CBCS SCHEME

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

17CS61

Sixth Semester B.E. Degree Examination, June/July 2024
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. 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. Justify how challenge response protocol prevents replay attack. **(08 Marks)**

b. What is Reflection attack? Demonstrate it with a diagram. **(06 Marks)**

c. Explain Encryption key exchange protocol with a diagram. **(06 Marks)**

OR

6 a. Discuss the problems in earlier versions of Needham – Schroeder protocols. How are they fixed in the Final version? **(08 Marks)**

b. What are IP Sec cookies? Explain its significance in Internet key exchange protocol. **(04 Marks)**

c. What is Secure Socket layer? Explain the main steps in SSL handshake protocol, with a neat diagram. **(08 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)

* * * * *