

## MODULE- II

SYMMETRIC KEY CIPHERS: SDES – Block Ciphers – DES, Strength of DES – Differential and linear cryptanalysis – Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES– Pseudorandom Number Generators– RC4 –Key distribution

Sl No.	Question	Mark	BT Level
1	Differentiate between stream cipher and block cipher.	5	L3
2	What is meant by confusion and diffusion in cryptography?	5	L3
3	Differentiate between DES and AES encryption algorithms.	5	L3
4	List the different modes of operation in block ciphers.	5	L2
5	Distinguish between ECB and CBC modes of operation.	5	L3
6	Define pseudorandom number generator. What is RC4?	5	L3
7	Explain the DES algorithm with a neat block diagram	10	L2
8	Describe the AES encryption algorithm with a block diagram. Explain the four transformations used in AES.	10	L2
9	Illustrate ECB mode and CBC mode of block cipher operation with diagrams. Compare their features.	10	L3
10	Perform SDES encryption for plaintext “11001100” with key “0111111101”. Show the steps for key generation and encryption process.	10	L3