Hacettepe University

Computer Engineering Department

BBM465 INFORMATION SECURITY - 2022 FALL

Assignment 1

November 2, 2022

Student names:
Yiğit Emir İŞIKÇI
Abdullah Mert DİNÇER

Student Numbers:
2200356028 - 2200356016

1 Problem Definition

In this assignment the problem is encrypting some plain text according to various algorithms (DES, 3DES) and various modes (CBC, CFB, OFB, CTR). These modes should be based on ECB (Electronic Code Book) concept.
Also, we are supposed to measure their run times.

2 Method - Solution

We was supposed to implement 2 algorithms (DES, 3DES) based on ECB scheme. ECB divides the problem into blocks, which is 64 bit in this assignment, and solves them seperately.
Our approach:
Firstly we divide the input text into 8 byte blocks. Then for each block, we encrypted or decrypted it according to the provided algorithm and mode.

2.1 DES - 3DES difference

DES is a symmetric-key algorithm that uses the same key for encryption and decryption processes. 3DES was developed as a more secure alternative because of DES's small key length. 3DES or Triple DES was built upon DES to improve security

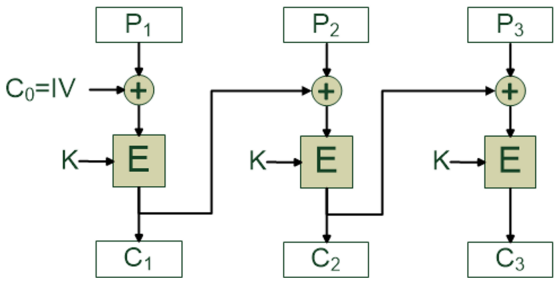
2.2 CBC (Cipher Block Chaining)

In CBC mode, firstly plain text block and initialization vector are entered XOR process. The product is encrypted with provided key. The result is the cipher text. We are giving this cipher text to following block as a initialization vector. This is the encryption process.

In decryption, firstly cipher text is decrypted with provided key. Then the result is entered XOR process with initialization vector. The result is plain text. In the next block, we are using previous block's cipher text as a initialization vector.

Cipher Block Chaining (CBC)

- Cipher Block Chaining (CBC): next input depends upon previous output
  - Encryption: $C_i = E_k [P_i \oplus C_{i-1}]$, with $C_0 = IV$
  - Decryption: $P_i = C_{i-1} \oplus D_k[C_i]$, with $C_0 = IV$

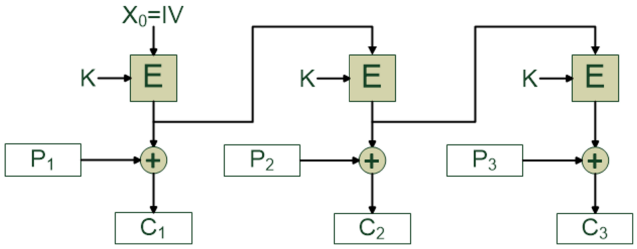


2.3 OFB (Output Feedback)

In OFB mode, firstly initialization vector encrypted with provided key. The result is entered XOR process with plain text to obtain cipher text. Also, same result is passed to following block as a initialization vector. This is the encryption.
In decryption, firstly initialization vector enters encryption process with provided key. The result is entering XOR process with cipher text to provide plain text. Meanwhile same result is passing to following block's initialization vector.

Output Feedback (OFB)

- Output feedback (OFB): construct a pseudorandom number generator (PRNG) to obtain a one time pad and XOR the message with the pad
  - Encryption: X_0=IV, $X_i = E_k[X_{i-1}]$, $C_i = P_i \oplus X_i$
  - Decryption: X_0=IV, $X_i = E_k[X_{i-1}]$, $P_i = C_i \oplus X_i$

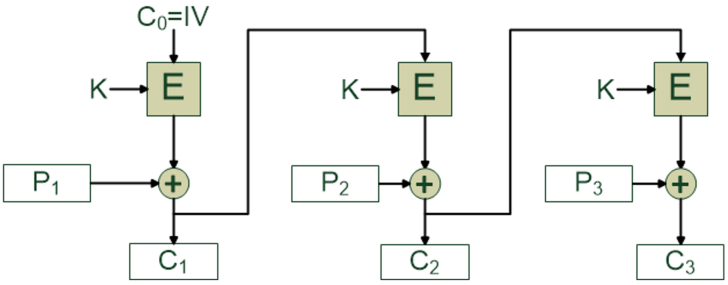


2.4 CFB (Cipher Feedback)

Only difference between OFB and CFB is that in OFB we are passing result of encryption to following block whereas we are passing result of XOR operation in CFB.

Cipher Feedback (CFB)

- Cipher Feedback (CFB): the message is XORed with the feedback of encrypting the previous block
  - Encryption: C_0=IV, $C_i = E_k[C_{i-1}] \oplus P_i$
  - Decryption: C_0=IV, $P_i = E_k[C_{i-1}] \oplus C_i$

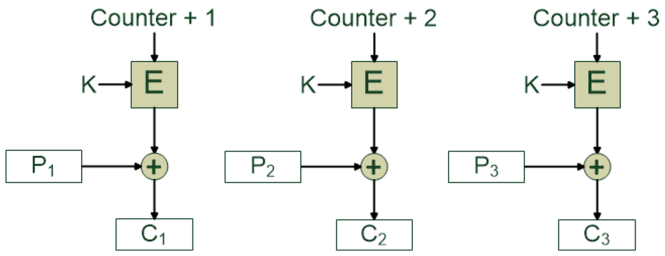


2.5 CTR (Counter Mode)

In CTR mode, we are encrypting a nonce and continuously increasing counter value. The result is entering XOR operation with plain text to obtain cipher text.

Counter Mode (CTR)

- Counter Mode (CTR): Another way to construct pseudo random number generator using DES
  - $X_i = E_k[\text{Counter}+i]$
  - $C_i = P_i \oplus X_i$
  - Sender and receiver share a counter value (does not need to be secret) and the secret key



3 Example code for CBC

```
public static byte[] encryptCBC(byte[] plain, byte[] key, byte[] IV) {
      //firstly obtaining the xor_result with plain text and initialization
         vector.
      byte[] xor_result = xor_op(plain, IV);
      //encrypting the obtained xor_result with provided key.
      SecretKeySpec secret_key = new SecretKeySpec(key, "TripleDES");
      Cipher cipher = Cipher.getInstance("TripleDES/ECB/NoPadding");
      cipher.init(Cipher.ENCRYPT_MODE, secret_key);
      //return the cipher text
      return cipher.doFinal(xor_result);
   }
```

We are using these function for all of the plain text blocks to get full cipher text.

```
public static void __DES_CBC_ENCRYPT__(FileOutputStream fos, byte[] key,
    byte[] IV) {
       //encrypt all plaintext blocks with for loop
       for(String eightByteWord : __INPUT_ARRAY_FOR_ENCRYPT__){
          //obtaining cipher text
          byte[] cipherBlock =
             DES.encryptCBC(eightByteWord.getBytes(StandardCharsets.ISO_8859_1),key,IV);
          fos.write(cipherBlock);
          //passing cipher text to following blocks initialization vector.
          IV = cipherBlock.clone();
       }
    }
```

Resources:
https://www.techtarget.com/searchsecurity/definition/Electronic-Code-Book