Course Code: 25MC9128 **R25**

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY::PUTTUR
(AUTONOMOUS)
Siddharth Nagar, Narayanavanam Road – 517583

QUESTION BANK (DESCRIPTIVE)

Subject with Code: Network Security (25MC9128) **Course & Branch**: MCA
Year & Sem: II-MCA & I-Sem **Regulation:** R25

UNIT-I
Fundamentals Of Security Mechanisms And Attacks

1		Explain security attacks. Classify and explain passive and active attacks with suitable examples.	**[L1][CO1]**	**[12M]**
2		Explain security services in detail. Discuss the objectives and applications of different security services.	**[L1][CO1]**	**[12M]**
3	**a)**	What is authentication? Explain the different authentication techniques.	**[L2][CO1]**	**[6M]**
	b)	Explain the advantages and limitations of various authentication methods.	**[L2][CO1]**	**[6M]**
4	**a)**	What is data integrity?	**[L2][CO1]**	**[6M]**
	b)	Explain different integrity checking techniques used in network security.	**[L2][CO1]**	**[6M]**
5		Explain digital signatures. Describe the generation and verification process with a neat diagram.	**[L1][CO1]**	**[12M]**
6		Explain in detail about hash algorithms	**[L2][CO1]**	**[12M]**
7		Explain security mechanisms in detail. Discuss different types of security mechanisms with suitable examples.	**[L2][CO1]**	**[12M]**
8		Explain the relationship between security attacks, security services, and security mechanisms.	**[L3][CO1]**	**[12M]**
9	**a)**	Explain digital signatures and authentication	**[L2][CO1]**	**[6M]**
	b)	Describe the role of hash algorithms in secure communication.	**[L2][CO1]**	**[6M]**
10		Explain the role of security attacks, security services, security mechanisms, authentication, digital signatures, integrity checking, and hash algorithms in network security with a neat diagram.	**[L2][CO1]**	**[12M]**

Course Code: 25MC9128 **R25**

UNIT-II

Symmetric Key Cryptography And Block Ciphers

1		What is block encryption? Explain the working principle of block cipher encryption with a neat diagram.	**[L1][CO2]**	**[12M]**
2	**a)**	Explain the overview and structure of the Data Encryption Standard (DES).	**[L1][CO2]**	**[6M]**
	b)	Explain the 16 rounds of DES with a neat block diagram.	**[L1][CO2]**	**[6M]**
3		Explain the different applications (uses) of Secret Key Cryptography with suitable examples.	**[L1][CO2]**	**[12M]**
4	**a)**	What are S-Boxes in DES? Explain their role in encryption.	**[L2][CO2]**	**[6M]**
	b)	Explain the key expansion (key schedule) process in IDEA.	**[L1][CO2]**	**[6M]**
5		Explain the overview and working of the International Data Encryption Algorithm (IDEA) with a neat diagram.	**[L2][CO2]**	**[12M]**
6	**a)**	Compare DES and IDEA.	**[L1][CO2]**	**[6M]**
	b)	Explain the advantages and disadvantages of DES and IDEA.	**[L1][CO2]**	**[6M]**
7		Explain the different modes of block cipher operation: ECB, CBC, OFB, and CFB with suitable diagrams.	**[L2][CO2]**	**[12M]**
8	**a)**	Explain the different rounds of IDEA with a neat diagram.	**[L3][CO2]**	**[6M]**
	b)	Describe the encryption and decryption process of IDEA.	**[L3][CO2]**	**[6M]**
9		Explain Multiple DES (Double DES and Triple DES). Discuss their working principles, advantages, and limitations.	**[L3][CO2]**	**[12M]**
10	**a)**	Explain the modes of operation ECB, CBC, OFB, and CFB with suitable examples.	**[L3][CO2]**	**[6M]**
	b)	Compare all four block cipher modes based on operation, security, advantages, disadvantages, and applications.	**[L2][CO2]**	**[6M]**

Course Code: 25MC9128 **R25**

UNIT-III

Hash Functions And Public Key Cryptography

1		Explain hash functions. Discuss the length of a hash, characteristics, uses, and applications of hash functions in network security.	**[L1][CO3]**	**[12M]**
2		Explain the MD2 algorithm. Describe its padding, checksum generation, and pass operations with a neat diagram.	**[L1][CO3]**	**[12M]**
3	**a)**	Explain the MD4 algorithm with its padding, stages, and digest computation.	**[L2][CO3]**	**[6M]**
	b)	Explain the MD5 algorithm with its padding, stages, and digest computation.	**[L2][CO3]**	**[6M]**
4		Explain the Secure Hash Standard (SHS). Discuss its overview, padding process, stages, and working algorithm with a suitable example.	**[L2][CO3]**	**[12M]**
5	**a)**	Explain modular arithmetic and discuss addition and multiplication operations with suitable examples.	**[L2][CO3]**	**[6M]**
	b)	Explain modular inverse and modular exponentiation with suitable examples.	**[L2][CO3]**	**[6M]**
6		Explain the RSA algorithm. Describe the process of key generation, encryption, and decryption with a suitable example.	**[L1][CO3]**	**[12M]**
7		Explain Zero-Knowledge Signatures. Discuss their working principle, advantages, limitations, and applications in secure communication.	**[L3][CO3]**	**[12M]**
8	**a)**	Explain the Diffie–Hellman Key Exchange algorithm with a neat diagram.	**[L3][CO3]**	**[6M]**
	b)	Explain the ElGamal Digital Signature algorithm with suitable examples.	**[L3][CO3]**	**[6M]**
9	**a)**	Compare MD2, MD4, MD5, and SHS based on their features, security, and applications.	**[L3][CO3]**	**[6M]**
	b)	Compare RSA, Diffie–Hellman, ElGamal, and DSS with respect to key generation, security, and applications.	**[L3][CO3]**	**[6M]**
10	**a)**	Explain the PKCS (Public Key Cryptography Standards) and its importance.	**[L2][CO3]**	**[6M]**
	b)	Explain the Digital Signature Standard (DSS) and its applications.	**[L2][CO3]**	**[6M]**

Course Code: 25MC9128 **R25**

UNIT-IV

Password Based And Cryptographic Authentication

1		Explain password-based authentication. Discuss the advantages and disadvantages of password authentication.	**[L1][CO4]**	**[12M]**
2		Explain passwords in distributed systems. Discuss online password guessing and offline password guessing attacks with suitable examples.	**[L2][CO4]**	**[12M]**
3	**a)**	Explain address-based authentication.	**[L1][CO4]**	**[6M]**
	b)	Explain cryptographic authentication with suitable examples.	**[L1][CO4]**	**[6M]**
4		Explain cryptographic authentication protocols. Discuss the role of authentication protocols in secure communication.	**[L2][CO4]**	**[12M]**
5	**a)**	Explain different techniques used for storing passwords securely.	**[L2][CO4]**	**[6M]**
	b)	Explain the concept of passwords as cryptographic keys.	**[L2][CO4]**	**[6M]**
6	**a)**	Explain the role of a Key Distribution Center (KDC) in authentication.	**[L2][CO4]**	**[6M]**
	b)	Explain certificate revocation and its importance in network security	**[L2][CO4]**	**[6M]**
7	**a)**	What are smart cards? Explain their applications in authentication.	**[L1][CO4]**	**[6M]**
	b)	Explain biometric authentication with its advantages and limitations.	**[L1][CO4]**	**[6M]**
8		Explain the authentication of people. Discuss different verification techniques, password policies, password length, password distribution methods, smart cards, and biometrics.	**[L3][CO4]**	**[12M]**
9	**a)**	Explain interdomain authentication.	**[L3][CO4]**	**[6M]**
	b)	Explain group authentication and delegation authentication with suitable examples.	**[L3][CO4]**	**[6M]**
10		Explain cryptographic authentication in detail. Discuss passwords as keys, authentication protocols, Key Distribution Center (KDC), certificate revocation, interdomain authentication	**[L2][CO4]**	**[12M]**

Course Code: 25MC9128 **R25**

UNIT-V

Security Policies And Advanced Authentication Mechanisms

1		What is a security policy? Explain the different types of security policies and discuss user-related security issues.	**[L1][CO5]**	**[12M]**
2		Explain protocol problems in network security. Discuss the assumptions made while designing secure authentication protocols.	**[L2][CO5]**	**[12M]**
3	**a)**	What is a shared secret protocol? Explain its working with a suitable example.	**[L1][CO5]**	**[6M]**
	b)	Explain public key protocols and compare them with shared secret protocols.	**[L1][CO5]**	**[6M]**
4		Explain the role of timestamps, nonces, and sequence numbers in authentication protocols. Compare their advantages and limitations.	**[L2][CO5]**	**[12M]**
5	**a)**	What is mutual authentication? Explain its importance in secure communication.	**[L2][CO5]**	**[6M]**
	b)	Explain reflection attacks and suggest methods to prevent them.	**[L2][CO5]**	**[6M]**
6	**a)**	What are session keys? Explain how session keys are generated and used in secure communication.	**[L2][CO5]**	**[6M]**
	b)	Discuss the advantages of session keys in network security.	**[L2][CO5]**	**[6M]**
7		Explain one-way public key-based authentication with a neat diagram. Discuss its advantages and applications.	**[L2][CO5]**	**[12M]**
8	**a)**	Explain two-way public key-based authentication with a neat diagram.	**[L3][CO5]**	**[6M]**
	b)	Differentiate between one-way and two-way public key-based authentication.	**[L3][CO5]**	**[6M]**
9	**a)**	Explain the working of mutual authentication using public key cryptography.	**[L3][CO5]**	**[6M]**
	b)	Describe how timestamps, nonces, and session keys improve the security of authentication protocols.	**[L3][CO5]**	**[6M]**
10		Discuss the role of security policies, authentication protocols, shared secret protocols, public key protocols, mutual authentication	**[L3][CO5]**	**[12M]**

Prepared by:

Department of MCA
SIETK