CBCS SCHEME

USN | | | | | | | | | | |

17CS61

Sixth Semester B.E./B.Tech. Degree Examination, Dec.2025/Jan.2026
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.***

Module-1

1 a. Which are protocol and software vulnerabilities? How are these used to attack a network? **(06 Marks)**

b. How can different defense strategies be applied to thwart common attacks on a network? **(10 Marks)**

c. Why diffusion and confusions are essential in developing a cipher? **(04 Marks)**

OR

2 a. How a monoalphabetic cipher works? How can it be attacked? **(08 Marks)**

b. Explain the working of a transposition cipher. **(08 Marks)**

c. How are intrusion and interruption attacks applied on a computer network? **(04 Marks)**

Module-2

3 a. Explain Diffie – Hellman key exchange protocol. Two parties A and B use Diffie – Hellman key exchange protocol with p = 23 and g = 5. If the initial secret choose by A = 6 and B = 15, compute the common secret that both sides compute. **(10 Marks)**

b. List and explain the properties of Hash function. What are the applications of Hash functions? Explain any 4. **(10 Marks)**

OR

4 a. Demonstrate how Jennifer and Ted share are asymmetric secret communication. Jennifer creates a pair of key for herself. She chooses p = 7, q = 11 and e = 13. Suppose Ted wants to send a message NO to Jennifer, model this with a neat diagram. Ted knows e and n. **(10 Marks)**

b. With a sketch, explain the process of computing Hash of a message using SHA – 1. **(10 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 Four-Way handshake in 802.11i. **(06 Marks)**

b. With a flow chart show the tasks performed by an IDS. **(06 Marks)**

c. Which are the types of a firewall? How do they work? **(08 Marks)**

OR

8 a. What is an worm? Which are its characteristics? **(06 Marks)**

b. Which are the practical issues occur while implementing a firewall? **(06 Marks)**

c. How XML is used in secured web services? Explain XML encryption. **(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)**

* * * * *