Five Modes of Operation

- Electronic codebook mode (ECB)
- Cipher block chaining mode (CBC)
- Output feedback mode (OFB)
- Cipher feedback mode (CFB)
- Counter mode (CTR)

Electronic Code Book (ECB)

- The plaintext is broken into P_1, P_2, P_3, ...
- Each block is encrypted independently:

$$C_i = E_K(P_i)$$

- Each block is a value,which is substituted,like a code book hence the name

Remarks on ECB

- Strength: it’s simple.
- Weakness:
  - Repetitive information contained in the plaintext may show in the ciphertext, if aligned with blocks.
  - If the same message (e.g., an SSN) is encrypted (with the same key) and sent twice, their ciphertexts are the same.
- Typical application: secure transmission of short pieces of information (e.g. a temporary encryption key)

Cipher Block Chaining (CBC)

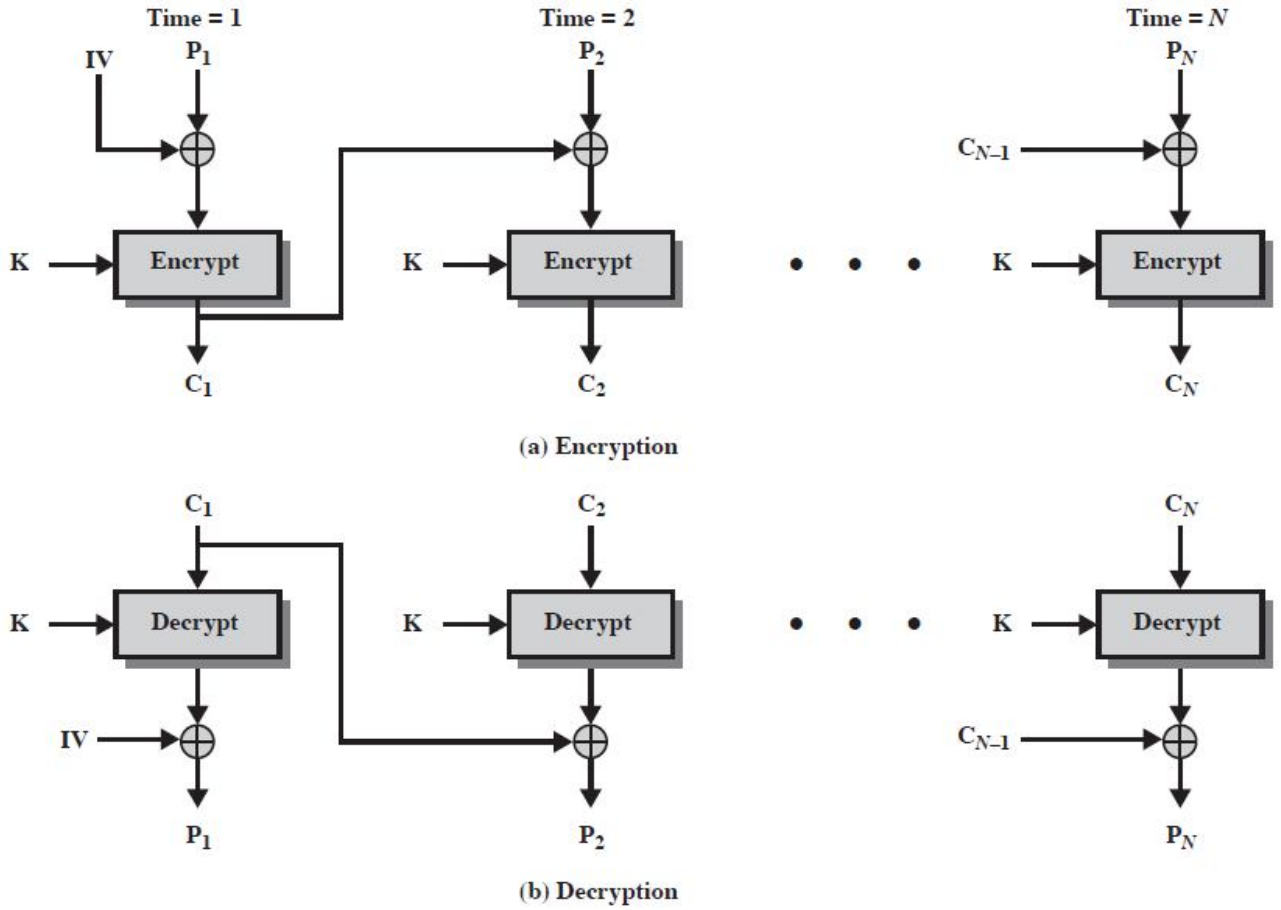
- The plaintext is broken into blocks: $P_1,\ P_2,\ P_3,\ \ldots$
- Each plaintext block is XORed $\left(\text{chained}\right)$ with the previous ciphertext block before encryption (hence the name):

$$C_i = \mathrm{E}_K\left(C_{i-1} \oplus P_i\right)$$

$$C_0 = \mathrm{IV}$$

- Use an Initial Vector $\left(\mathrm{IV}\right)$ to start the process.
- Decryption : $P_i = C_{i-1} \oplus \mathrm{D}_K(C_i)$
- Application : general block-oriented transmission.

Cipher Block Chaining (CBC)



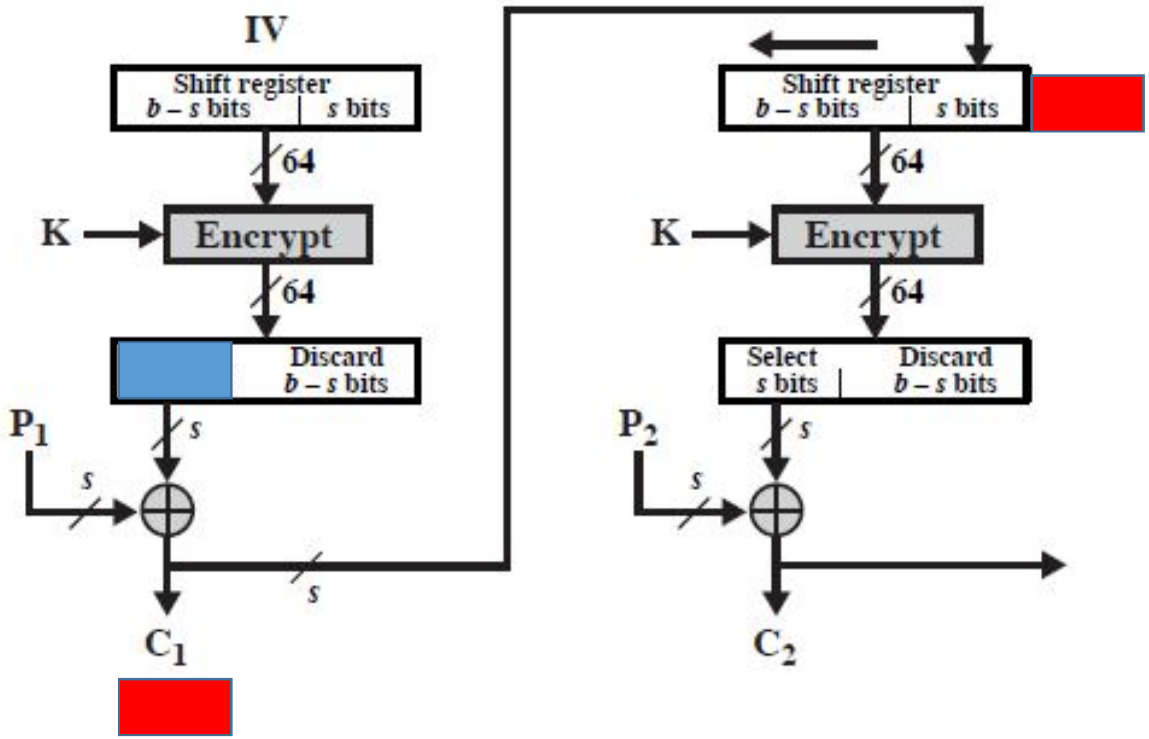
Remarks on CBC

- The encryption of a block depends on the current and **all** blocks before it.
- So, repeated plaintext blocks are encrypted differently.
- Initialization Vector (IV)
  - Must be known to both the sender & receiver
  - Typically, IV is either a fixed value or is sent encrypted in ECB mode before the rest of ciphertext.

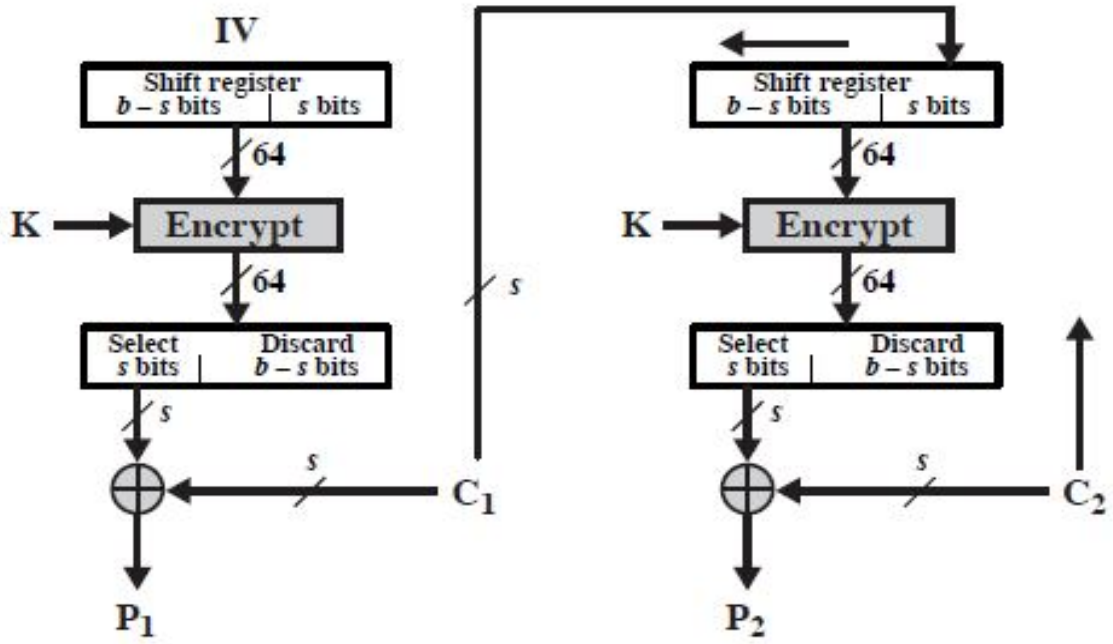
Cipher Feedback (CFB) Mode

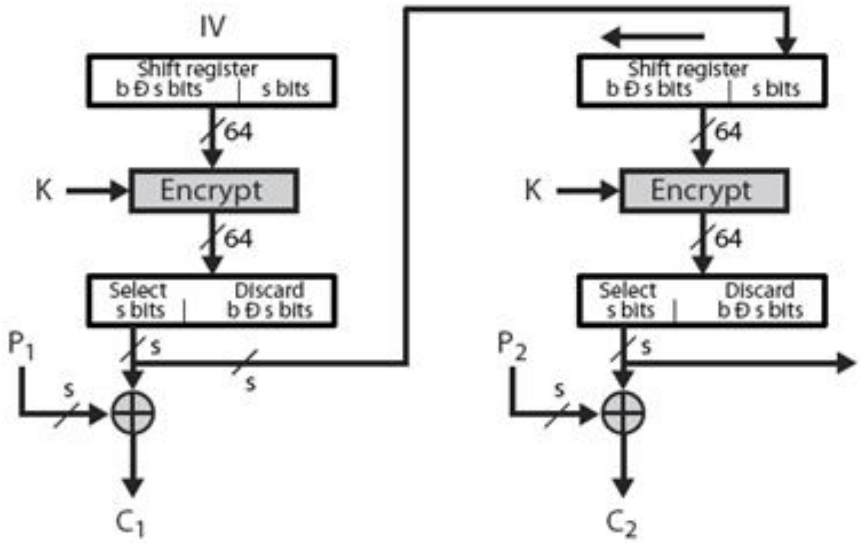
- The plaintext is a sequence of segments of s bits (where $s \leq$ block-size): $P_1, P_2, P_3, P_4, \ldots$
- Encryption is used to generate a sequence of keys, each of s bits: $K_1, K_2, K_3, K_4, \ldots$
- The ciphertext is $C_1, C_2, C_3, C_4, \ldots$, where $C_i = P_i \oplus K_i$
- How to generate the key stream?

Encryption in CFB Mode



Decryption in CFB Mode





Output Feedback(OFB)

Counter Mode (CTR)

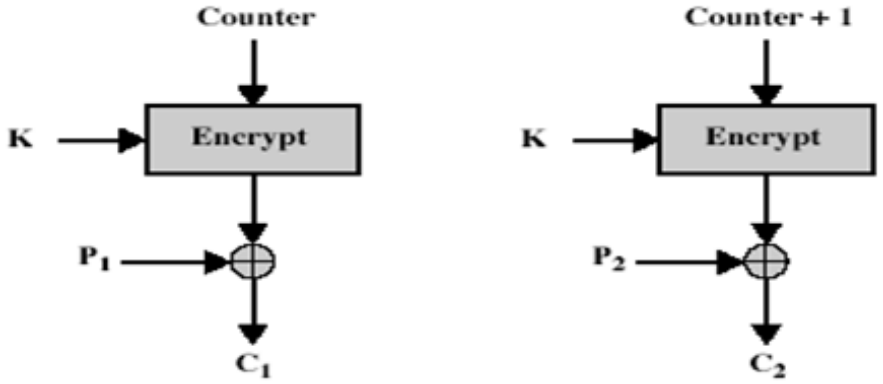
- Plaintext blocks: $p_1, p_2, p_3, \ldots$
- Key: k
- Basic idea: construct key stream $k_1, k_2, k_3, \ldots$
- Encryption:

$T_1 = IV$ (random)

$T_i = IV + i - 1$

$C_i = P_i \eth E_K(T_i)$

$C = (IV, C_1, C_2, C_3, \ldots)$



Remark on CTR

- Strengthes:
  - Needs only the encryption algorithm
  - Fast encryption/decryption; blocks can be processed (encrypted or decrypted) in parallel; good for high speed links
  - Random access to encrypted data blocks
- IV should not be reused.