MALLA REDDY UNIVERSITY

Department of Computer Science and Engineering

Subject Name: CRYPTOGRAPHY & NETWORK SECURITY

Subject Code: MR22-1CS0109

Year & Semester: III Year - II Semester

Unit-Wise Question Bank

Qno	Question	Marks	Section	UNIT
1	Explain the concept of CIA principle of security with examples.	8M	Section-I	1
2	Demonstrate substitution techniques in classical cryptography with examples	8M	Section-I	1
3	Let message = "INDIAN NAVY", Ignore the space between words. Keyword = "MRUH", find cipher-text using playfair cipher.	8M	Section-I	1
4	Discuss examples from real life, where the following security objectives are needed: i) Authentication ii) Authorization iii) Non-repudiation. Suggest suitable security mechanisms to achieve them.	8M	Section-I	1
5	Define cryptography and its type. Explain following basic terms with example. i) Plain Text ii) Cipher Text iii) Encryption iv) Decryption	8M	Section-I	1
6	Define steganography? Discuss the role of steganography in augmenting the corporation's security posture, including practical applications and potential challenges.	8M	Section-I	1
7	Explain active and passive attack with example.	8M	Section-I	1
8	What is the role of Key Range and Key Size of different types of ciphers? Explain it with examples.	8M	Section-I	1
9	Encrypt the message "I AM INDIAN" using Caesar cipher with key = 15. Ignore the space between words. Decrypt the message to get the Original plaintext.	8M	Section-I	1
10	Differentiate Substitution Techniques and Transposition Techniques?	8M	Section-I	1
11	Explain following Algorithm Types with example: i) Block Cipher ii) Stream Cipher	8M	Section-II	2
12	List out difference between Differential and Linear Cryptanalysis.	8M	Section-II	2
13	What do you mean by DES? Diagrammatically illustrate the structure of DES & describe the steps in DES encryption process with example	8M	Section-II	2
14	Elaborate the encryption and key schedule operations of AES Algorithm.	8M	Section-II	2
15	Describe International Data Encryption (IDEA) algorithm with its Key generation, encryption and its applications in Cyber security world.	8M	Section-II	2
16	Explain about Blowfish Algorithm with focus on Key generation and Encryption and Decryption process.	8M	Section-II	2
17	Explain following Algorithm Modes with example: i) Electronic Code Book (ECB) ii) Cipher Block Chaining (CBC), Iii) Cipher Feedback (CFB) iv) Output Feedback (OFB).	8M	Section-II	2
18	What are different block cipher algorithms? Explain each algorithm with a suitable diagram and also present the pros and cons of each algorithm.	8M	Section-II	2

19	Explain about symmetric key cryptography with examples.	8M	Section-II	2
20	Calculate the cipher text with Knapsack weight value D=1, 2, 4,10,20,40 and Plain Text value 100100 111100 101110.	8M	Section-II	2
21	Compare and contrast on Asymmetric and Symmetric Key cryptography with suitable parameters.	8M	Section-III	3
22	Explain the concept of RSA Algorithm. Describe Security Analysis of RSA.	8M	Section-III	3
23	Write and explain the Digital Signature Algorithm.	8M	Section-III	3
24	Illustrate the working of MD-5. List out difference between MD5 and MD4.	8M	Section-III	3
25	Write a short notes on Secure Hash Algorithms with examples.	8M	Section- III	3
26	Define Public Key Infrastructure (PKI) and explain its role in ensuring secure communication on the internet. How does PKI utilize digital certificates for authentication and encryption?	8M	Section- III	3
27	Explain the PKIX model and its significance in establishing trust relationships within a PKI ecosystem.	8M	Section- III	3
28	Compare and contrast SSL with Secure Hypertext Transfer Protocol (SHTTP) in terms of security mechanisms, compatibility, and adoption.	8M	Section- III	3
29	Discuss the purpose and functionality of the Time Stamping Protocol in ensuring the integrity and authenticity of digital documents. How does time stamping contribute to non-repudiation in electronic transactions?	8M	Section- III	3
30	Describe the advantages and disadvantages of symmetric and asymmetric-key cryptography.	8M	Section-III	3
31	Compare and contrast Secure Socket Layer (SSL) and Secure Electronic Transaction (SET) protocols in terms of their security features and suitability for different types of online transactions.	8M	Section-IV	4
32	What is the purpose of Public Key Infrastructure (PKI) in the context of digital certificates?	8M	Section-IV	4
33	Describe the role of XML (eXtensible Markup Language) in PKI and security. How is XML utilized in the representation and exchange of security-related information in web-based applications?	8M	Section-IV	4
34	Provide an overview of basic concepts in Internet Security Protocols. What are the primary objectives of these protocols, and how do they contribute to securing online communication?	8M	Section-IV	4
35	Explain the Secure Socket Layer (SSL) protocol and its role in providing secure communication over the internet. Discuss the key features, components, and handshake process of SSL.	8M	Section-IV	4
36	Discuss the role of 3-D Secure Protocol in enhancing the security of online card payments.	8M	Section-IV	4
37	What are Public Key Cryptography Standards (PKCS), and how do they standardize cryptographic operations within a PKI environment? Provide examples of commonly used PKCS standards and their applications.	8M	Section-IV	4
38	Explain Digital Certificate Creation Steps with suitable diagram.	8M	Section- IV	4
39	What do you mean by Private Key Management? Explain Mechanisms for protecting private keys	8M	Section- IV	4
40	Critically assess the security implications of using crypto currencies like Bitcoin in online transactions, considering factors such as anonymity, decentralization, and regulation.	8M	Section- IV	4
41	Explain the authentication standards Kerberos with suitable diagram.	8M	Section-V	5
42	Define the term "password authentication" and explain its basic process.	8M	Section-V	5
43	What are the security implications of implementing biometric authentication systems? How can these systems be protected against attacks and misuse?	8M	Section-V	5
44	What are the fundamental concepts of authentication, and why is it essential in information security?	8M	Section-V	5

45	Discuss the role and types of Firewall for organization level with suitable diagram.	8M	Section-V	5
46	Explain the concept of authentication tokens. What are the different types of authentication tokens, and how do they enhance security?	8M	Section-V	5
47	Describe the process of two-factor authentication (2FA). How does it enhance security compared to traditional password-based authentication?	8M	Section-V	5
48	Explain the role of E-mail Security. How PGP will help for E-mail security.	8M	Section-V	5
49	What is IP Security? Give brief note on IPSec Key Management.	8M	Section-V	5
50	Write a short Notes on: a) Virtual Private Networks b) Intrusion Detection	8M	Section-V	5