ECB

Full Form - Electronic Codebook

The simplest of the encryption modes is the electronic codebook (ECB) mode. The message is divided into blocks, and each block is encrypted separately.Thus, it is possible to encrypt and decrypt by using many threads simultaneously. However, in this mode the created ciphertext is not blurred.

Formula - $Yi = F(Pi, K)$

Advantages -

Disadvantages -

CBC

Full Form - Cipher Block Chaining

In this mode we add XOR of each plaintext block to the ciphertext block that was previously produced. The result is then encrypted using the cipher algorithm in the usual way. As a result, every subsequent ciphertext block depends on the previous one. The first plaintext block is added XOR to a random initialization vector (commonly referred to as IV). The vector has the same size as a plaintext block.

Formula - $Yi = Pi \wedge Ci-1$

Advantages -

Disadvantages -

PCBC

Full Form - Propagating Cipher Block Chaining

The propagating cipher block chaining or plaintext cipher-block chaining mode was designed to cause small changes in the ciphertext to propagate indefinitely when decrypting, as well as when encrypting. In PCBC mode, each block of plaintext is XORed with both the previous plaintext block and the previous ciphertext block before being encrypted. Like with CBC mode, an initialization vector is used in the first block.

Formula - $Y_i = P_i \text{ ^ } (C_{i-1} \text{ ^ } P_{i-1})$

Advantages -

Disadvantages -

CFB

Full Form - Cipher Feedback

The CFB mode of operation allows the block encryptor to be used as a stream cipher.First, CFB will encrypt the IV, then it will xor with plaintext block to get ciphertext. Then we will encrypt the encryption result to xor the plaintext. Because this mode will not encrypt plaintext directly, it just uses the ciphertext to xor with the plaintext to get the ciphertext. So in this mode, it doesn't need to pad data.And it could decrypt data in parallel, not encryption. This mode is similar to the CBC, so if there is a broken block, it will affect all following block.

Formula - $Y_i = C_{i-1}$

Advantages -

Disadvantages -

OFB

Full Form - Output Feedback

The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error-correcting codes to function normally even when applied before encryption.

Formula - $Y_i = F(Y_{i-1}, K)$
$Y_0 = F(IV, K)$

Advantages -

Disadvantages -

CTR

Full Form - Counter Mode

Using the CTR mode makes block cipher way of working similar to a stream cipher. As in the OFB mode, keystream bits are created regardless of content of encrypting data blocks. In this mode, subsequent values of an increasing counter are added to a nonce value and the results are encrypted as usual. The nonce plays the same role as initialization vectors in the previous modes.

Formula - Yi = F(IV + g(i), K)
IV = token()

Advantages -

Disadvantages -