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

IT023: Cryptography and Network Security

Major Examination (Session 2024–25)

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

Note: Attempt all questions. Internal choice is provided where applicable.

1. (a) Differentiate between block cipher and stream cipher with examples. (4 Marks)
   (b) Discuss the concept of avalanche effect in cryptographic design. (4 Marks)

2. **(Numerical)** Use RSA with $p = 17, q = 19, e = 7$ to encrypt the message $M = 10$. Show key generation, encryption, and decryption. (10 Marks)

3. (a) Explain DES structure with diagram. (6 Marks) (b) Compare DES, 3DES, and AES. (6 Marks)

4. Attempt any **two**: (a) SHA-256 algorithm and its applications (6 Marks) (b) Role of Digital Signatures in e-Governance (6 Marks) (c) Difference between IDS and Firewalls (6 Marks)

5. **Case Study (15 Marks):** A multinational bank wants to secure its online transactions against eavesdropping and identity theft. Requirements: - Strong encryption of transaction data - Authentication of customers - Prevention of phishing and replay attacks

   Propose a cryptographic framework (algorithms + protocols) for the bank. Justify your design.

6. (a) Explain Kerberos authentication mechanism with diagram. (6 Marks) (b) What is Public Key Infrastructure (PKI)? How does it work? (6 Marks)

7. Write short notes (2 marks each): (a) IPsec (b) SSL/TLS (c) Zero-knowledge proof (d) Man-in-the-middle attack (8 Marks)