CBCS SCHEME

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

17CS61

Sixth Semester B.E. Degree Examination, Feb./Mar. 2022
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. List and explain any 6 different types of Cyber attacks. **(06 Marks)**

b. Make use of Fiestel structure to construct and explain a single round of DES model. List the different DES modes of operation. **(08 Marks)**

c. Write the Extended Euclidean Algorithm. Apply this algorithm to find the inverse of 23 Modulo 100. **(06 Marks)**

OR

2 a. Apply Chinese Remainder Theorem to find square roots of 3 Modulo 143 and list them. **(08 Marks)**

b. Apply Hill Cipher technique to encrypt and decrypt the plain text CRYPTO with key matrix.

$$K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}.$$ **(08 Marks)**

c. Distinguish between :
i) Confusion and Diffusion Ciphers ii) Block and Stream Ciphers. **(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. 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. What are the main functions of Firewall? List Firewall types and explain any two. **(08 Marks)**

b. What is Anomaly and Signature intrusion detection system? Give example. **(04 Marks)**

c. Explain key hierarchy in WLAN. What are the goals in four – way handshake in 802.11i? Explain with a neat diagram. **(08 Marks)**

OR

8 a. What are the functions of WS security? Explain token type with an example. **(07 Marks)**

b. What is IP trace back? Explain the principle of packet marketing. **(07 Marks)**

c. Explain how Simple Epidemic Model can be used. Determine the number of infected machines. **(06 Marks)**

Module-5

9 a. What is IT Act 2000? What are its aim and objectives? **(06 Marks)**

b. List and discuss the important provisions of IT Act 2000. **(06 Marks)**

c. What is a digital signature certificate? How is it issued and under what circumstances it is revoked? **(08 Marks)**

OR

10 a. What is the Cyber Regulation Appellate Tribunal? Highlight the powers of this Appellate tribunal. **(08 Marks)**

b. Discuss OFFENCES defined under IT Act 2000. **(08 Marks)**

c. List the penalties and adjudication defined under IT Act 2000. **(04 Marks)**

* * * * *