

UNIT-II

Part – A (Short Answer Questions)

S.No	Questions	BT	CO	PO
1	Define block cipher.	L1	CO2	PO2
2	What is DES?	L1	CO2	PO2
3	Expand AES.	L1	CO2	PO2
4	What is Blowfish algorithm?	L1	CO2	PO2
5	Define RC4.	L1	CO2	PO1
6	What is public key cryptography?	L1	CO2	PO1
7	Define RSA algorithm.	L1	CO2	PO2
8	What is Diffie–Hellman key exchange?	L1	CO2	PO1
9	Define digital envelope.	L1	CO2	PO1
10	What is ElGamal cryptography?	L1	CO2	PO1

Part – B (Long Answer Questions)

1	Explain the DES algorithm with neat block diagram.	L2	CO2	PO3
2	Describe the AES encryption algorithm in detail.	L2	CO2	PO2
3	Explain the working of RSA algorithm with example.	L2	CO2	PO3
4	Compare symmetric and asymmetric key cryptography.	L2	CO2	PO5
5	Explain Diffie–Hellman key exchange algorithm.	L2	CO2	PO3
6	Explain the principles of public key cryptosystems and their applications.	L2	CO2	PO1
7	Discuss stream ciphers and compare stream ciphers with block ciphers.	L2	CO2	PO3
8	Explain the Knapsack Cryptosystem and its working mechanism.	L2	CO2	PO2
9	Explain the ElGamal Cryptographic Algorithm with suitable examples			
10	Explain the working of RSA algorithm with example.	L2	CO2	PO3