Atal Bihari Vajpayee Indian Institute of Information Technology & Management, Gwalior

IT403: Cryptography

Major Examination (Session 2024–25)

Maximum Time: 3 Hours **Max Marks: 70**

Note: Answer all questions. Wherever possible, illustrate with examples or calculations.

1. (a) Explain substitution-permutation networks. Why are they fundamental in block cipher design? (b) Draw and explain one round of the AES encryption process. (10 Marks)

2. (a) Perform encryption and decryption using RSA for the following: $p = 19, q = 23, e = 5, M = 15$. (b) Discuss how padding (OAEP) improves RSA security. (12 Marks)

3. Compare the security and performance of DES, 3DES, and AES. Which one is considered secure today and why? (8 Marks)

4. (a) What is a digital certificate? Explain the role of a Certificate Authority (CA). (b) Discuss Kerberos authentication protocol. (10 Marks)

5. **Case Study:** A government organization wants to secure confidential files shared between departments. The requirements are: - Confidentiality against outside attackers - Integrity of documents during transfer - Authentication of officials accessing files

   Design a cryptographic framework (algorithms, key management, protocols). Justify each choice. (15 Marks)

6. Write short notes on any three: (i) Elliptic Curve Diffie–Hellman (ECDH) (ii) Man-in-the-Middle Attack in key exchange (iii) Zero Knowledge Proofs (iv) Applications of Hash Functions beyond security (15 Marks)