विश्वजीवनामृतं ज्ञानम्

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

IT403: Cryptography

Minor Examination (Session 2024–25)

Maximum Time: 1.5 Hours **Max Marks: 25**

Note: Attempt all questions. Neat diagrams are expected where necessary.

1. Explain the differences between classical ciphers and modern block ciphers. Give one example of each. (5 Marks)
2. Encrypt the plaintext `ATTACK` using a Rail Fence cipher with depth $= 3$. Show all steps. (5 Marks)
3. In RSA, $p = 11$, $q = 13$, $e = 7$. (a) Compute n and $\phi(n)$. (b) Find the private key d. (c) Encrypt message $M = 9$. (8 Marks)
4. What is Diffie–Hellman key exchange? Explain with a small numerical example. (4 Marks)
5. Write short notes on: (a) Avalanche Effect in DES (b) Digital Signatures (3 Marks)