Quiz-2
Cryptography and Network Security

[Total marks - 20]

[**Instructions**: Please upload your answers in Microsoft Teams by **02/10/2020**. Your **Roll No.** and **Name** must be mentioned.]

1. DES S-Boxes. Perform the following DES S-box computations
   (a) $S_3(101010)$
   (b) $S_6(011010)$
   (c) $S_3(111010)$
   (d) $S_1(111111)$ [2 marks]
2. *Complementary Keys and Plaintext Yield Complementary Plaintexts in DES*. The complement of a bit vector (or string) P is the bit vector $\overline{P}$ of the same length whose bits are the opposites of those of P. Put differently, $\overline{P} = P \oplus 11111\cdots$. Prove that the complement $\overline{C}$ of a ciphertext message produced by DES from a plaintext P and using a key K is the same as the ciphertext message produced (directly) by DES using plaintext $\overline{P}$ and key $\overline{K}$. This result may be symbolized as $\overline{\mathsf{DES}_K(P)} = \mathsf{DES}_{\overline{K}}(\overline{P})$. [4 marks]
3. We consider the following (very simple) block encryption function $E_K = E$ on 2-bit blocks (so the block size is $l = 2$) that is defined in Table 1. The following sequence of plaintext is to be transmitted: 1010100011.
   (a) Determine the corresponding ciphertext sequence that gets transmitted if electronic codebook mode is used.
   (b) Determine the corresponding ciphertext sequence that gets trans-

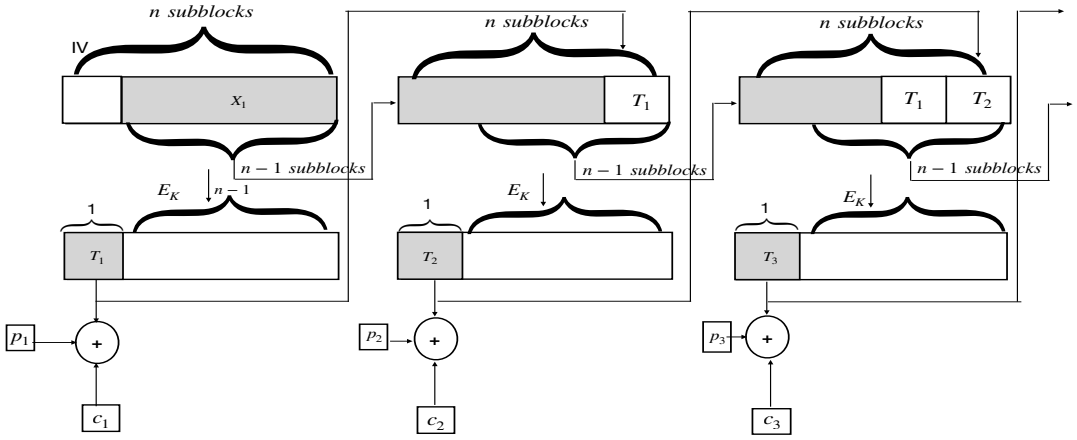
mitted if cipherblock chaining mode is used with initial vector $\mathsf{IV} = 10$. [1+1=2 marks]

Table 1: Block Encryption Function of Question 3 and 4

P	00	01	10	11
$E(P)$	10	00	11	01

4. Determine the ciphertext that gets transmitted if the encryption function of Table 1 is used in output feedback mode as in Figure 1 with the plaintext 101110 and parameters $k = 1$ and initial vector $\mathsf{IV} = 10$. Here l is the block size, k is the subblock size, $n = l/k$ is the number of subblocks and $k|l$. [4 marks]

Figure 1: The output feedback (OFB) mode of encryption for block cryptosystems



5. *Propagation of Errors in Block Cryptosystem Modes of Operation.* Throughout this exercise, we assume (as in the development of the modes of operation) that we have an underlying block cryptosystem with block size l. We denote the encryption mapping by E, and the corresponding decryption mapping by D. In cases of a stream mode of operation, we let

k denote the subblock size, so that $k|l$. Suppose that a single plaintext bit has been entered incorrectly.

(a) How many ciphertext bits could be possibly corrupted if the electronic code-book mode is used?

(b) How many ciphertext bits could be possibly corrupted if the cipherblock chaining mode is used?

(c) How many ciphertext bits could be possibly corrupted if the cipher feedback mode is used?

(d) How many ciphertext bits could be possibly corrupted if the output feedback mode is used? [2+2+2+2=8 marks]