GEETHANJALI INSTITUTE OF SCIENCE & TECHNOLOGY: NELLORE
Department of Computer science &Engineering CSE (CYBER SECURITY)

Subject: (CRYPTOGRAPHY AND NETWORK SECURITY)

Class : II Year II Sem **Academic Year : 2023-24**

Branch : CSE(Cyber Security) **Name of the Faculty : Mr.V.Chaithanya**

UNIT-I

S.No	Question	CO	BL	Marks
1.	Explain Cryptography Security Architecture (Attacks, Mechanism and Services)?	1	2	10
2.	What is Active and Passive Attacks in network security?& Differentiate between them?	1	2	10
3.	What is need for security?&Explain the Principles of security in Cryptography?	1	2	10
4.	What is Symmetric and Asymmetric key cipher model?&Differentiate between them?	1	2	10
5.	(a) Apply Caesar Cipher to Encrypt the word "GEETHANJALI" (assume key as 5) (b) Apply Playfair cipher to Encrypt the word "SECRET WRITTINGS" using key "GIST"	1	3	10
6.	Explain Substitution & transposition techniques with Suitable examples?	1	3	10
7.	Differentiate Between Monoalphabetic ciphers and Polyalphabetic ciphers?	1	2	10
8.	Explain possible types of attacks in Cryptography?	1	2	10
9.	Explain Suitable Model for Network Security and its elements in cryptography?	1	3	10
10.	What is the importance of "key range and key size" of a Crypto System?&Explain Steganography with a neat sketch?	1	2	10
11.	Define the following terms (a). Threat(b). Attack(c). DoS Attack(d). Brute Force Attack.	1	1	10
12.	What is plain text& Cipher text?&Explain with its Encryption &Decryption Algorithms with a neat sketch?	1	2	10

UNIT-II

S.No	Question	CO	BL	Marks
1.	Explain Block Cipher principles in Symmetric key cryptography ?	2	2	10
2.	Explain Data Encryption Standard Algorithm with a neat sketch?	2	2	10
3.	Explain Advanced Encryption Standard Algorithm with a neat sketch?	2	2	10
4.	Write a short note on Blowfish Algorithm& key Distribution?	2	2	10
5.	Explain Block cipher modes of operation in in Symmetric key cryptography?	2	2	10
6.	Explain RC4 algorithm with Suitable example?	2	2	10
7.	Explain Principles of public key cryptosystems in Asymmetric key cryptography?	2	2	10
8.	Explain Rivest Shamir Adleman Algorithm with example?	2	3	10
9.	Write a short note on Elliptic Curve Cryptography with suitable examples?	2	2	10
10.	Explain Diffie- Hellman key Exchange Cryptography with suitable examples?	2	2	10
11.	Define the following : (a). Stream cipher (b). Private Key (c)Man in the Middle Attacks (d) Cryptanalysis?	2	1	10

UNIT-III

S.No	Question	CO	BL	Marks
1.	Describe generation of Hash Function based on Cipher Block Chaining	3	1	10
2.	Explain Applications of Hash Functions?	3	1	10
3.	Demonstrate SHA-512 Algorithm?	3	3	10
4.	Demonstrate Message Authentication Code (MAC) role in integrity check	3	3	10
5.	Explain MD5 algorithm?	3	2	10
6.	Explain Message authentication Requirements?	3	2	10
7.	Explain Requirements and Security of Hash Functions	3	2	10
8.	Write HMAC Algorithm	3	1	10
9.	Write CMAC Algorithm	3	1	10
10.	Explain Whirlpool algorithm?	3	1	10
11.	Explain knapsack algorithm?	3	2	10
12.	Explain DSA and Digital Signatures Signature Algorithm?	3	2	10

UNIT-IV

S.No	Question	CO	BL	Marks
1.	Explain Pretty Good Privacy for e-mail security?	4	2	10
2.	Write S/MIME standers for e-mail security?	4	2	10
3.	(a). Explain Applications and Advantages of IPSec **(5 M)** (b). Explain IPSec Protocols **(5 M)**	4	2	10
4.	Explain Authentication Header (AH) ?	4	2	10
5.	Explain Encapsulating Security Payload (ESP) ?	4	2	10
6.	Describe IPSec Key Management ?	4	2	10
7.	Explain security associations in IPSec	4	2	10
8.	Explain the following (a). VPN **(4 M)** (b).Tunnel Mode **(4 M)** (b). HTTPS **(2 M)**	4	2	10
9.	Explain Formats of 'ESP' and 'AH'?	4	2	10
10	Compare PGP with S/MIME?	4	1	10

UNIT-V

S.No	Question	CO	BL	Marks
1.	Summarize SSL Architecture	**5**	**2**	10
2.	Explain job of four protocols of SSL?	**5**	**2**	10
3.	Draw SSL message formats?	**5**	**2**	10
4.	Explain Transport Layer Security Mechanism?	**5**	**2**	10
5.	Explain Secure Electronic Transaction (**SET**)	**5**	**2**	10
6.	What is Firewall? Explain various types of Firewalls?	**5**	**1**	10
7.	Explain a. Virus related threats **(5 M)** b. IP SPOOFING ATTACKS **(5 M)**	**5**	**2**	10
8.	Explain Intrusion Detection (IDS) and Intrusion Prevention System (IPS)	**5**	**2**	10
9.	Explain (a). Password management (b). Network Address Translation (NAT)	**5**	**2**	10
10	Describe Firewall Possible Configurations	**5**	**1**	10
11	Demonstrate Virtual Elections	**5**	**3**	10
12	Demonstrate Cross site Scripting Vulnerability with examples	**5**	**3**	10