

## MODULE- I

**Computer Security Concepts** – The OSI Security Architecture – Security Attacks – Security Services and Mechanisms – A Model for Network Security – Classical encryption techniques: Substitution techniques, Transposition techniques, Steganography – Foundations of modern cryptography: Perfect security – Information Theory – Product Cryptosystem – Cryptanalysis.

SI No.	Question	Mark	BT Level
1	Distinguish between passive attack and active attack	5	L3
2	Define cryptography. Distinguish between Encryption and Decryption.	5	L4
3	Define security mechanisms.	5	L3
4	Summarize the difference between Substitution and Transposition techniques.	5	L3
5	Differentiate symmetric and asymmetric encryption?	5	L4
	Given Cipher text “YMJTYMJWXNIJTKXNQJSHJ”, the message is encrypted by shift cipher and k=5. Try to decrypt the message.	5	
6	Define Steganography.	5	L3
7	Explain the network security model and its important parameters with a neat block diagram.	10	L4
8	Encrypt and decrypt the following using play fair cipher using the keyword “gandhiengineeringcollege”. Use X for filter letter. Given plain text: “BALLOON”, cipher text: “OIRXPCUPPCRH”.	10	L4
9	Describe Hill Cipher and perform encryption using Hill Cipher for the following. Message: PAY and Key: $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$	10	L4
10	Using the Vigenère cipher, encrypt the message “we are discovered save yourself” using the word “deceptive”.	10	L4

