Computer Science and Engineering Department

Group Name&Surname: Mehmet Taha USTA & Burcu ÖZTAŞ

Identity Numbers: 21527472 & 21483435

Course: BBM-465 Information Security Lab.

Experiment: Assignment 1

Subject: Block Cipher

Due Date: 4/11/2019 - 23:59

Advisor: Dr. Ahmet Selman BOZKIR

Main Program: Java

Problem

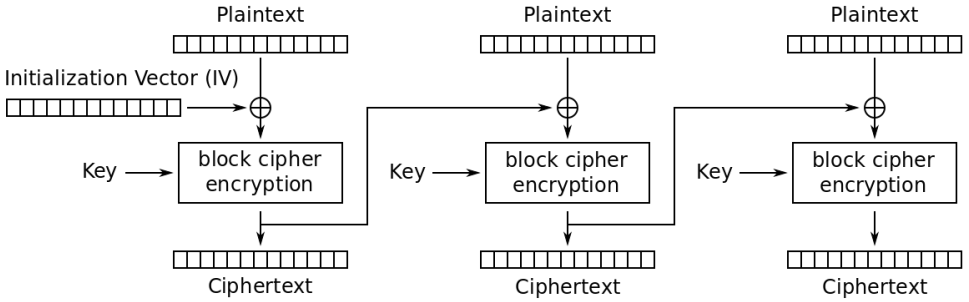
In this project, it is expected to support 3 encryption modes (CBC, OFB, CTR) and 2 encryption algorithms (AES, DES).
These modes should be based on the ECB (Electronic code book) concept.
And the current CBC, OFB, CTR modes should be applied manually through ECB mode instead of being used directly.

Method & Solution of Problem

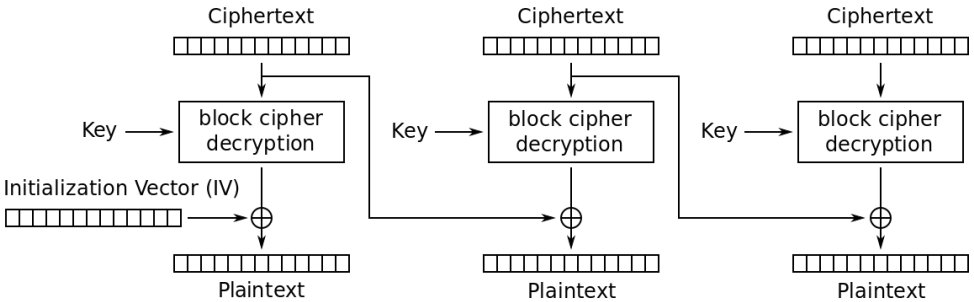
Our project, which is designed in accordance with the ECB concept, is based on two basic encryption algorithms.

Our first algorithm, AES 128 bit base, is designed with 3 basic modes, our first basic mode is

1)CBC mode provides encryption and decryption process.
In CBC mode, our Plaintexts enter XOR process with initialization vector and provide Ciphertext result with Block cipher encryption method.
Similarly, key with Ciphertext for decryption
block cipher decryption process.
After this process, the initialization vector (IV) is processed with Xor function and plaintext is obtained.With CBC mode encryption, each ciphertext block is dependent on all plaintext blocks processed up to that point. This adds an extra level of complexity to the encrypted data.

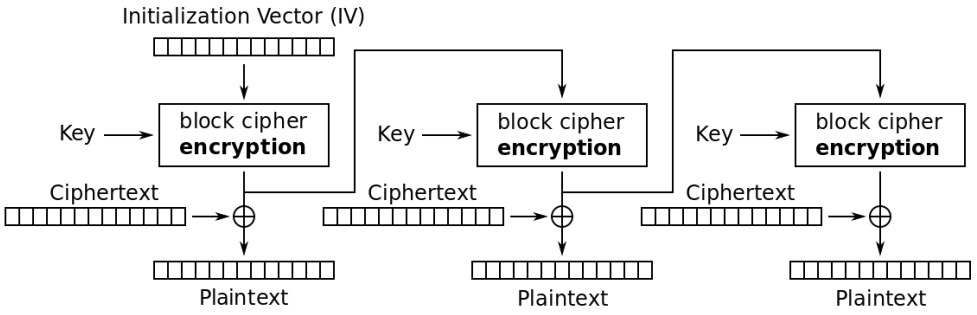


Cipher Block Chaining (CBC) mode encryption

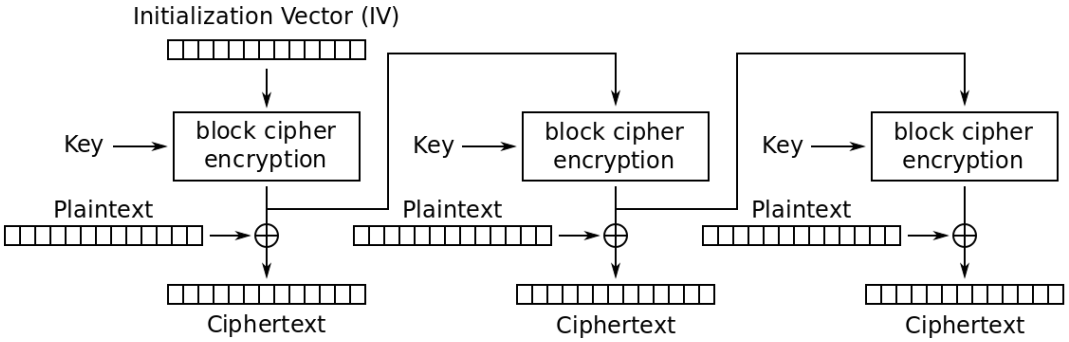


Cipher Block Chaining (CBC) mode decryption

2)Another mode, OFB 128/8 = 16 bit, creates block size.
Initialization vector and key has encryption or decryption process in this mode.
With the result, our cipher text enters Xor function and plaintext is obtained.

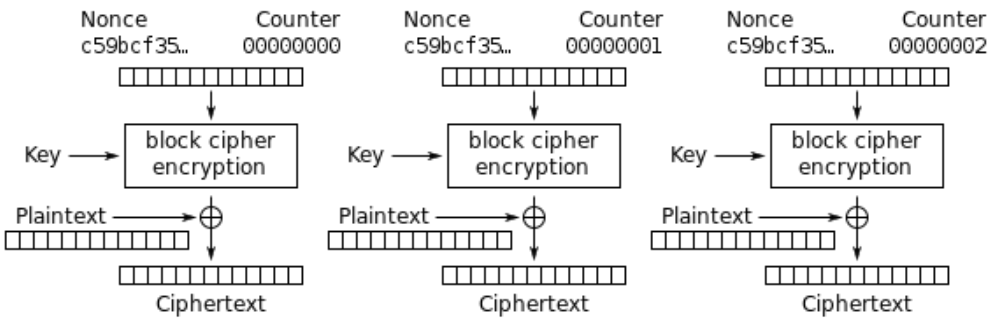


Output Feedback (OFB) mode decryption



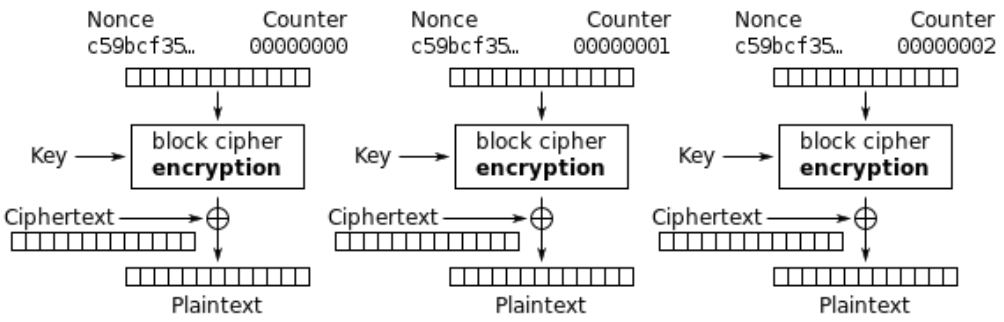
Output Feedback (OFB) mode encryption

3)CTR mode has a counter which is different from other modes.
With each cycle,substring is containing last 8 characters.(As long as it is bigger than 8 bits).
In this way, the counter bit formed by combining the nonce bit with the generated password value enters the encryption block.
The result and the ciphertext enters the Xor process and plaintext is obtained.
For Decryption mode, the counter value is increased by one for our coding.
(As long as it is less than 8 bits).And Some way is applied.
In decryption and encryption operations, ciphertext and plaintext are replaced.
In order to obtain plaintext for the encryption process, when entering the ciphertext xor process,



In the decryption process, plaintext enters xor with the result of the block and obtains ciphertext.

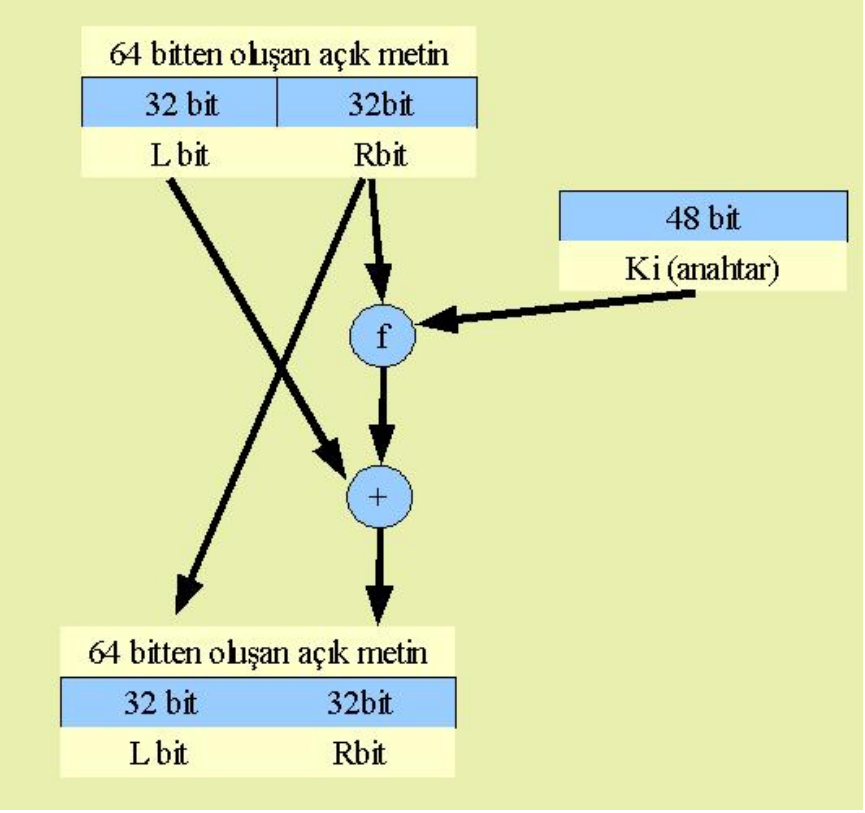
Counter (CTR) mode encryption



Counter (CTR) mode decryption

Our second algorithm, DES 64 bit base, is designed with 3 basic modes as well.

DES divides the plain text to be encrypted into pieces (blocks) and encrypts each part independently, and performs the same operation on blocks to open the cipher text. The length of these



blocks is 64 bits.
The following shows the operations that a 64bit data entry performs during a pass:

DES also receives a 64bit key. However, the valid length of this key is 56 bits because it is spent for 8 bit lots.According to Intructer 's request,64 bit selects from least significant bit. And the same Encryption modes are handling for DES algorithms.

The DES algorithm encrypts the 64-bit length M block and converts it to a 64-bit C block. If each 64-bit encryption is performed separately, this type of encryption is called the Electronic Code Book (ECB).

Resources;

1-https://en.wikipedia.org › wiki › Encryption

2-http://bilgisayarkavramlari.sadievrenseker.com/2008/03/13/des-veri-sifreleme-standardi-data-encryption-standard/

3-"Cryptography and Network Security" Seventh Edition by William Stallings

4-https://datalocker.com/what-is-the-difference-between-ecb-mode-versus-cbc-mode-aes-encryption/