RAMAIAH Institute of Technology

Department of Computer Science and Engineering

Academic Year 2024-2025(Odd)
SAMPLE QUESTIONS - UNIT 3, 4 & 5(Text Book 2-Chapter 20 – Intruders)

Course: CRYPTOGRAPHY AND NETWORK SECURITY **Course Code: CSE555**
Semester: V **Section: A,B,C**

UNIT 3

1. List and explain the different modes of operation designed to be use with modern block ciphers?
2. Write an encryption algorithm for RC4 and explain it with example.
3. Explain Secret communication with Knapsack Cryptosystem.
4. Assume that a=[3, 7, 12, 30, 60,115] and s = 82 . Find tuple x using inv_knapsack sum.
5. Write RSA Algorithm.
   Bob chooses 13 and 11 as p and q and calculates n value. Find the value of φ(n). Find the two exponents e and d. Now assume that Alice wants to send the plain text 13 to Bob. Find the cipher text and decrypt it on receiving side to get plaintext using RSA algorithm.
6. Describe the taxonomy of potential attacks on RSA.
7. Explain optimal asymmetric encryption padding with neat block diagram.
8. Draw the block diagram for encryption, decryption and key generation for Rabin cryptosystem.
9. Illustrate ElGamal Encryption and decryption algorithm.

UNIT 4& UNIT 5

1. Explain the following uses of message encryption with neat diagram.
   i. Symmetric encryption.
   ii. Public key encryption.
2. Illustrate the limitations of the Kerberos Version 4 with respect to environmental shortcomings and technical deficiencies.
3. With a neat diagram, illustrate the generation of a public-key certificate.
4. Discuss about Revocation of Certificate.
5. Describe with a neat diagram, the Digital signature algorithm Signing and Verifying.
6. Discuss various types of attacks identified in message authentication requirements.
7. Discuss the general format and elements of X.509 certificate.
8. Summarize the Message Exchanges of Kerberos version 4.
9. Illustrate secret key distribution with confidentiality and authentication.
10. Explain the use of Message authentication and confidentiality when authentication tied to plaintext and cipher text with an example.
11. What are the environmental shortcomings of Kerberos4? How does Kerberos 5 address them?
12. Delineate the different message authentication functions with neat diagrams.