Marks

Q.1 **(A)** What is the difference between passive and active security threats? List and briefly define categories of passive and active security attacks. **[4]**

(B) (1) Define the term – confusion, diffusion. **[2]**

(2) What is block cipher and stream cipher? **[2]**

(3) What is differential and linear cryptanalysis? **[2]**

Q.2 **(A)** Encrypt the following message using playfair cipher. **[5]**

Message: COMSEC

Keyword: GALOIS

(B) Explain various types of cryptanalytic attacks in brief. **[5]**

OR

Q.2 **(A)** Use Hill cipher to encrypt and decrypt the text DEF. **[5]**

The key to be used is

$$\begin{matrix} 2 \\ 9 \\ 3 \end{matrix}\begin{bmatrix} 4 & 5 \\ 2 & 1 \\ 8 & 7 \end{bmatrix}$$

(B) Explain Electronic code Book block cipher mode of operation in detail with figure. **[5]**

Q.3 **(A)** Explain the steps involved in International data encryption standard algorithm. What is the purpose of the S-boxes in DES? **[5]**

(B) Find the multiplicative inverses of the following using extended Euclidean algorithm. **[5]**

(1) 50 mod 71

(2) 43 mod 64

OR

Q.3 **(A)** Explain various steps of AES algorithm in brief. **[5]**

(B) For each of the following equations, find an integer x that satisfies the equation. **[5]**

(1) $7x \equiv 5 (\text{mod } 3)$.

(2) $5x \equiv 6 (\text{mod } 17)$.
