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

IT403: Cryptography

Minor Examination (Session 2023–24)

Maximum Time: 1 Hour **Max Marks: 20**

Note: Attempt all questions. Justify your answers with examples wherever possible.

1. Define cryptography. Differentiate between symmetric key and public key cryptography with examples. (4 Marks)

2. Encrypt the word HELLO using the Caesar cipher with key = 5. Show all steps. (4 Marks)

3. What is a one-way hash function? Explain its role in digital signatures. (4 Marks)

4. A message needs to be transmitted over an insecure channel. Suggest a cryptographic mechanism to ensure **(i) confidentiality, (ii) authentication, (iii) integrity**. (4 Marks)

5. Write short notes on any one: (a) Playfair cipher (b) Diffie–Hellman Key Exchange (4 Marks)