FIT2093: Tutorial 5

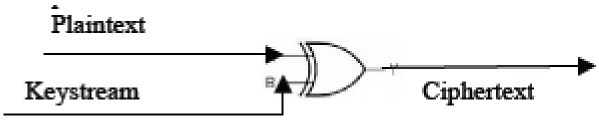
Symmetric Key Cryptography

Review

1. What is the purpose of the S-boxes in DES?
2. What is the difference between a block cipher and a stream cipher?
3. What is triple encryption?
4. How many keys are used in triple encryption?
5. Does a substitution need to be a permutation of the plaintext symbols? Why or why not?
6. Explain why the product of two relatively simple ciphers, such as a substitution and a transposition, can achieve a high degree of security.
7. What is a meet-in the-middle attack?

Problems

1. Why is it not desirable to reuse a stream cipher key?
2. Stream Cipher:



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

3. Perform encryption and decryption using TPC for Plaintext “25” and key [1,6].
4. The role of the S-boxes in the function F of DES is illustrated in Figure 1 and 2. The substitution consists of a set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output. These transformations are defined in Table 1, which is interpreted as follows: The first and last bits of the input to box S_i form a 2-bit binary number to select one of four substitutions defined by the four rows in the table for S_i. The middle four bits select one of the sixteen columns. Find the output for the following input:

   a. S_1 (011001)
   b. S_5 (000000)
   c. S_6 (111111)
5. Why do some block cipher modes of operation only use encryption while others use both encryption and decryption?

6. 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.
7. 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?
8. If a bit error occurs in the transmission of a ciphertext charater in 8-bit CFB mode shown in Figure 6.5, how far does the error propagate?
9. 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 (2×10^{-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.

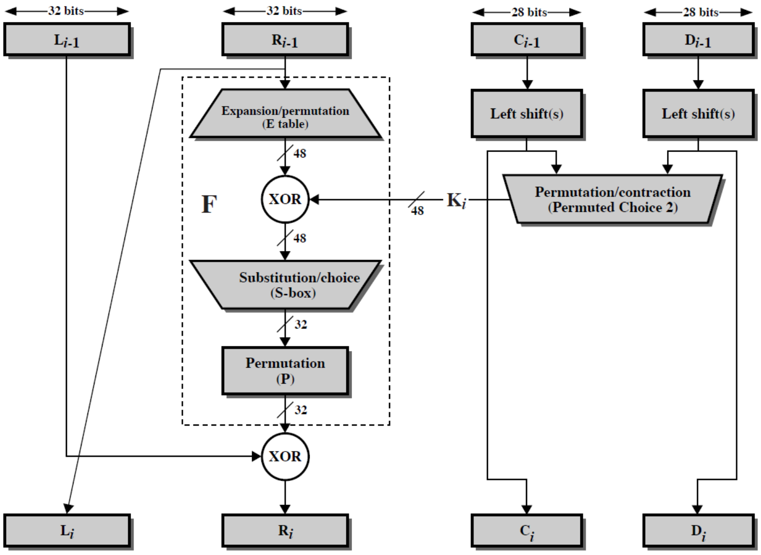


Figure 1 Single Round of DES Algorithm

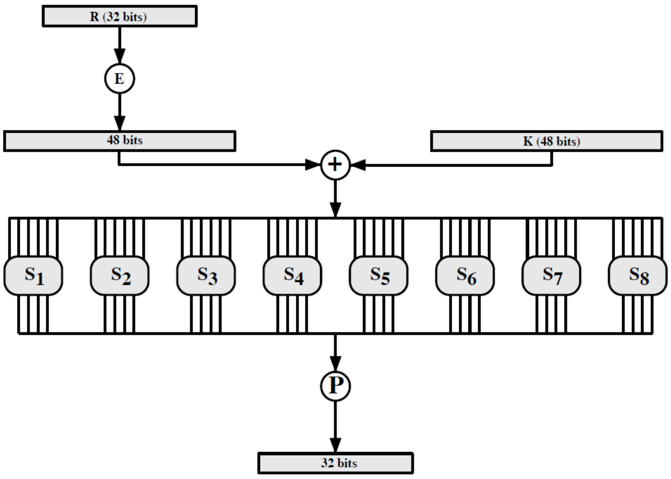


Figure 2 Calculation of F(R, K)

Table 1 Definition of DES S-Boxes

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

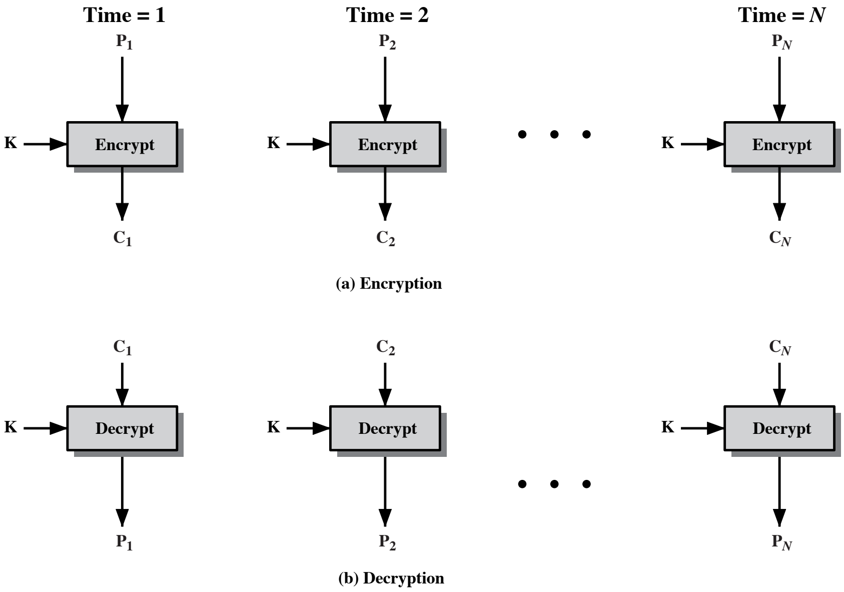


Figure 6.3 Electronic Codebook (ECB) Mode

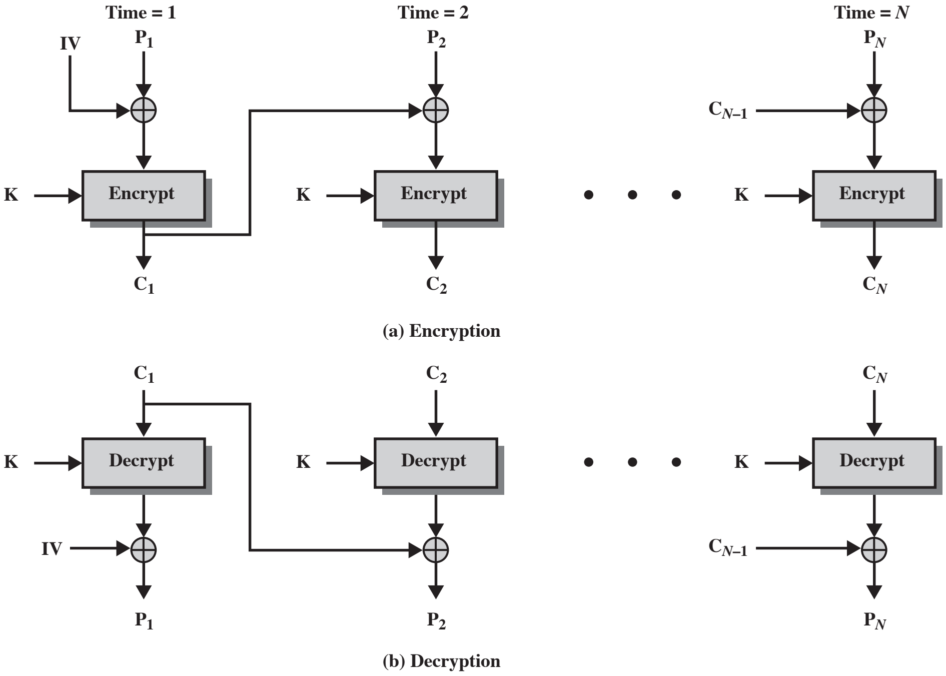


Figure 6.4 Cipher Block Chaining (CBC) Mode

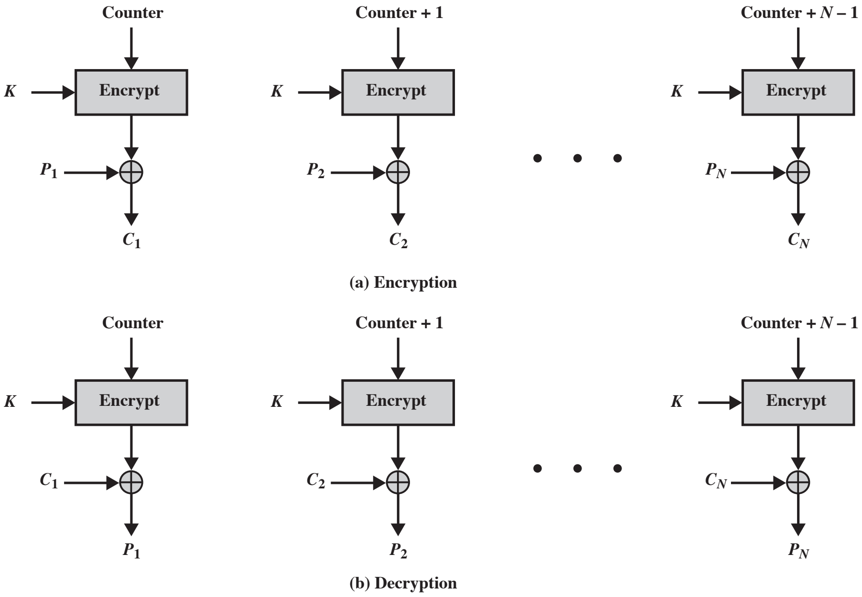


Figure 6.7 Counter (CTR) Mode

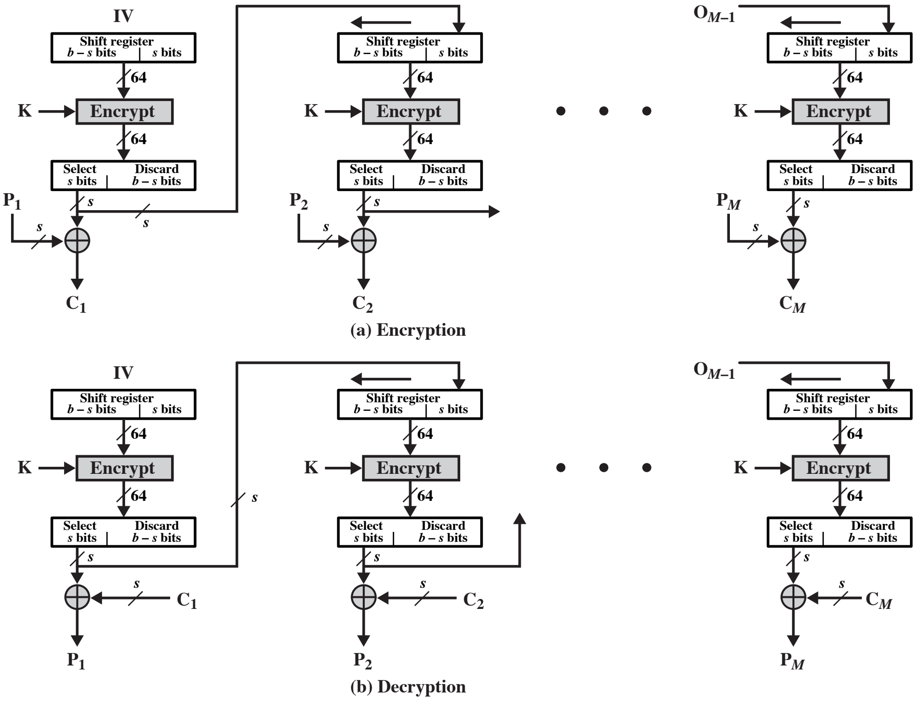


Figure 6.6 *s*-bit Output Feedback (OFB) Mode

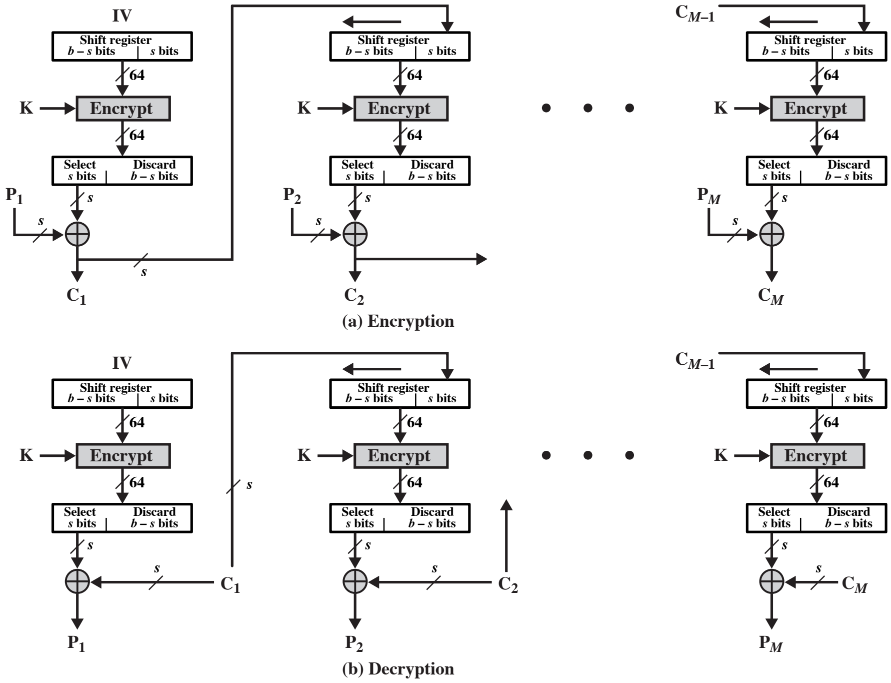


Figure 6.5 *s*-bit Cipher Feedback (CFB) Mode