विश्वजीवनामृतं ज्ञानम्

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

IT023: Cryptography and Network Security

Minor Examination (Session 2023–24)

Maximum Time: 1.5 Hours **Max Marks: 30**

Note: Attempt all questions. Wherever possible, illustrate with examples.

1. Define the following (2 marks each): (a) Cryptanalysis (b) Stream Cipher (c) Replay Attack (6 Marks)
2. Encrypt the plaintext `SECURE` using Playfair cipher with keyword = ”NETWORK”. Show matrix and steps. (7 Marks)
3. Explain how Diffie–Hellman key exchange works. Use $p = 23$, $g = 5$, private keys $a = 6$, $b = 15$ to compute the shared secret. (9 Marks)
4. Differentiate between Message Authentication Code (MAC) and Digital Signature with neat diagrams. (4 Marks)
5. Briefly explain the concept of Firewall and IDS. (4 Marks)