

Advanced data Security

Part I:

Cryptography and Network Security

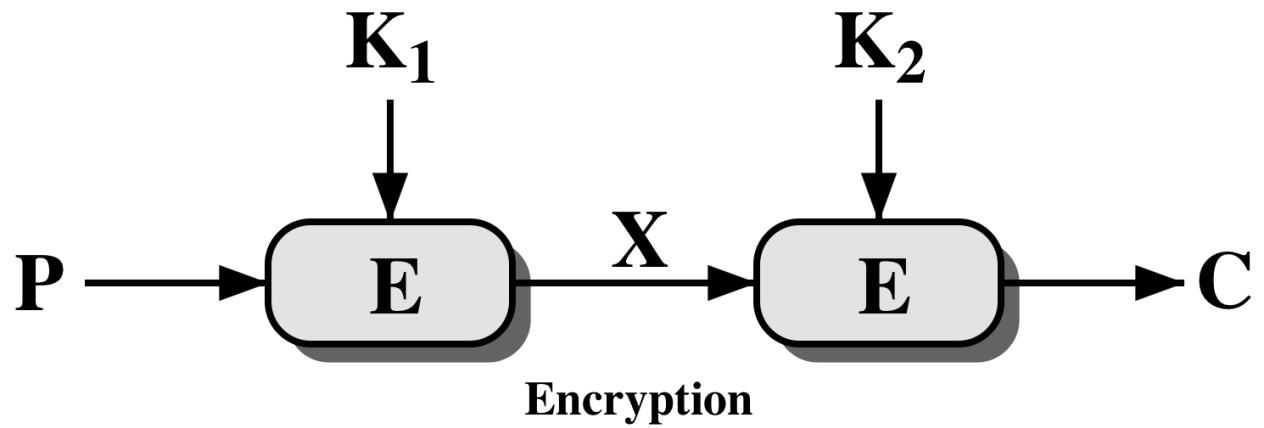
Chapter4:

3DES-Block Cipher Operation

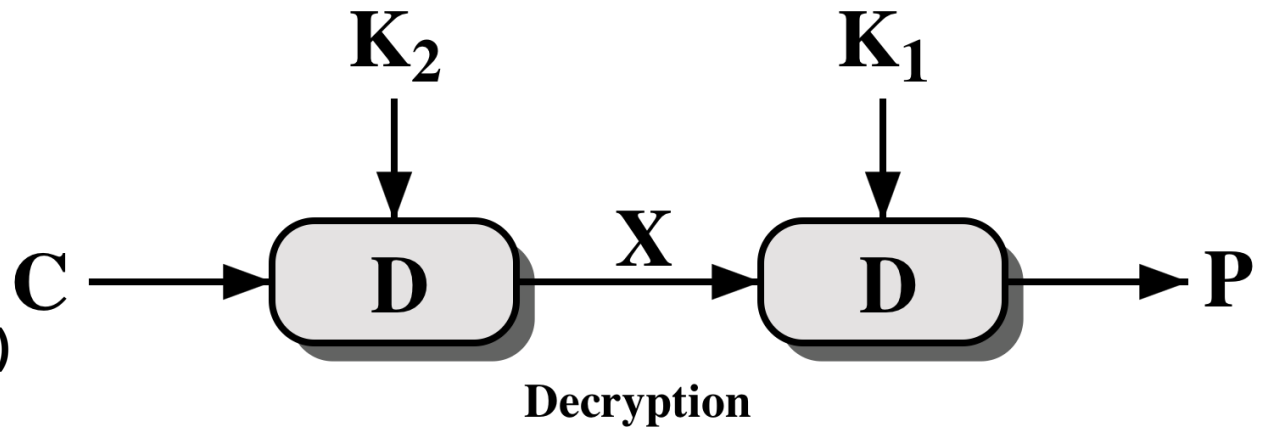
Prepared by:

Dr. Hamssa Hasrouny

Double DES



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



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

(a) Double Encryption

key length: $56 * 2 = 112$ bits,

resulting in a **dramatic increase** in cryptographic strength.

Meet-in-the-Middle Attack

The use of double DES results in a mapping that is not equivalent to a single DES encryption

The **meet-in-the-middle attack algorithm** will attack this scheme and does not depend on any particular property of DES but will work against any block encryption cipher



Triple-DES with Two-Keys

- Obvious counter to the meet-in-the-middle attack is to use three stages of encryption **with three different keys**
 - This raises the cost of the meet-in-the-middle attack to 2^{112} , which is beyond what is practical
 - Has the drawback of requiring a key length of $56 \times 3 = 168$ bits, which may be somewhat unwieldy
 - As an alternative Tuchman proposed a triple encryption method that uses only two keys
- 3DES with two keys is a relatively popular alternative to DES and has been adopted for use in the key management standards ANSI X9.17 and ISO 8732

Multiple Encryption

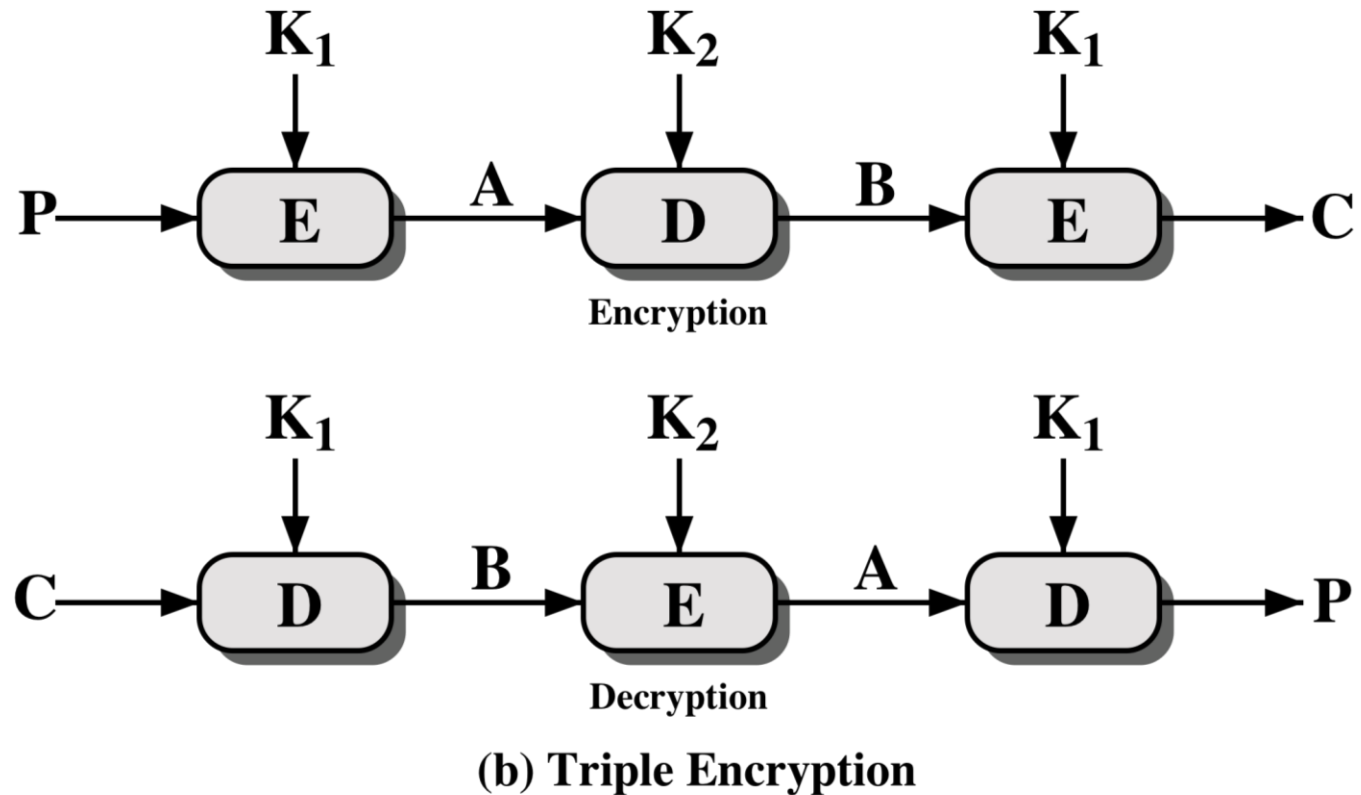


Figure 6.1 Multiple Encryption

Triple DES with Three Keys

- Many researchers now feel that three-key 3DES is the preferred alternative

Three-key 3DES has an effective key length of 168 bits and is defined as:

- $C = E(K_3, D(K_2, E(K_1, P)))$

Backward compatibility with DES is provided by putting:

- $K_3 = K_2$ or $K_1 = K_2$

- A number of Internet-based applications have adopted three-key 3DES including PGP and S/MIME

Block Cipher-Modes of Operation

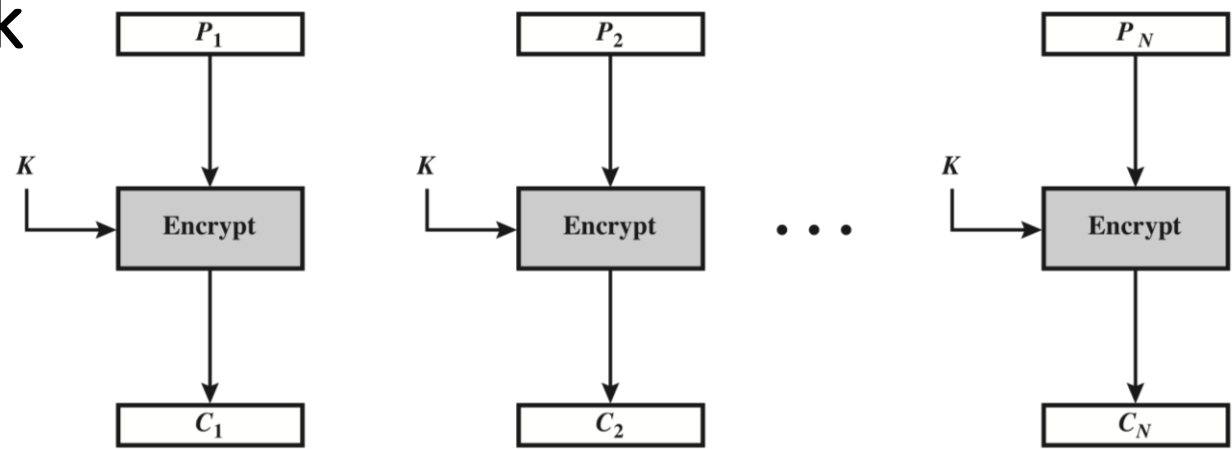
A block cipher takes a fixed-length block of text of length b bits and a key as input and produces a b -bit block of ciphertext.

- If plaintext to be encrypted is **greater than b bits**, then the block cipher is used by **breaking the plaintext up into b -bit blocks**.
- When **multiple blocks of plaintext** are encrypted using the same key, a **number of security issues arise**.
- **Mode of Operation:**
 - A technique for **enhancing the effect of a cryptographic algorithm** or adapting the algorithm for an application
- To apply a block cipher in a variety of applications, **five *modes of operation*** have been defined by NIST
 - These modes are intended for use with any **symmetric block cipher**, including triple **DES and AES**

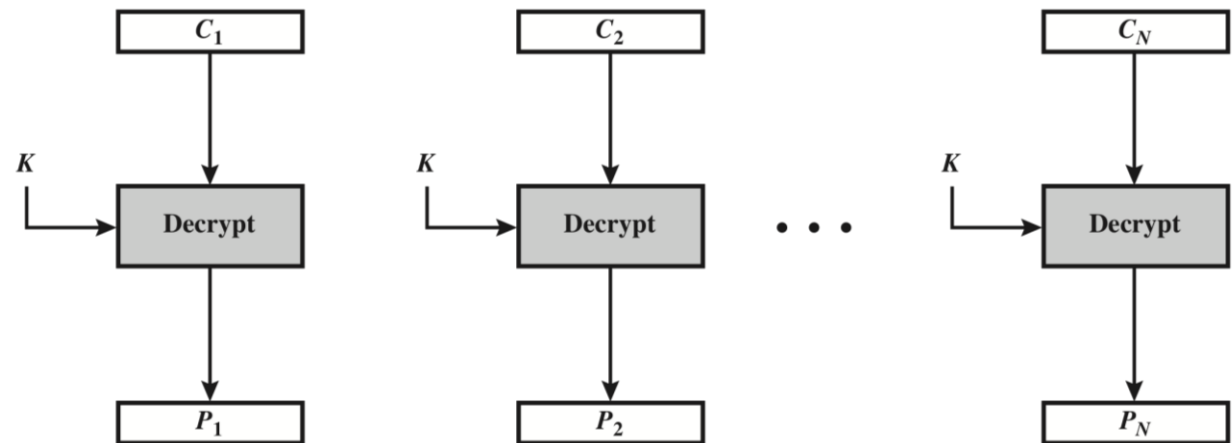
Table 6.1 Block Cipher Modes of Operation

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

In Figure 6.3, the plaintext (padded as necessary) consists of a sequence of b -bit blocks, $P_1, P_2, \dots, P_N$; the corresponding sequence of ciphertext blocks is $C_1, C_2, \dots, C_N$. We can define ECB mode as follows.

$$\text{ECB } C_j = E(K, P_j) \quad j = 1, \dots, N \quad P_j = D(K, C_j) \quad j = 1, \dots, N$$

Figure 6.3 Electronic Codebook (ECB) Mode

Electronic Codebook Mode (ECB)

- The simplest mode .
- Ideal for a **short amount of data**, such as an **encryption key**.
 - if you want to transmit a DES or AES key securely, ECB is the appropriate mode to use.
- If the same b-bit block of plaintext appears more than once in the message, it always produces the same ciphertext.
- For **lengthy messages**, ECB mode **may not be secure**. If the message is highly structured, it may be possible for a cryptanalyst to exploit these regularities.
 - **Ex:** if it is known that the message always starts out with certain predefined fields, then the cryptanalyst may have a number of known plaintext– ciphertext pairs to work with.
 - message has **repetitive elements** with a period of repetition a multiple of b bits, then these elements can be identified by the analyst...

Criteria and properties for evaluating and constructing block cipher modes of operation that are superior to ECB:



- **Overhead**

- additional operations for encryption and decryption operation

- **Error recovery**

- an error in **i th ciphertext block is inherited** by only a few plaintext blocks after which the mode resynchronizes

- **Error propagation**

- an error in **i th ciphertext block is inherited by i th and all subsequent plaintext blocks.**(in the transmission of a ciphertext, not a computational error in encryption of a plaintext)

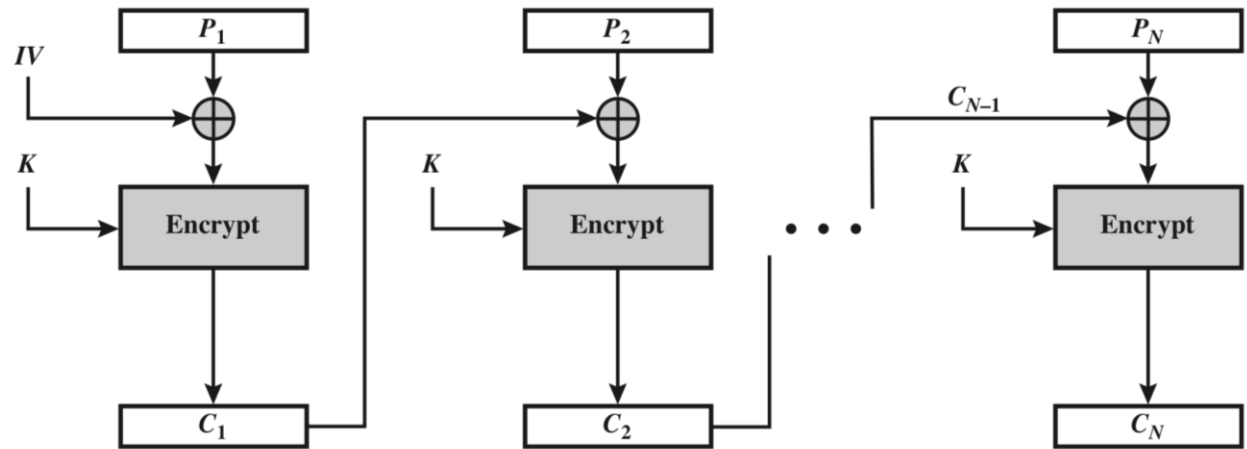
- **Diffusion**

- lack of order or predictability; gradual decline into disorder

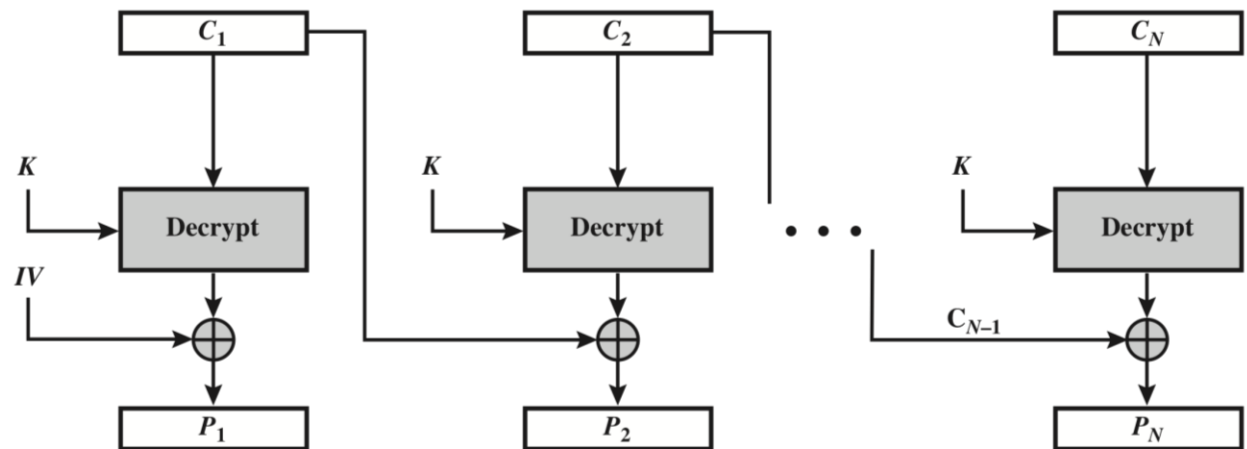
- **Security**

- Ciphertext blocks leak information about the plaintext blocks

Cipher Block Chaining (CBC)



(a) Encryption



(b) Decryption

(IV):
initialization
vector

Figure 6.4 Cipher Block Chaining (CBC) Mode

Cipher Block Chaining (CBC)

- CBC requires that the last block be **padded** b bits if it is a **partial block**.
- IV is a data block that is same size as cipher block.
- IV must be known to both sender and receiver but be **unpredictable** by a third party. It is random.
- For **maximum security**, IV should be **protected** against unauthorized changes (sending it **using ECB encryption**).
- **Choice of IV**, SP800-38A recommends **two possible methods**:
 1. apply the **encryption function**, under the same key that is used for the encryption of the plaintext, to **a nonce**. The nonce must be a **data block that is unique** to each execution of the encryption operation. **Ex**: the nonce may be a counter, a timestamp, or a message number.
 2. Or **generate a random data** block using a random number generator.
- Because **chaining mechanism**, **CBC** is an appropriate mode for **encrypting messages of length greater than b bits**.
- **CBC achieves confidentiality** and can be used for **authentication**.

Cipher Feedback Mode

- For AES, DES, or any block cipher, encryption is performed on a block of b bits
 - In the case of DES $b = 64$
 - In the case of AES $b = 128$
- A stream cipher eliminates the need to pad a message to be an integral number of blocks.

There are three modes that make it possible to convert a block cipher into a stream cipher:

Cipher
feedback
(CFB) mode

Output
feedback
(OFB) mode

Counter
(CTR) mode

s-bit Cipher Feedback (CFB) Mode

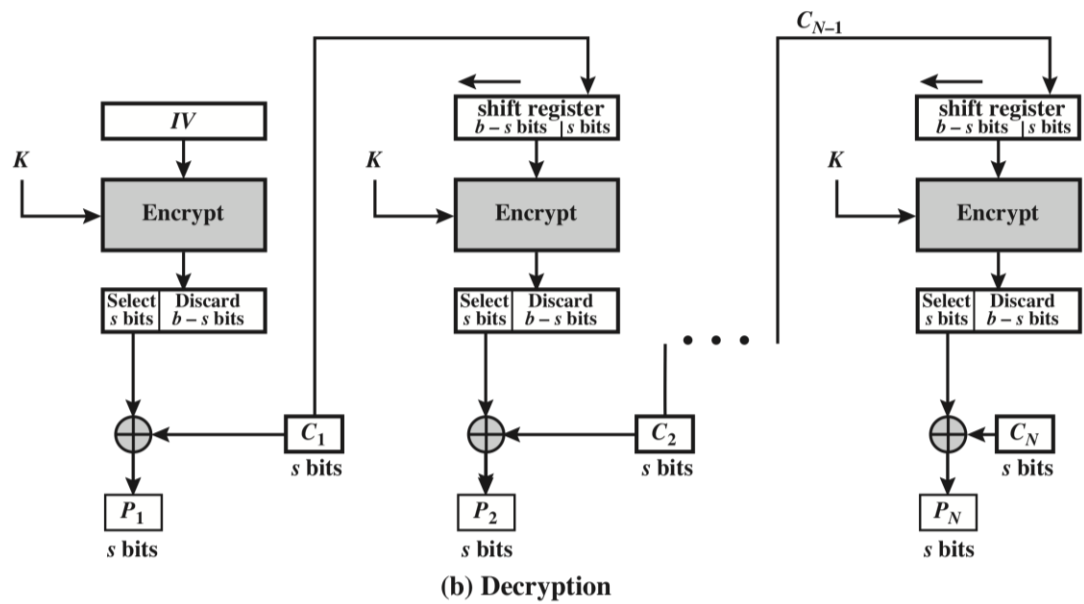
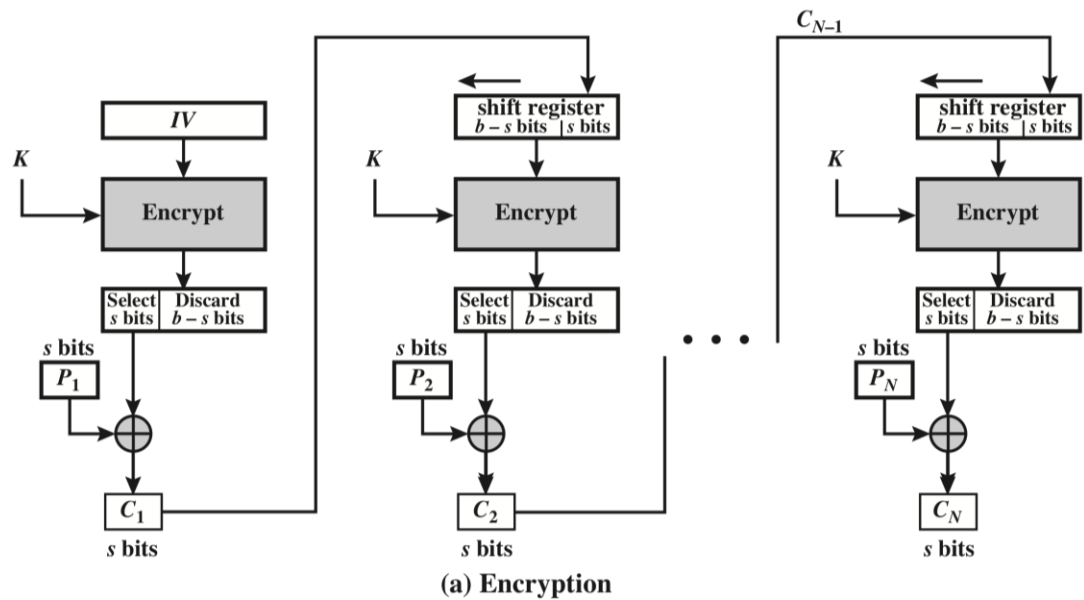
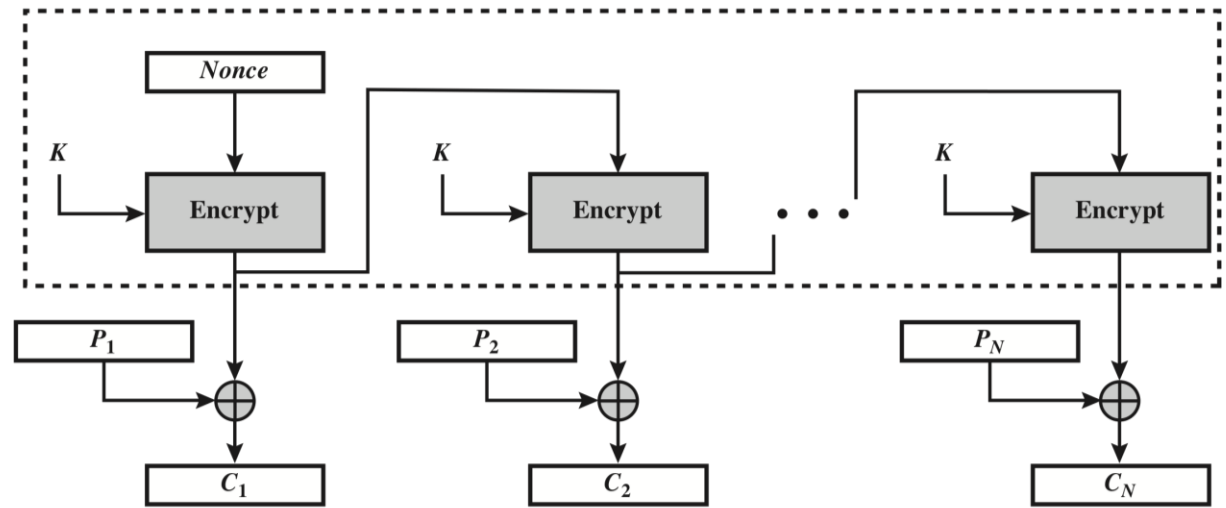


Figure 6.5 s-bit Cipher Feedback (CFB) Mode

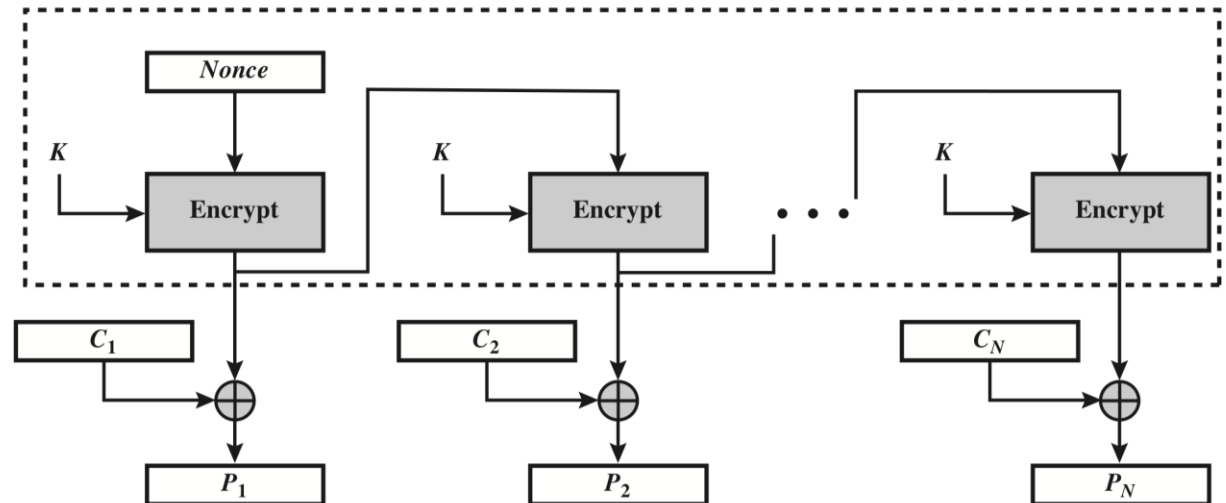
s-bit Cipher Feedback (CFB) Mode

- a common value is $s = 8$
- For **decryption**, the **encryption function is used**, not the decryption function.
- In **CFB encryption**, like CBC encryption, the input block to each forward Cipher function (except the first) depends on the result of the previous forward Cipher function; **multiple forward cipher operations cannot be performed in parallel**.
- In **CFB decryption**, the required forward cipher operations **can be performed in parallel** if the input blocks are first constructed (in series) from the IV and the ciphertext.

Output Feedback (OFB) Mode



(a) Encryption



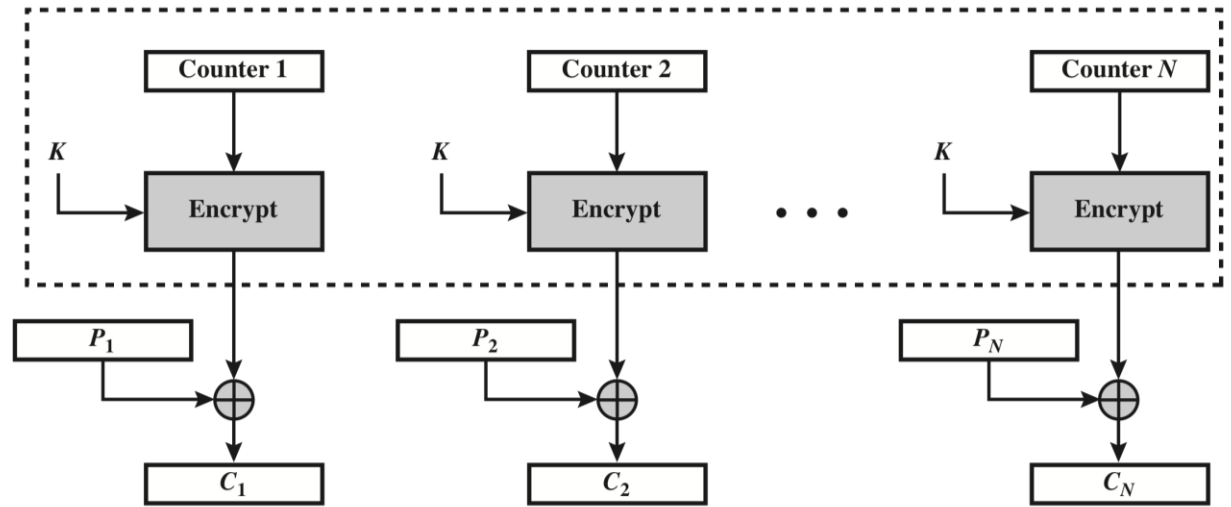
(b) Decryption

Figure 6.6 Output Feedback (OFB) Mode

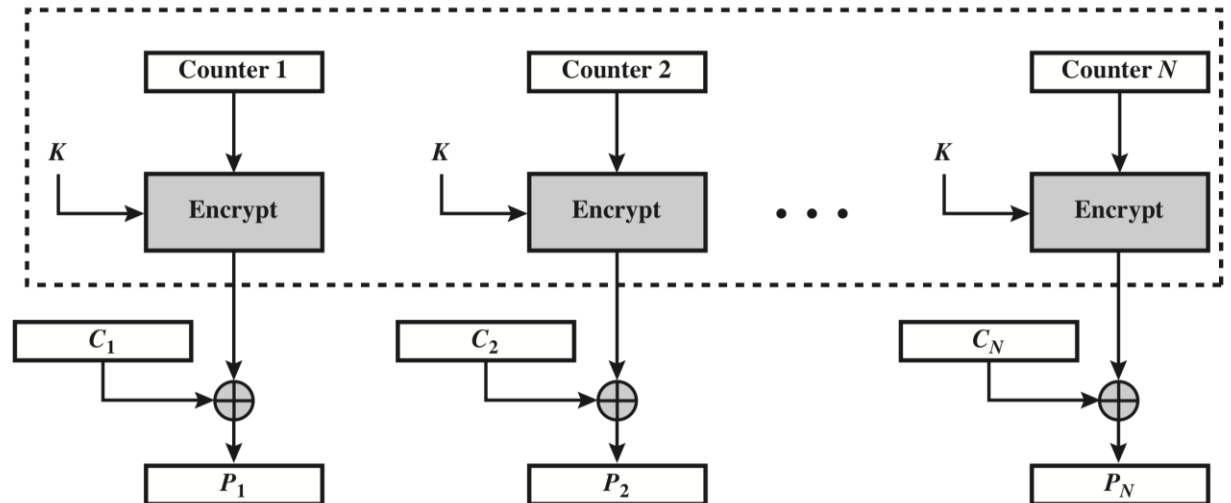
Output Feedback (OFB) Mode

- OFB mode is similar in structure to CFB.
- **OFB operates on full blocks of plaintext and ciphertext, whereas CFB operates on an s-bit subset.**
- **IV must be unique to each execution of the encryption operation.**
- **One advantage:**
 - **bit errors in transmission do not propagate.**
 - **Ex, if a bit error occurs in C_1 , only the recovered value of P_1 is affected; subsequent plaintext units are not corrupted.**
- **disadvantage of OFB:**
 - **It is more vulnerable to a message stream modification attack than is CFB.**
- **OFB encrypts plaintext a full block at a time, (block of 64 or 128 bits).**

Counter (CTR) Mode



(a) Encryption



(b) Decryption

Figure 6.7 Counter (CTR) Mode

Counter (CTR) Mode

- **CTR mode is used recently with applications: ATM (asynchronous transfer mode) network security and IP sec (IP security).**
- **There is no chaining.**
- **A counter equal to the plaintext block size is used.**
- **The counter value must be different for each plaintext block that is encrypted.**
- **It is initialized to some value and then incremented by 1 for each subsequent block.**
- **The initial counter value must be made available for decryption.**



Advantages of CTR

- **Hardware efficiency**

- encryption (or decryption) can be done in parallel on multiple blocks of plaintext or ciphertext.
- Throughput is only limited by the amount of parallelism achieved.

- **Software efficiency**

- parallel execution, processors that support parallel features, such as aggressive pipelining, multiple instruction dispatch per clock cycle, a large number of registers, and SIMD instructions, can be **effectively utilized**.

- **Preprocessing**

- When the plaintext or ciphertext input is presented, then the only computation is a series of XORs. Such a strategy greatly enhances throughput.

- **Random access**

- i th block (plaintext/ciphertext) can be processed in random-access fashion. the random access feature is attractive

- **Provable security**: CTR is at least as secure as the other modes discussed.

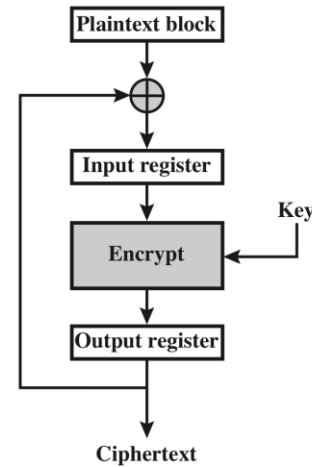
- **Simplicity**

- It requires the implementation of encryption algorithm and not decryption algorithm.

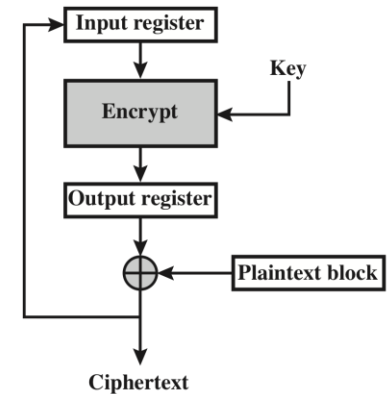
Feedback

Characteristics of Modes of Operation

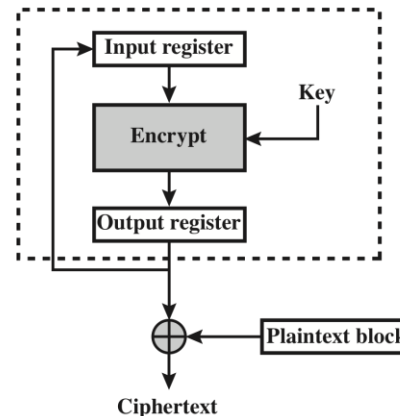
- To highlight the **feedback mechanism**, consider the encryption function as taking input from an input register whose length equals the encryption block length and with output stored in an output register. The input register is update one block at a time by the feedback mechanism.
- After each update, the encryption algorithm is executed, producing a result in the output register. Meanwhile, a block of plaintext is accessed.
- Note that both OFB and CTR produce output that is independent of both the plaintext and the ciphertext (natural candidates for stream ciphers that encrypt plaintext by XOR one full block at a time).



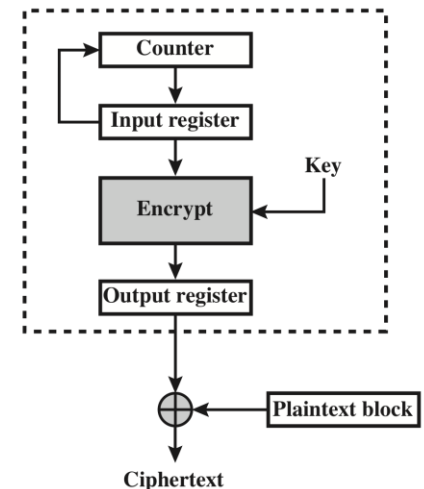
(a) Cipher block chaining (CBC) mode



(b) Cipher feedback (CFB) mode



(c) Output feedback (OFB) mode



(d) Counter (CTR) mode

Figure 6.8 Feedback Characteristic of Modes of Operation