Hacettepe University

Department of Computer Engineering

BBM 465 Information Security Laboratory

Assignment-1 Block Cipher

Prepared by

21527084 Anıl Helvacı
21591223 Ömer Faruk Boztaş

November 4, 2019

INTRODUCTION

In this assignment, we implemented encryption/decryption tool for block ciphers (AES,DES). The different modes of operation of a block cipher used in this program. Interestingly, the different modes result in different properties being achieved which add to the security of the underlying block cipher. A block cipher processes the data blocks of fixed size. Usually, the size of a message is larger than the block size. Hence, the long message is divided into a series of sequential message blocks, and the cipher operates on these blocks one at a time. In this assignment, AES and DES encryption/decryption methods were used together with CBC, OFB and CTR techniques.

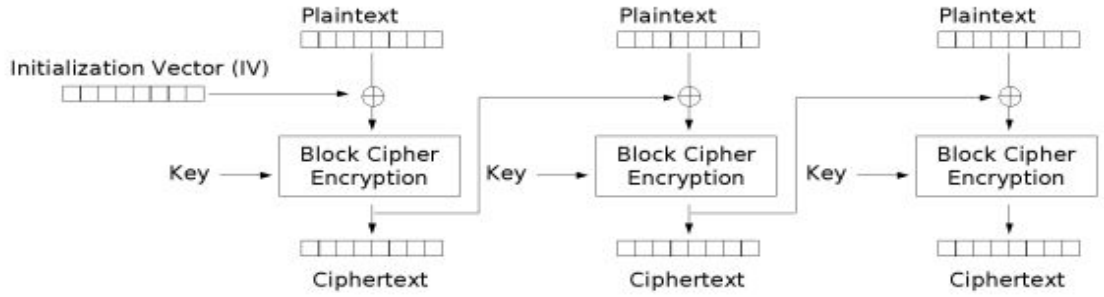
AIM

Our goal is to be able to run different encryption algorithms and its modes by invoking prebuilt ECB mode. It seems like a puzzle.

Messages are encrypted using AES and DES. These algorithms use three encryption modes (CBC, OFB, CTR). The program has been developed in accordance with object oriented programming techniques in Java.

DESIGN

CBC Design



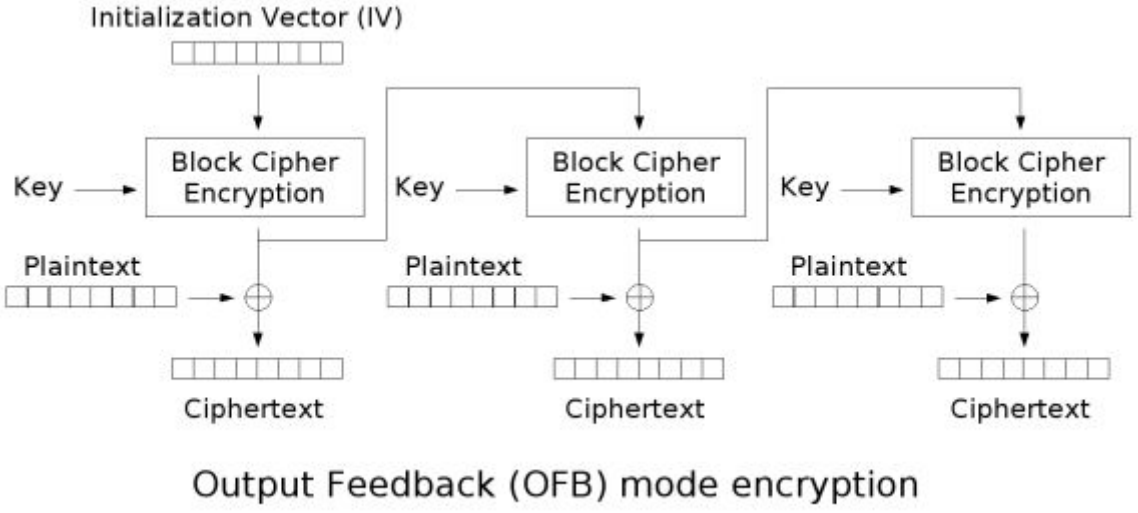
Cipher Block Chaining (CBC) mode encryption

The possibility of finding a pattern was increased because ECB mode encrypts each block of plaintext separately into the same encryption algorithm. Confusion must be increased. When the hacker looked at the ciphertext, he shouldn't have seen the same plaintext block produce the same ciphertext block. For this reason CBC mode is derived. Plaintext would be xorized with one vector at a time, and this value would be encrypted. As a result, no pattern could be captured in the ciphertext blocks. The vector to xor; IV for plaintext-block-1 , other vectors are the encrypted version of the previous blocks. Ciphertext-block-1 for plaintext-block-2 and etc. (the IV must be already shared between the message sender and receiver.) For IV and block size; AES uses 16 bytes, DES uses 8 bytes.

In CBC mode, there is a failure(while sending) in ciphertext block n, the plaintext block n and plaintext block n+1 will disrupted. The failure in IV(while sending) affects only first block while decryption.

There is a time problem in CBC, because blocks are waiting for previous block to encrypt. Because of the waiting time, it is not a perfect solution.

OFB Design



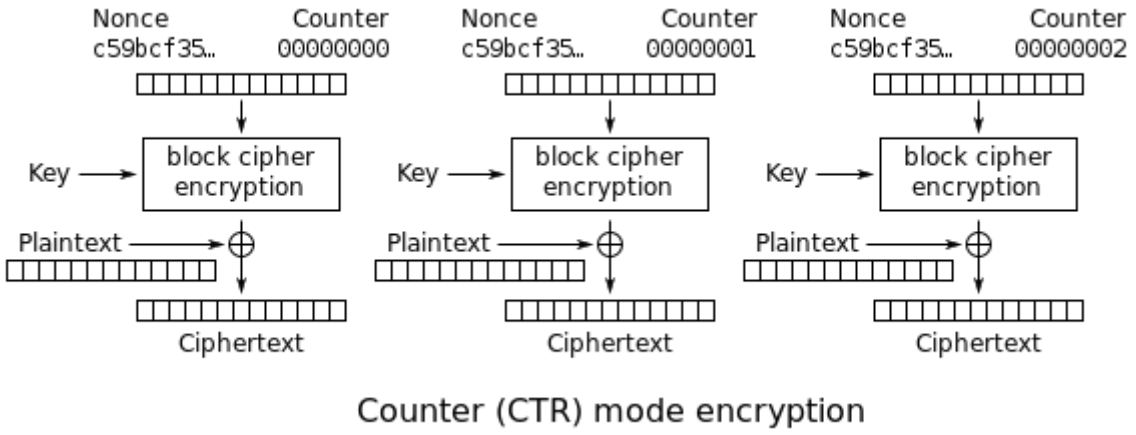
Output Feedback (OFB) mode encryption

OFB is derived to reduce the time in CBC. Here, the things needed for encryption and decryption can be prepared in advance. This shortens the time.

In OFB mode, there is a failure (while sending) in ciphertext block n, only affects plaintext block n. The failure in IV, all the blocks are affected. Immutability of IV is very very important in OFB mode. Sender and receiver must take care of it.

Block size and iv; 16 bytes for AES, 8 bytes for DES.

CTR Design



Counter (CTR) mode encryption

In our work, we concatenate nonce and counter byte arrays (AES 8 byte nonce, 8 byte counter, DES 4 byte nonce, 4 byte counter). Counter starts with 1.
The things needed for encryption and decryption can be prepared in advance. This shortens the time.
Another advantage is we decrypt the ciphertext blocks in parallel. (We did not do this in our work).
Any ciphertext block can be encrypt/decrypt separately.
Any failure on ciphertext block n (while sending) , only plaintext block n affects. Failure on nonce affects all the blocks, immutability of nonce is very very important. Sender and receiver must take care of it.