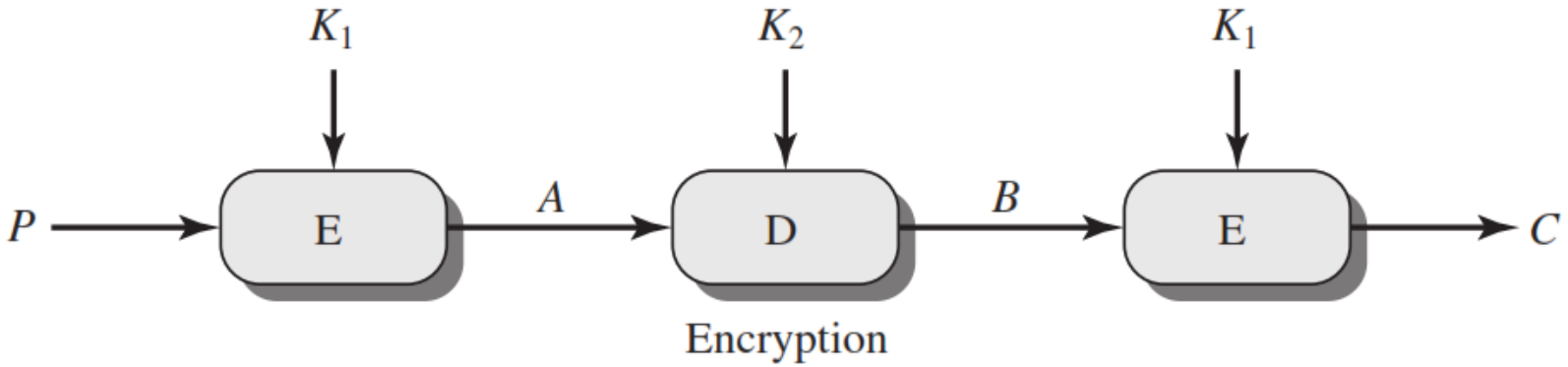
Cryptanalyst decryption operation

Thus, K1 and K2 can be obtained

Triple DES

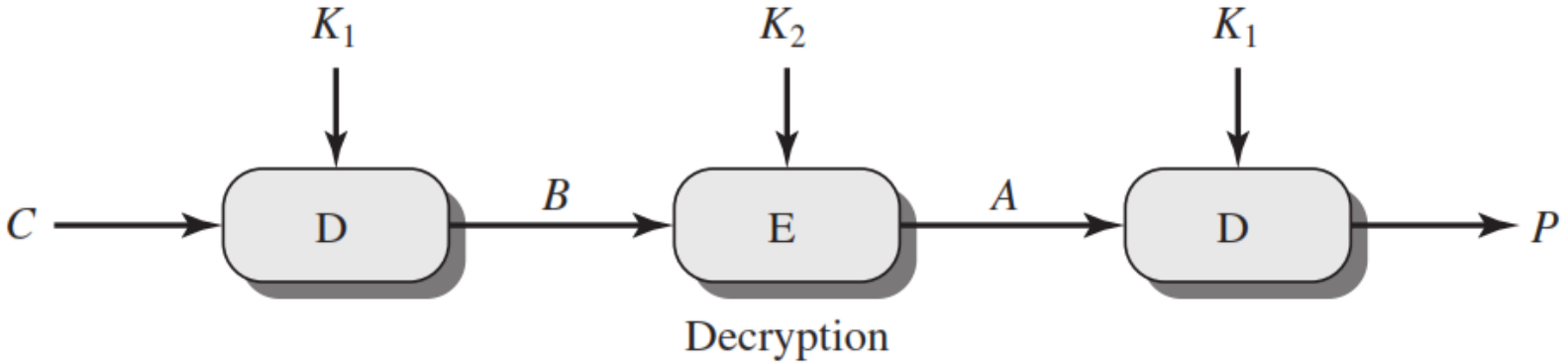
- An obvious counter to the meet in the middle attack is to use 3 stages of encryption with 3 different keys
- However, if 3 different keys are used, it has limitations of requiring a key length of 56x3= 168 bits which may be somewhat unwisely.
- As an alternative, Tuchman proposed a triple encryption method that uses **only 2 keys**.

Triple DES



Encryption

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



Decryption

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