CBCS SCHEME

USN □□□□□□□□□□

17CS61

Sixth Semester B.E. Degree Examination, Jan./Feb.2021
Cryptography, Network Security and Cyber Law

Time: 3 hrs. Max. Marks: 100

Note: *Answer any FIVE full questions, choosing ONE full question from each module.*

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

Module-1

1 a. List and explain the various types of Vulnerabilities with common cyber attack. **(06 Marks)**

b. Write the extended Euclidean algorithm with an example. **(08 Marks)**

c. Encrypt the plaintext "ATTACK" using Hill Cipher technique with key matrix.

$$K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}.$$ **(06 Marks)**

OR

2 a. With neat schematic, explain the single round of DES encryption model. **(08 Marks)**

b. Explain three round SPN network. **(08 Marks)**

c. Distinguish between confusion and diffusion cipher. **(04 Marks)**

Module-2

3 a. Illustrate the RSA algorithm for encryption and decryption. In RSA system, it is given p = 03, q = 11 and M = 5. Find the Cipher 'C' and message 'M' from decryption. **(10 Marks)**

b. Define Hash function. Explain its basic properties. **(06 Marks)**

c. Explain Birthday attack. **(04 Marks)**

OR

4 a. With a diagram, explain the process of computing Hash function using SHA-1 algorithm. **(08 Marks)**

b. Explain the working of Diffie-Hellman key exchange protocol. **(08 Marks)**

c. Briefly explain Public Key Cryptography Standards (PKCS). **(04 Marks)**

Module-3

5 a. What is digital certificate? Explain the X.509 digital certificate format. **(08 Marks)**

b. Explain Password based one way authentication. **(06 Marks)**

c. Explain Needham-Schroeder protocol version--1. **(06 Marks)**

OR

6 a. Explain Kerberos message sequence with diagram. **(08 Marks)**

b. List and explain PKI architecture. **(06 Marks)**

c. What is Secure Socket layer? Explain SSL hand shake protocol. **(06 Marks)**

Module-4

7 a. Explain how 802.111 provides message confidentiality and integrity. **(08 Marks)**

b. Define firewall. List and explain practical issues of firewall. **(08 Marks)**

c. Briefly explain DDOS attack prevention and detection. **(04 Marks)**

OR

8 a. What is Instrusion Detection System (IDS). Explain different types of IDS. **(06 Marks)**
b. Explain the characteristics of virus and worms. **(06 Marks)**
c. Explain technologies for Web services. **(08 Marks)**

Module-5

9 a. Explain digital signature certificates. **(06 Marks)**
b. Describe the duties of subscribers. **(06 Marks)**
c. List and explain functions of controller. **(08 Marks)**

OR

10 a. List and explain the objectives and scope of IT ACT 2000. **(08 Marks)**
b. Explain the various OFFENCES and Punishments on cyber crime. **(06 Marks)**
c. Explain the process of attributions, acknowledgement and dispatch of electronic records. **(06 Marks)**

* * * * *