1. ECB (Electronic Codebook) Mode:

In ECB mode, the plaintext is divided into blocks, and each block is encrypted independently with the same key.

- Step 1: Divide the plaintext into two 8-bit blocks.
    - Plaintext: A8B9 (in Hex) → A8 (LT) || B9 (RT)
- Step 2: Use the encryption function (LC = LK XOR RT and RC = RK XOR LT) with the key C5.
    - Key: C5 (in Hex) → C5 in binary = 11000101
    - First block: LT = A8 (in Hex) → 10101000, RT = B9 (in Hex) → 10111001.
- LC Calculation: LC = LK XOR RT = 11000101 XOR 10111001 = 01111100 (in binary) = 7C (in Hex).
- RC Calculation: RC = RK XOR LT = 11000101 XOR 10101000 = 01101101 (in binary) = 6D (in Hex).
- Encrypted output: 7C6D.

2. CBC (Cipher Block Chaining) Mode:

In CBC, the previous ciphertext block is XORed with the plaintext block before encryption. We start with the initialization vector (IV).

- Step 1: XOR the IV with the first block of plaintext.
    - IV = A9 (in Hex) → 10101001 (in binary)
    - First block of plaintext: A8 (in Hex) → 10101000 (in binary)
    - XOR: 10101001 XOR 10101000 = 00000001 (in binary) = 01 (in Hex).
- Step 2: Encrypt the result (01) with the key C5.
    - Key: C5 (in Hex) → 11000101 (in binary)
    - Plaintext after XOR: 01 (in Hex) → 00000001 (in binary)
- LC Calculation: LC = LK XOR RT = 11000101 XOR 00000001 = 11000100 (in binary) = C4 (in Hex).
- RC Calculation: RC = RK XOR LT = 11000101 XOR 00000001 = 11000100 (in binary) = C4 (in Hex).
- Encrypted output: C4C4.

3. OFB (Output Feedback) Mode:

In OFB mode, the encryption function is applied to the IV, and the result is XORed with the plaintext.

- Step 1: Apply encryption to IV with key C5.

    - IV = A9 (in Hex) → 10101001 (in binary)
    - Key: C5 (in Hex) → 11000101 (in binary)
    - Use the encryption function: LC = LK XOR RT and RC = RK XOR LT.
        - LC Calculation: LC = 11000101 XOR 10101001 = 01101100 (in binary) = 6C (in Hex).
- Step 2: XOR the result (6C) with the plaintext (A8).
    - Plaintext: A8 (in Hex) → 10101000 (in binary)
    - XOR: 10101000 XOR 01101100 = 11000100 (in binary) = C4 (in Hex).
- Encrypted output: C4.

4. CFB (Cipher Feedback) Mode:

In CFB mode, the previous ciphertext block is shifted and XORed with the current plaintext block.

- Step 1: XOR the IV with the first block of plaintext.
    - IV = A9 (in Hex) → 10101001 (in binary)
    - Plaintext: A8 (in Hex) → 10101000 (in binary)
    - XOR: 10101001 XOR 10101000 = 00000001 (in binary) = 01 (in Hex).
- Step 2: XOR the result (01) with the plaintext (A8).
    - XOR: 00000001 XOR 10101000 = 10101001 (in binary) = A9 (in Hex).
- Encrypted output: A9.

5. CTR (Counter) Mode:

In CTR mode, the counter value is incremented after each block is encrypted, and the result is XORed with the plaintext.

- Step 1: The stream of counter bits starts from 0001 (in binary).
    - The counter is 0001 (in binary) → 01 (in Hex).
- Step 2: XOR the counter with the plaintext.
    - Counter = 01 (in Hex) → 00000001 (in binary)
    - Plaintext = A8 (in Hex) → 10101000 (in binary)
    - XOR: 00000001 XOR 10101000 = 10101001 (in binary) = A9 (in Hex).
- Encrypted output: A9.