BLOCK CIPHER MODE OF OPERATION (Part 1)

NOTE 1:

One of the main issues with block ciphers is that **they only allow you to encrypt messages the same size as their block length**. If you're using **TEA**, which has a block size of 64 bits, to encrypt a 65 bit message, you need a way to define how the second block should be encrypted.

NOTE 2:

Tiny Encryption Algorithm (TEA)

The Tiny Encryption Algorithm is a Feistel type cipher (Feistel, 1973) that uses operations from mixed (orthogonal) algebraic groups. A dual shift causes all bits of the data and key to be mixed repeatedly. The key schedule algorithm is simple; the 128-bit key K is split into four 32-bit blocks K = (K[0], K[1], K[2], K[3]). TEA seems to be highly resistant to differential cryptanalysis and achieves complete diffusion (where a one bit difference in the plaintext will cause approximately 32 bit differences in the cipher text). Time performance on a workstation is very impressive.

The block cipher operation modes are divided into five essential parts and These modes of operation help in enhancing the algorithm such that there could be a wide application range that could be adapted to use the encryption of block cipher.

These modes are:

1. Electronic Code Book Mode
2. Cipher Block Chaining Mode
3. Cipher Feedback Mode
4. Output Feedback Mode
5. Counter Mode

Several block cipher modes of operation exist with varying advantages and disadvantages

Table 6.1 Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 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 64 bits of plaintext and the preceding 64 bits 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