Scribe: Cryptography and Network Security

Ashish Kumar Singh

21-Oct-2020

1 Introduction

Mode of Operation of Block Cipher :
The Encryption of plain-text in block cipher takes place in smaller block.
When we have large volumes of data, and when we encrypt it using block ciphers, then there will be a possibility of using same secret key bits for encrypting the plain-text part.
So, the adversary will be able to access some information by knowing the distribution of the message part, even if they won't be able to decrypt the complete plain-text.

2 Electronic Code Book (ECB)

- Naive use of block cipher ie., Simplest Encryption Mode.
- Each block is encrypted and decrypted separately.
- One drawback is that same plaintext gets converted to the same cipher text.
- Single bit error transmission only affect the corresponding block.

2.1 Advantage

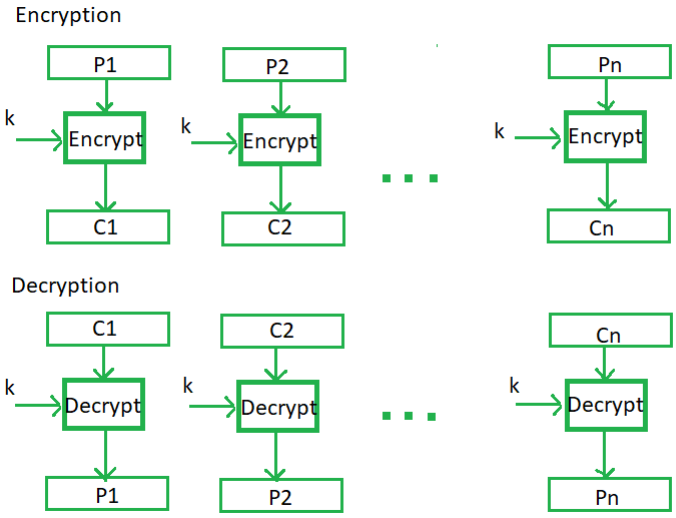
- Simple way of block cipher.
- Simultaneously encryption/decryption of blocks makes it faster.

2.2 Disadvantage

- Since there is a direct mapping between plaintext and ciphertext, there is a high possibility of finding it out using cryptanalysis.
- ECB can leak secret for the low entropy plaintext space.

2.3 CipherText Stealing

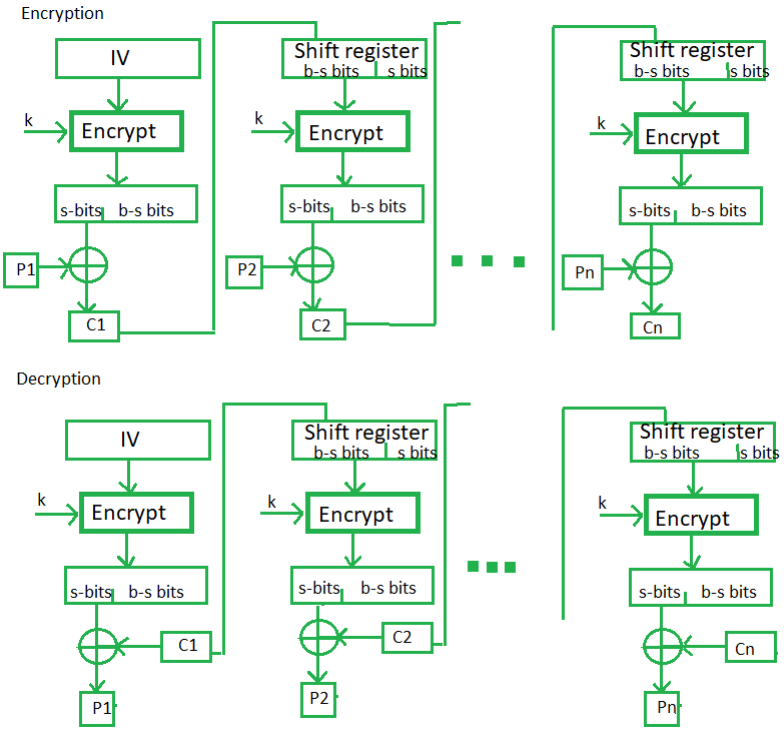
- The message encrypted using ECB mode should be expanded to size equal to the integral multiple of the size of one block using padding.
- CipherText Stealing technique is used, in which we pad the last (n-m) bits from the second last cipher block to the last block's plaintext. Then , we encrypt the last block. ('n' is the block size and 'm' is the number of bits present in the last block ,st. n¿m). Then, Swipe last and second last block.
- Encryption :
  X=$E_k(P_{N-1}) --> C_{N-1} = head_m(X)$
  Y=$P_N||tail_{n-m}(X) --> C_N = E_k(Y)$
- Decryption :
  $Y = D_K(C_N) --> P_N = head_m(Y)$
  $X = C_{N-1}||tail_{n-m}(Y) --> P_{N-1} = D_K(Y)$



3 Cipher Block Chaining

- Cipher block chaining or CBC is a development made in the ECB because the ECB puts at risk some security requirements. In CBC, the previous cipher block is provided as an integration into the next XOR encryption algorithm with a real plaintext block block. Briefly here, the cipher block is generated by encrypting the XOR output of the previous block and the current display block.
- Solves the problem of mapping same plaintext to same ciphertext.

- For the first block, Initialization vector (IV) is used, which is not secret(means IV is known by everyone).
- In this, we encrypt the blocks serially.



3.1 Error Propagation

- If there is some error in cipherText block C_j during transmission , then only two blocks P_j,P_{j+1}, will get affected while doing decryption.
- Entire plaintext P_j is wrong, and there will be a single bitb error in the plaintext P_{j+1}

3.2 Advantage :

- CBC works well for input greater than n bits.
- Better resistive nature towards cryptanalsis than ECB. CBC is a good authentication mechanism.

3.3 Disadvantage :

- Parallel encryption is not possible since every encryption requires previous cipher.
- random Access file can't be encrypted.
- Same messages encrypted to same cipher text iff IV is same.
- Because of chaining, the attacker can add some ciphertext blocks at the end.

4 Conclusion

Electronic Cipher Book mode of operation is a simple Block cipher method. It maps the same plaintext block to the same ciphertext block. To resolve this problem, we came up with another mode of operation , which is Cipher Block Chaining (CBC) , in which every block of plaintext is encrypted will be encrypted using the previous block of cipher text. In this , every identical block also encrypted to the different cipherText block. This Mode of opertaion also has some drawbacks, which results in the formation of some other modes of operations.