



विश्वजीवनमृतं ज्ञानम्

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

IT023: Cryptography and Network Security

Minor Examination (Session 2024–25)

Maximum Time: 1 Hour

Max Marks: 25

Note: Attempt all questions. Neat and logical steps carry weight.

1. Answer briefly (2 marks each): (a) Steganography vs Cryptography (b) One-time pad (c) Passive attack example (6 Marks)
2. Encrypt the plaintext HELLO using Vigenère cipher with keyword = "KEY". Show steps. (6 Marks)
3. Explain the working of RSA algorithm. Compute public/private keys for $p = 7, q = 13, e = 5$. Find ciphertext for $M = 9$. (8 Marks)
4. Write short notes (any two): (a) Digital Certificates (b) Replay Attack (c) Hash functions in Blockchain (5 Marks)