COLLEGE OF ENGINEERING TRIVANDRUM
DEPARTMENT OF COMPUTER APPLICATIONS
Third Semester M.C.A Degree
First Series Examination January-2021

20MCA263: CYBER SECURITY & CRYPTOGRAPHY

Time: 1 hr **Max. Marks: 20**

PART-A

(***Answer All Questions. Each question carries 2.5 marks***)

1. What is the difference between Monoalphabetic cipher and Polyalphabetic cipher?

2 Compare phishing and ransomware attack.

3. Differentiate between block cipher and stream cipher.

4. How does 3-DES enhance the security than that of DES?

(Total: 4*2.5= 10 marks)

PART-B

(***Each question carries 5 marks***)

5. Construct a playfair matrix with the key ***largest.*** Encrypt the message **“necessary”** using the created playfair matrix.

OR

6. Use the Vignere cipher to encrypt the word **“cryptography”** using the key ***house***

7. Briefly describe the fiestel cipher structure and justify that the input plaintext at the encryption side is reproduced at the decryption side of fiestel cipher structure.

OR

8. In a public-key cryptosystem using RSA, you intercepted the ciphertext C=8 send to a user whose public key is e=13, n=33. What is plaintext M?

(Total: 2*5= 10 marks)