OR

(b) Write short notes on the following :

10 Marks (CO1)

(i) Steganography

(ii) Security Attacks

(iii) Diffusion and Confusion

H Roll No. .....

TCS–604

B. TECH. (CSE) (SIXTH SEMESTER)
MID SEMESTER EXAMINATION, 2021

NETWORK AND CYBER SECURITY

Time : 1½ Hours

Maximum Marks : 50

Note : (i) Answer all the questions by choosing any ***one*** of the sub-questions.

(ii) Each question carries 10 marks.

1. (a) What taxonomy is used for the security goals, security services and security mechanism of cryptography ?

10 Marks (CO1)

OR

(b) What are the different types of Cryptography ? Using the Vigenère cipher, encrypt the word 'explanation' using the key leg. 10 Marks (CO1)

P. T. O.

2. (a) (i) Explain Caesar cipher with numerical example.

(ii) Encrypt the word "diamond" using affine cipher having key pair (5, 2).

10 Marks (CO2)

OR

(b) Explain DES structure. If the key with parity bit (64 bits) is 0123 ABCD 2562 1456, find the first round key.

10 Marks (CO2)

3. (a) (i) What is the Meet-in-the-Middle attack ?

(ii) Using Playfair cipher, encrypt the message "the platinum is precious than gold". Ignore the white paces between words. The key used for encryption is 'GUIDANCE.

10 Marks (CO2)

OR

(b) (i) Differentiate the Stream Cipher and Block Cipher.

(ii) In the columnar transposition cipher, the permutation key is (3, 5, 1, 2, 4). Find out the decryption key and encrypt the message given below : "lets meet today". 10 Marks (CO2)

4. (a) Discuss Public Key Cryptosystem. Explain RSA algorithm with suitable steps. Let $p = 17$, $q = 11$, $e = 7$ and $d = 23$. Calculate the public key and private key and 1053 show encryption and decryption for plain text M = 88 by using RSA algorithm.

10 Marks (CO2)

OR

(b) Discuss "AES" with general design. AES has a larger block size than DES (l28 VERSUS 64). Is this an advantage or disadvantage ? Explain. 10 Marks (CO2)

5. (a) Define the Euler's Theorem and Fermat's Theorem. Find the result of the following, using Euler's Theorem and Fermat's Theorem : 10 Marks (CO1)

12^{-1} MOD77, 27^{-1} MOD41.