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

IT023: Cryptography and Network Security

Major Examination (Session 2023–24)

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

Note: Attempt all questions. Marks for each question are indicated.

1. (a) What are substitution ciphers? Explain Caesar cipher with example. (4 Marks)
   (b) Prove that the key space of affine cipher is limited. (4 Marks)

2. Apply RSA encryption and decryption for $p = 17, q = 11, e = 7$, message $M = 8$. Show key generation, encryption, and decryption steps. (10 Marks)

3. (a) Explain the structure of DES algorithm with diagram. (6 Marks) (b) Compare DES with AES in terms of security and efficiency. (6 Marks)

4. Write short technical notes on (2 marks each): (a) Hash collisions (b) SSL/TLS (c) IPsec (d) Man-in-the-middle attack (8 Marks)

5. **Case Study:** A company is setting up a secure e-commerce platform. They need: - Secure customer authentication - Encrypted communication channel - Digital certificates for transactions

   Propose a complete cryptographic architecture. Include choice of algorithms (RSA, AES, TLS, Certificates, etc.) and justify. (16 Marks)

6. (a) Explain Kerberos authentication protocol. (6 Marks) (b) Differentiate between symmetric key and asymmetric key cryptography. Give examples. (6 Marks)

7. Discuss the role of Intrusion Detection Systems (IDS) in network security. Differentiate between signature-based and anomaly-based IDS with examples. (10 Marks)