विश्वजीवनामृतं ज्ञानम्

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

IT403: Cryptography

Major Examination (Session 2023–24)

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

Note: Answer all questions. Case study must be attempted with clear reasoning.

1. (a) Define cryptanalysis. Explain the difference between brute-force attack and differential cryptanalysis. (b) Show with an example how frequency analysis can be applied to break a monoalphabetic cipher. (10 Marks)

2. (a) Explain the RSA algorithm. Perform encryption and decryption for: $p = 7, q = 17, e = 5, M = 8$. (b) Discuss the significance of key size in RSA security. (12 Marks)

3. Compare stream ciphers and block ciphers with suitable examples. Which one is better for real-time applications? Why? (8 Marks)

4. (a) Define Message Authentication Code (MAC) and explain its difference from Digital Signatures. (b) How does SHA-256 ensure collision resistance? (10 Marks)

5. **Case Study:** A multinational company is planning to secure its internal communication. It wants: - Secure e-mail exchange - Employee authentication - Protection against message tampering

   Propose a complete cryptographic solution. Mention specific algorithms and justify why they are chosen. (15 Marks)

6. Write short notes on any three: (i) Elliptic Curve Cryptography (ECC) (ii) Kerberos Authentication Protocol (iii) Digital Certificates and PKI (iv) Applications of Cryptography in Blockchain (15 Marks)