# FIT3031 - Tutorial 2

# SYMMETRIC ENCRYPTION

## Review

Q1. What are the essential ingredients of a symmetric cipher?

Q2. What are the two basic functions used in encryption algorithms?

Q3. How many keys are required for two people to communicate via a symmetric cipher? How many keys are required for n people to communicate with each other securely?

Q4. What is the difference between a block cipher and a stream cipher?

a. Why is it not desirable to reuse a stream cipher key?

b. Why do some block cipher modes of operation only use encryption while others use both encryption and decryption?

Q5. What are the two general approaches to attacking a cipher?

Q6. List and briefly define types of cryptanalytic attacks based on what is known to the attacker.

Q7. What is triple encryption? Why is the middle portion of 3DES a decryption rather than an encryption?

Q8. List ways in which secret keys can be distributed to two communicating parties.

Q9. What is the difference between a session key and a master key?

Q10. What is a key distribution center?

## Problems

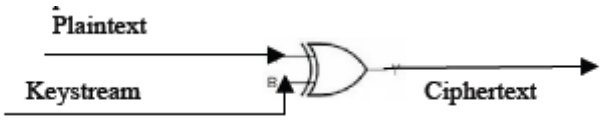
1. Prove the following:
   a. $(A \oplus B) \oplus C = A \oplus (B \oplus C)$
   b. $A \oplus A = 0$
   c. $A \oplus 0 = A$
   d. $A \oplus 1$ = bitwise complement of A = A'

e. $(A \oplus B)' = A' \oplus B = A \oplus B'$
f. $A' \oplus B' = A \oplus B$

where

A, B, C are *n*-bit strings of bits
0 is an *n*-bit string of zeros
1 is an *n*-bit string of ones

2. Stream Cipher:




What is the value of ciphertext if:
Plaintext : 1010101010100
Keystream : 1100110001001

**3.** With the ECB mode, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC mode this error propagates. For example, an error in the transmitted $C_1$ (Figure 6.4 below) obviously corrupts $P_1$.
**a.** Are any blocks beyond $P_2$ affected?
**b.** Suppose there is a bit error in the source version of $P_1$. Through how many ciphertext blocks is this error propagated? What is the effect at the receiver?
**c.** Is it possible to perform encrytions operation in parallel on multple blocks of plaintext in the CBC mode? How about decryption?
**d.** Suppose there is an error in a block of ciphertext on transmission using CBC, with reference to the Figure given below. What effect is produced on the recovered plaintext blocks?

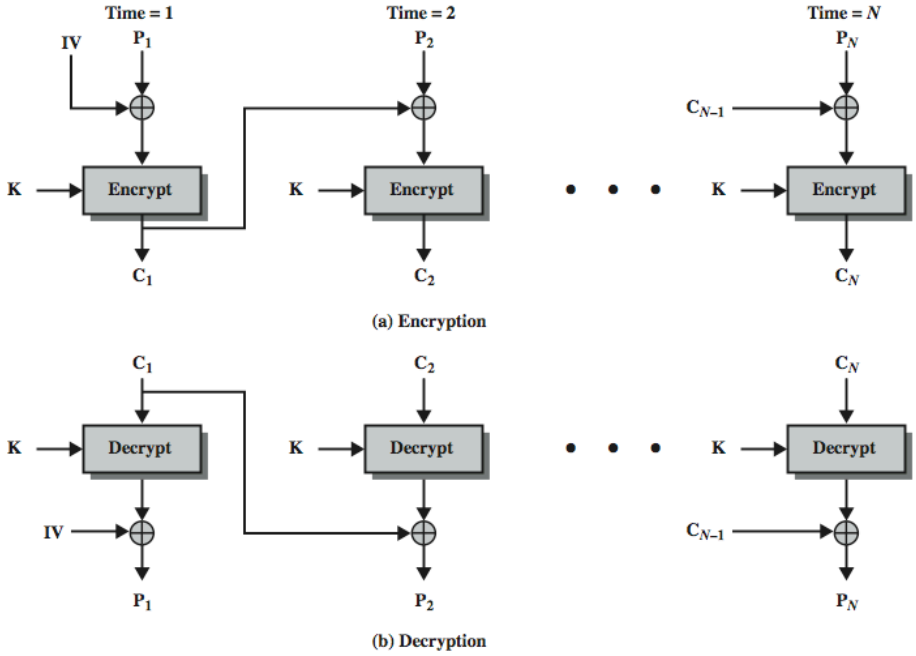



**Figure 6.4 Cipher Block Chaining (CBC) Mode**

**4.** For each of the modes ECB, CBC, CTR shown in Figures 6.3, 6.4 and 6.7 respectively:

a. Identify which decrypted plaintext blocks $P_x$ will be corrupted if there is an error in block $C_4$ of the transmitted ciphertext.

b. Assuming that the ciphertext contains N blocks, and there was a bit error in the source version of $P_3$, identify through how many ciphertext blocks this error is propagated.

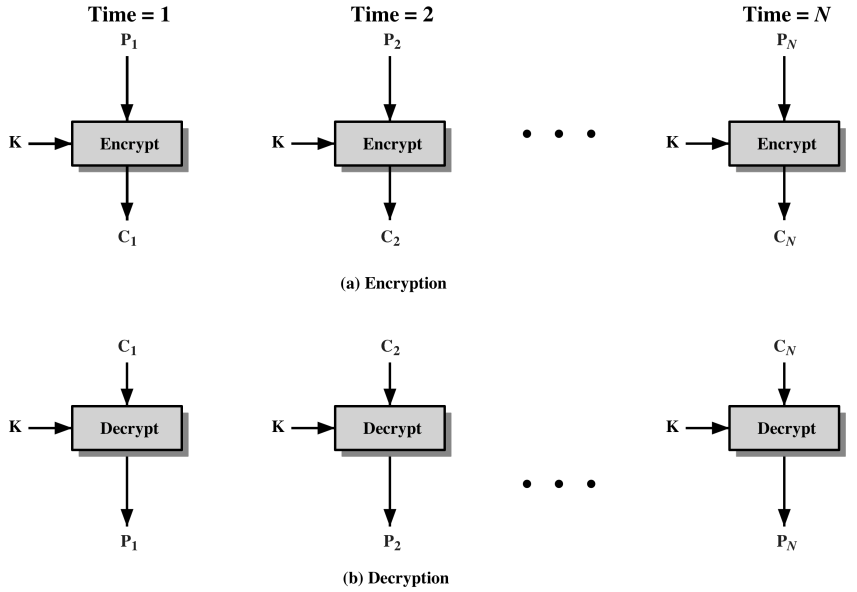



**Figure 6.3 Electronic Codebook (ECB) Mode**

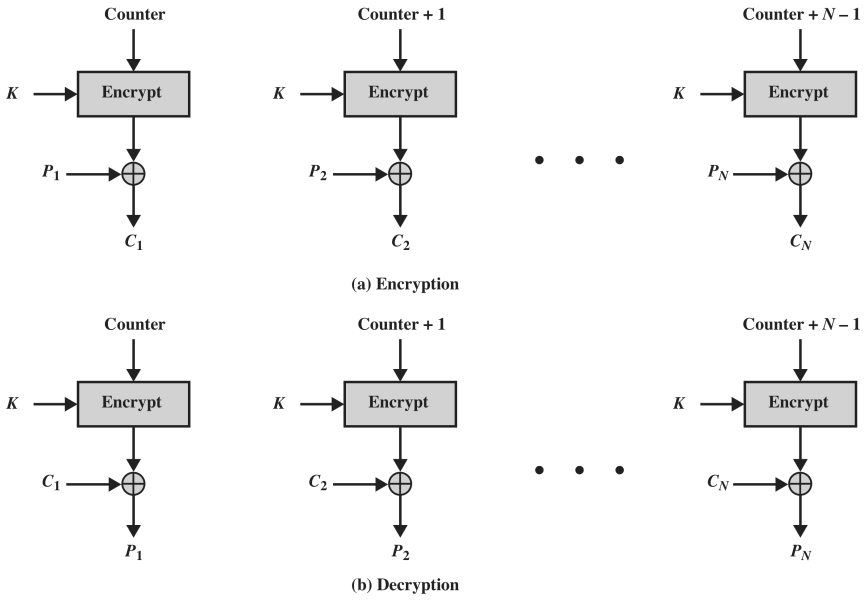



**Figure 6.7 Counter (CTR) Mode**

**5.** Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in OFB mode which is shown in Figure 6.6? How about decryption?

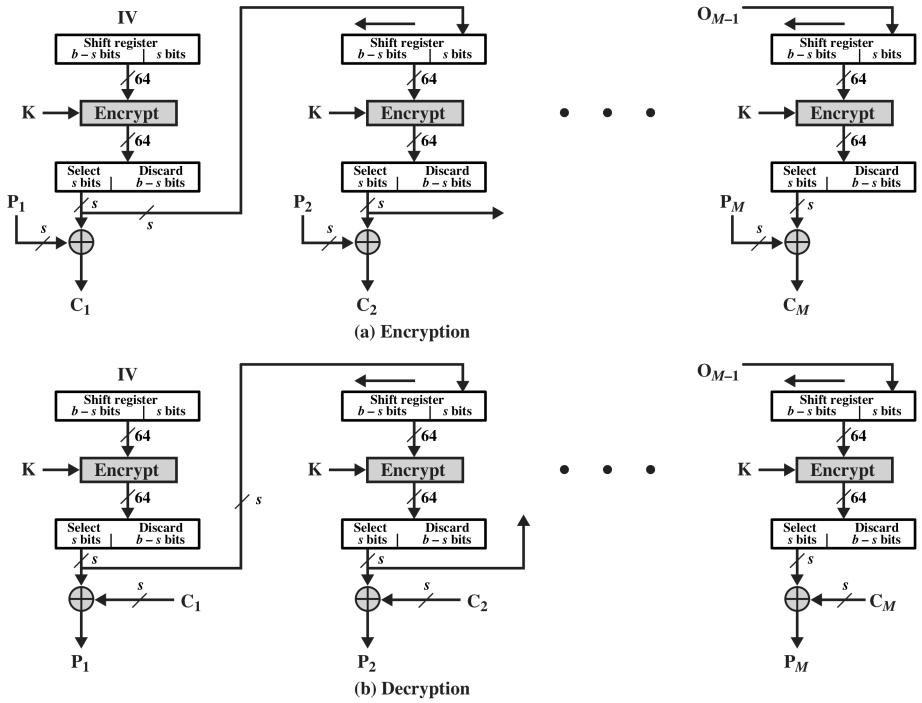



**Figure 6.6** ***s*-bit Output Feedback (OFB) Mode**

---

**6.** Consider a block cipher algorithm with the following properties:

- Input and output block length of 64 bits and the key size is 56 bits
- Given a key K, the key scheduling requires 2 microseconds ($2 \times 10^{-6}$ secs)
- After the key scheduling produces all the sub-keys (if required), the encryption of a single block of 64 bits block takes 0.5 microseconds.

Compute the following information:

a. The total time required (of course in microseconds) to encrypt **1MBytes** (**$2^{20}$** bytes) of data.

b. Given 2 values C and M such that $C = E_K(M)$ under the unknown key value K, how many years (at most) are required to crack the cipher on a single computer.