Cryptography And Network Security
(Lec 28: Modes of Operation of Block Ciphers)

Maniteja Tallapally

26-Oct-2020

1 Block Ciphers: Introduction

A block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks, the length being block size. It uses an unvarying encryption i.e a symmetric key. Block ciphers are key components in the design of many cryptographic protocols and are widely used to implement the encryption of large amounts of data. There are several modes of operation of block ciphers such as

- Electronic Code Book
- Cipher Block Chaining
- Output Feedback Mode
- Counter Mode etc

Among the others, Electronic Code Book(ECB) and Cipher Block Chaining(CBC) are primarily used.

1.1 Electronic Code Book

In ECB mode,a message is first split into blocks(each of size "block size") and then each block is encrypted and decrypted independently. This method is insecure because equal plaintext blocks will always generate equal ciphertext blocks (symmetric key), so patterns in the plaintext message become evident in the ciphertext output, which makes it easier to crack the key.

1.1.1 Advantages of using ECB

- Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption.

• Simple way of block cipher.

• An Error in one block is localized to that single block. The other blocks are not affected.

1.1.2 Disadvantages of using ECB

• Same block always encrypts to the same ciphertext, so patterns in the plaintext message become evident in the ciphertext output, making it utterly insecure.

1.2 Cipher Block Chaining

Cipher Block Chaining is an improvement on the ECB, compensating the security requirement with a little more complexity in encryption process.
In This mode, a previous cipher block is an input to the next encryption algorithm after XORing with the original plaintext block. To put it simply a cipher block is produced by encrypting a XOR output of previous cipher block and present plaintext block. This chaining introduces a complexity which nullifies the pattern recognition of same plaintext, since a text is encrypted with a common key and a varying vector i.e previous cipher block.
Here, for the very first block, there is no previous cipher block. For that, an initialization vector(IV) is used. As the secrecy is to the key, the integrity is to the IV.

1.2.1 Advantages of using CBC

• Works well for input of multiple block size.

• Well protected and secure.

• More immune to cryptanalysis than ECB.

• A single bit error in one block doesn't reflect in all blocks(self recovery).

1.2.2 Disadvantages of using CBC

• Parallel encryption is not possible since every encryption requires previous ciphertext.

• Random access files cannot be encrypted.

• IV Based attacks.