

need to know how they work, and to compute them by hand

## Information Systems Security

### Series 4 : Block Ciphers

October 27th, 2021

#### Exercice 1 : Linear encryption

Let  $EL(k, m)$  be a block cipher linear encryption, with  $k$  the key and  $m$  the block of the message, with nominal size of 128 bits (blocks of plaintext, blocks of ciphertext, and keys are all 128 bits). Since it's linear, we have :

$$EL(k, (m_1 \oplus m_2)) = EL(k, m_1) \oplus EL(k, m_2)$$

- You are allowed to choose 128 "chosen ciphertexts", i.e., you can choose 128 different ciphertexts as you want, and obtain for each one the corresponding plaintext.  
By choosing carefully these 128 chosen ciphertexts, show that you can then decipher every cipher you encounter without needing the key.
- Is it a good idea to have a linear encryption system ?

#### Exercices 2 to 6 : Global Framework

In a block cipher, we work by dividing the plaintext/ciphertext into blocks of fixed size. In this kind of cipher, there are two important choices that impact how the encryption works : the encryption mode, and the encryption function. The encryption mode allows to chain or link different blocks in different ways. The encryption function is the core of the encryption, and is used many times in different ways depending on which mode is used.

For all following exercises, we will consider :

- Plaintext  $P$ , written as blocks  $P_i$  of size 1 byte = 8 bits.
- Key  $K$ , with a length of 1 byte.
- Ciphertext  $C$ , as blocks  $C_i$  of size 1 byte.

- Initial value (if needed) IV, also 1 byte.
- Each element may be expressed in hexadecimal. Then, each block is simply written as two hexadecimal characters.

## Exercice 2 : Fonctions d'Encryption pour Chiffrements par Blocs

We consider a block  $B$  from the plaintext. We write it as  $(B_1 B_2)_{16}$ . Similarly, we write  $K = (K_1 K_2)_{16}$  the key, and  $E = (E_1 E_2)_{16}$  the resulting ciphertext block.

We're proposing the following encryption functions :

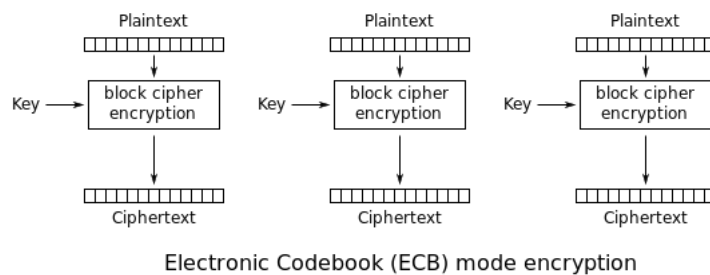
1.  $E = B \oplus K$
2.  $E_i = (B_i + K_i) \bmod 16$
3.  $E_i = (B_i - 2 * K_i) \bmod 16$
4.  $E_i = (2 * B_i - K_i) \bmod 16$
5.  $E_i = (B_i * K_i) \bmod 16$
6.  $E_i = (7 * B_i + K_i) \bmod 16$
7.  $E_i = (4 * B_i + K_i) \bmod 16$
8.  $E_1 = (3 * B_1 + K_2) \bmod 16, E_2 = (11 * B_2 - K_1) \bmod 16$

Which ones of these methods can be used as encryption functions (We are asking which ones can be used, not if they should be or if they are effective) ?

*Reminder : If we want to encrypt something, we need to be able to decrypt it.*

## Exercice 3 : ECB

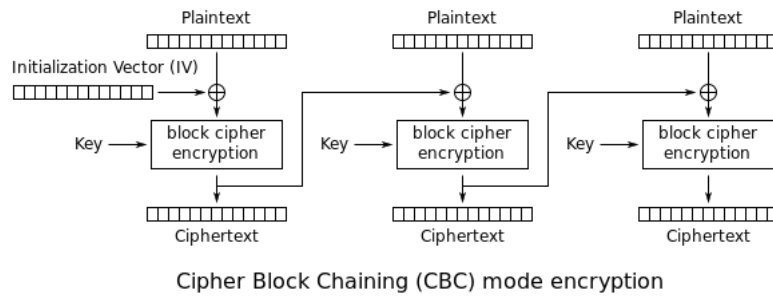
ECB (Electronic CodeBook) :



1. Let  $K = (AB)_{16}$ ,  $IV = (AD)_{16}$ . Encrypt message  $m = (A741BA)_{16}$ , with function  $E_K(B) = K \oplus B$  and 8 bit blocks.
2. Same question, but with the function  $E_K(B_i) = (7 * B_i + K_i) \bmod 16$ .

## Exercice 4 : CBC

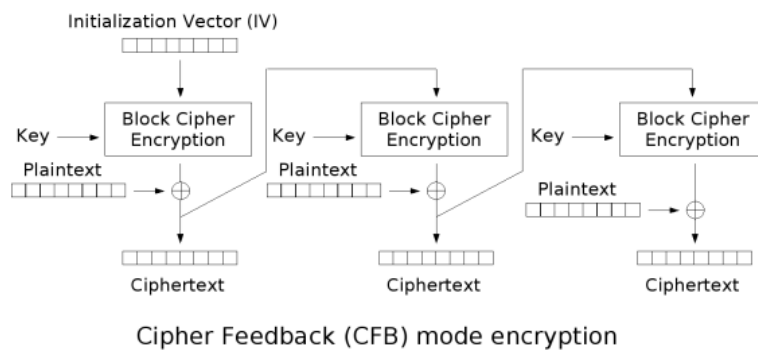
CBC (Cipher Block Chaining) :



1. Let  $K = (AB)_{16}$ ,  $IV = (AD)_{16}$ . Encrypt message  $m = (A741BA)_{16}$ , with function  $E_K(B) = B \oplus K$  and 8 bit blocks.
2. Same question, but with encryption function  $E_K(B_i) = (7 * B_i + K_i) \bmod 16$ .

## Exercice 5 : CFB

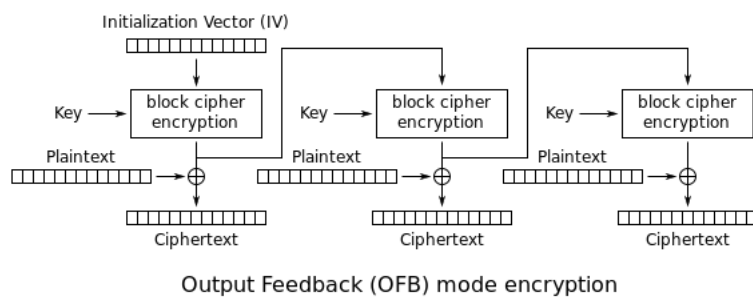
CFB (Cipher FeedBack) :



1. Let  $K = (74)_{16}$ ,  $IV = (AA)_{16}$ . Encrypt message  $m = (2468AC)_{16}$  with function  $E_K(B_i) = (7 * B_i + K_i) \bmod 16$  and 8 bit blocks.
2. Now, decipher the ciphertext  $c = (123456)_{16}$ , knowing the encryption was done with the same key, IV and function.

## Exercice 6 : OFB

On rappelle le schéma du mode OFB (Output FeedBack) :



1. Let  $K = (74)_{16}$ ,  $IV = (AA)_{16}$ . Encrypt message  $m = (13579B)_{16}$  with function  $E_K(B_i) = (11 * B_i + K_i) \bmod 16$  and 8 bit blocks.
2. Now, decipher the ciphertext  $c = (123456)_{16}$ , knowing the encryption was done with the same K, IV and function.