USN ☐☐☐☐☐☐☐☐☐☐   **10EC832**

Eighth Semester B.E. Degree Examination, July/August 2021
Network Security

Time: 3 hrs.   Max. Marks:100

Note: *Answer any FIVE full questions.*

1 a. Explain the model of network security with neat diagram. List four basic tasks of designing security model. **(08 Marks)**
 b. Define and classify attacks. **(06 Marks)**
 c. Encrypt the message "Cryptography". Using play fair cipher with key "MONARCHY". **(06 Marks)**

2 a. Encrypt the plaintext "COMPUTER" using Hill cipher technique key
$$K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$$
 [Hint: a = 0, b = 1, ... z = 25]. **(08 Marks)**
 b. With neat diagram, explain single Round DES encryption. **(08 Marks)**
 c. Explain counter mode of operation. Mention its advantages. **(04 Marks)**

3 a. What requirements must a public key cryptosystem fulfill to be a secure algorithm? **(06 Marks)**
 b. Explain different techniques proposed for distribution of public keys. **(08Marks)**
 c. Discuss Diffie Hellman key exchange algorithm. **(06 Marks)**

4 a. Describe the requirements for a Hash function. **(06 Marks)**
 b. With diagrams, explain two approaches of digital signatures. **(06 Marks)**
 c. Write digital signature algorithm, explain the signing and verifying function of digital signature algorithm. **(08 Marks)**

5 a. Explain various phases of SSL handshake protocol. **(10 Marks)**
 b. Discuss the sequence of events that are required for a transaction of SET. **(10 Marks)**

6 a. Briefly explain Three Classes of Intruders. **(06 Marks)**
 b. Explain Unix Password Scheme with neat diagrams. **(06 Marks)**
 c. Explain password selection strategies in detail. **(08 Marks)**

7 a. Explain various phases of a virus. **(04 Marks)**
 b. Write a note on :
   i) Zombie
   ii) Logic Bomb. **(06 Marks)**
 c. Explain the following advanced antivirus techniques
   i) Digital Immune system
   ii) Behaviour blocking software **(10 Marks)**

8 a. Explain the various types of firewall configuration with relevant diagram. **(10 Marks)**
 b. Discuss the concept of reference monitor with diagram. Explain rules of multilevel security and security rules of reference monitor. **(10 Marks)**

* * * * *