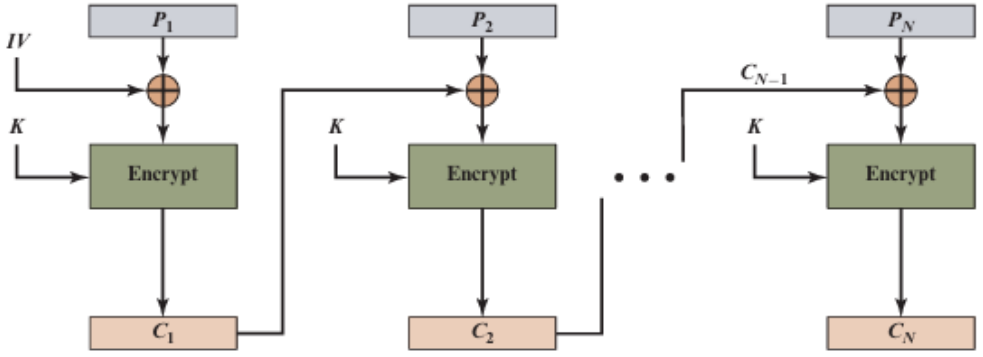
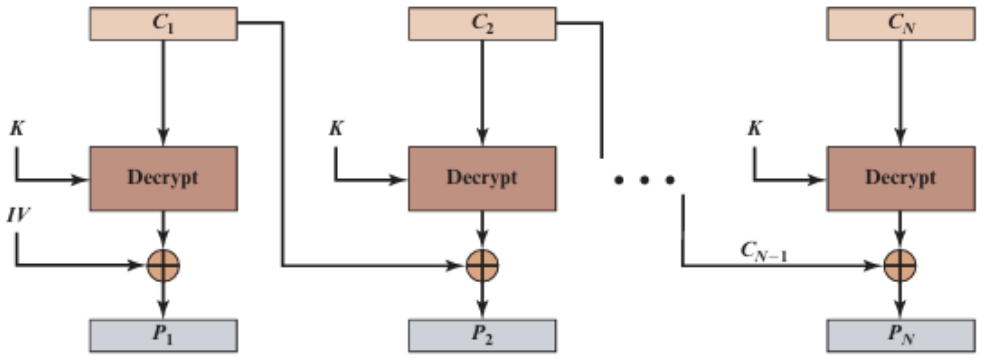
Course: Data Security
Lecturer: Dr. Mahmoud Yehia
TA: Eng. Eslam Osama
Block Cipher Operation Modes

# Questions)




(a) Encryption




(b) Decryption

Figure 7.4 Cipher Block Chaining (CBC) Mode

**(1)** With the ECB mode, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC mode, this error propagates. For example, an error in the transmitted C1 (Figure 7.4) obviously corrupts P1 and P2.

**a.** Are any blocks beyond P2 affected?

**b.** Suppose that there is a bit error in the source version of P1. Through how many ciphertext blocks is this error propagated? What is the effect at the receiver?

**Ans)**

**a. No. For example, suppose C1 is corrupted. The output block P3 depends only on the input blocks C2 and C3.**

**b. An error in P1 affects C1. But since C1 is input to the calculation of C2, C2 is affected. This effect carries through indefinitely, so that all ciphertext blocks are affected. However, at the receiving end, the decryption algorithm restores the correct plaintext for blocks except the one in error. You can show this by writing out the equations for the decryption. Therefore, the error only effects the corresponding decrypted plaintext block.**

**(2)** Why is the ECB mode not secured for encrypting large amounts of data or structured data?

**Ans)**

**ECB mode is not secure because it always encrypts identical plaintext blocks into identical ciphertext blocks. So, if the same word or pattern appears more than once in the data (like repeated words or shapes in an image), the ciphertext will show the same repeated patterns.**

**This makes it easy for an attacker to notice these patterns and possibly guess parts of the message or find out how the data is structured. Since ECB uses the same key for every block, this repetition becomes a big security risk.**

**(3)** Why should the initialization vector be protected against unauthorized use in the CBC mode of encryption?

**Ans)**

**CBC uses an IV to prevent having the same plaintext result in the same (guessable) ciphertext. It's important that the IV is random and unique. Otherwise, attackers might be able to guess the ciphertext and easily decrypt the data.**

**(4)** If a block of ciphertext gets corrupted during transmission in the OFB mode, how does it affect the decryption?

**Ans)**

**In OFB mode, if one block of the ciphertext gets damaged during transmission, only the matching block of the decrypted message will be wrong. The rest of the message will still be fine because OFB creates a separate keystream that doesn’t depend on the ciphertext itself, so the error doesn’t spread to other blocks.**

**(5)** Is it possible to parallelize encryption in the CFB mode? What about decryption?

**Ans)**

**In CFB mode, encryption cannot be easily parallelized because each block depends on the previous ciphertext block — you have to wait for one block to be encrypted before moving to the next.**

**However, decryption in CFB mode can be parallelized because each ciphertext block is known (already received), so multiple blocks can be decrypted at the same time**

**Course: Data Security**
**Lecturer: Dr. Mahmoud Yehia**
**TA: Eng. Eslam Osama**
**Block Cipher Operation Modes**

**(6)** What are the advantages of CTR mode over the CBC mode? Explain in terms of the implementation benefits in software, hardware, and decryption throughput?

**Ans)**

- **Parallel Processing:**
  - CTR mode allows both encryption and decryption blocks to be processed in parallel, because each block uses a counter, not the previous block's output.
  - CBC mode, on the other hand, requires sequential processing, especially during encryption, because each block depends on the one before it.

- **Faster Decryption (Higher Throughput):**
  - Since CTR decryption doesn't depend on earlier blocks, it can be done much faster — especially when multiple processors or threads are used.
  - CBC decryption is slower, as each block needs the previous ciphertext block.

- **Simpler Hardware and Software Design:**
  - CTR mode only uses the encryption function for both encryption and decryption, making it easier to implement in both hardware and software.
  - CBC needs both encryption and decryption functions, which adds complexity.

- **Preprocessing (Efficiency):**
  - In CTR mode, the keystream (from encrypting the counters) can be precomputed ahead of time, even before the actual data is ready — which boosts speed.
  - CBC can't do that, as it relies on real-time data.