U.S.N.										

B.M.S. College of Engineering, Bengaluru-560019

Autonomous Institute Affiliated to VTU

February / March 2023 Semester End Main Examinations

Programme: B.E. **Semester: VII**
Branch: ES – Cluster Elective **Duration: 3 hrs.**
Course Code: 19EC7CE2NC **Max Marks: 100**
Course: Network Security and Cryptography **Date: 28.02.2023**

Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

Important Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

UNIT - I

1 a) Describe X.800 security services, mechanisms and attacks in detail. **10**

b) Construct the cipher text for plain Text- "where there is a will there is a way" using the key matrix = $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ using Hill Cipher technique. **10**

UNIT - II

2 a) What is a digital signature? List the requirements for a digital signature and also the different types of digital signature functions. **10**

b) Discuss the modes of block cipher operation in detail. **10**

OR

3 a) Discuss the purpose, limitation, algorithm for Diffie-Hellman key exchange with an example. **10**

b) Discuss the digital signature standard in detail. **10**

UNIT - III

4 a) Describe the sequence of events that are required in a secured electronic transaction. **10**

b) What is the need of Intrusion Detection? Discuss the Intrusion detection approaches in detail. **10**

OR

5 a) Define VIRUS in Computer Terminology. Discuss its phases and types. **10**

b) Define a Firewall. List its design goals. Discuss the firewall configuration in detail. **10**

UNIT - IV

6 a) What is the goal of an incident response? Discuss the distinct phases of a good Incident Response plan. **10**

b) Define digital forensics. Enlist the possible steps to be taken for digital forensics or cybercrime investigation. **10**

UNIT - V

7 a) Describe the practical cryptographic implementation using Microsoft.NET **10**

b) Using Java programming, Discuss the practical cryptographic implementation. **10**

****