Course Code: 23CS0525 **R23**

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

QUESTION BANK (DESCRIPTIVE)

Subject with Code: CRYPTOGRAPHY & NETWORK SECURITY (23CS0525)

Regulation: R23

Course & Branch: B. Tech. - CSE & CSIT **Year & Sem. :** III - II

UNIT –I
Computer and Network Security Concepts

1	**a)**	Explain in detail about passive attacks with neat sketch.	**[L3, CO1]**	**5M**
	b)	Explain in detail about active attacks with neat sketch.	**[L3, CO1]**	**5M**
2	**a)**	List and Explain various Security Services	**[L2, CO2]**	**5M**
	b)	List and Explain various Security Mechanisms	**[L2, CO2]**	**5M**
3	**a)**	Explain the Caesar Cipher encryption technique with a suitable example	**[L2, CO1]**	**5M**
	b)	Define Mono-alphabetic Cipher, Polygram Substitution Cipher and explain its working principle with an example.	**[L2, CO1]**	**5M**
4	**a)**	Solve the playfair Using the keyword "MONARCHY", construct the 5×5 Playfair Cipher key matrix and encrypt the plaintext "INSTRUMENTS".	**[L4, CO1]**	**5M**
	b)	Explain the process of Steganography and differentiate it from Cryptography with suitable examples.	**[L2, CO3]**	**5M**
5	**a)**	Solve the plaintext "come Home Tomorrow" using the Rail Fence Cipher with a depth of 3. Show the step-by-step process of encryption and the resulting ciphertext.	**[L3, CO1]**	**5M**
	b)	Explain the working principle of the Simple Columnar Transposition Technique with an example	**[L2, CO3]**	**5M**
6		Describe the working of a Traditional Block Cipher Structure with Feistel Cipher Structure a neat block diagram	**[L3, CO2]**	**10M**
7		Explain the Data Encryption Standard by including the 16–round Feistel process.	**[L2, CO5]**	**10M**
8		Describe the internal structure of the Advanced Encryption Standard (AES) algorithm by explaining the key transformations	**[L2, CO1]**	**10M**
9		Explain the role of the various transformation functions used in AES encryption	**[L2, CO6]**	**10M**
10		Explain the Hill Cipher encryption technique and demonstrate the process of converting plaintext into ciphertext using matrix multiplication modulo 26. Provide a numerical example to illustrate the encryption steps	**[L3, CO6]**	**10M**

Course Code: 23CS0525 **R23**

UNIT –II
Conventional Encryption

1	**a)**	Define Modular Arithmetic and give one simple example.	**[L1,CO2]**	**[2M]**
	b)	What is the purpose of the Euclidean Algorithm in number theory?	**[L1,CO2]**	**[2M]**
	c)	State Fermat's Little Theorem.	**[L1,CO2]**	**[2M]**
	d)	What is the Discrete Logarithm Problem?	**[L1,CO2]**	**[2M]**
	e)	Define a finite field GF(p).	**[L1,CO2]**	**[2M]**
2	**a)**	Explain the Euclidean Algorithm with a suitable example.	**[L3,CO2]**	**[5M]**
	b)	Distinguish between Euclidean Algorithm and Extended Euclidean Algorithm.	**[L4,CO2]**	**[5M]**
3	**a)**	Describe Modular Arithmetic and its fundamental rules with examples.	**[L2,CO2]**	**[5M]**
	b)	Explain the application of modular arithmetic in cryptography.	**[L2,CO2]**	**[5M]**
4	**a)**	State and prove Fermat's Little Theorem.	**[L2,CO2]**	**[5M]**
	b)	Demonstrate the use of Fermat's theorem with an example.	**[L3,CO2]**	**[5M]**
5	**a)**	Explain Euler's Totient Function $\varphi(n)$ and compute $\varphi(21)$.	**[L5,CO2]**	**[5M]**
	b)	State Euler's Theorem and show how it is applied using a numeric example.	**[L3,CO2]**	**[5M]**
6	**a)**	State and explain the Chinese Remainder Theorem.	**[L2,CO2]**	**[5M]**
	b)	Solve the following using CRT: $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.	**[L3,CO2]**	**[5M]**
7	**a)**	What is the Discrete Logarithm Problem? Explain why it is considered computationally hard.	**[L2,CO2]**	**[5M]**
	b)	Discuss the importance of Diffie-Hellman with example	**[L3,CO2]**	**[5M]**
8	**a)**	Explain the structure and properties of finite fields GF(p).	**[L2,CO2]**	**[5M]**
	b)	Show how addition and multiplication are performed in GF(7) with an example.	**[L3,CO2]**	**[5M]**
9	**a)**	Describe finite fields of the form $GF(2^n)$.	**[L2,CO2]**	**[5M]**
	b)	Demonstrate multiplication in $GF(2^n)$ using polynomial representation.	**[L3,CO2]**	**[5M]**
10.	**a)**	Discuss the role of number theory in cryptography.	**[L2,CO2]**	**[5M]**
	b)	Compare prime fields and extension fields using examples.	**[L4,CO2]**	**[5M]**

Course Code: 23CS0525 **R23**

UNIT –III
Cryptographic Hash Functions

1		Explain the role of cryptographic hash functions in information security	**[L2, CO3]**	**10M**
2	**a)**	What are the key properties required for a secure cryptographic hash function?	**[L2, CO3]**	**5M**
	b)	How cryptographic hash functions are applied in digital signatures and block chain systems?	**[L2, CO3]**	**5M**
3		Explain the major applications of cryptographic hash functions with suitable examples.	**[L2, CO3]**	**10M**
4	**a)**	Explain the working of the Secure Hash Algorithm with a neat diagram.	**[L3, CO3]**	**5M**
	b)	Describe the applications of the Secure Hash Algorithm in information security.	**[L2, CO3]**	**5M**
5	**a)**	Explain the working of message authentication functions with a suitable example.	**[L3, CO4]**	**5M**
	b)	Describe different techniques used to achieve message authentication.	**[L2, CO4]**	**5M**
6	**a)**	Explain message authentication functions.	**[L2, CO4]**	**5M**
	b)	Explain the security issues and challenges in Public-Key Infrastructure.	**[L2, CO4]**	**5M**
7		Differentiate between HMAC and CMAC with suitable examples.	**[L4, CO4]**	**10M**
8		Explain digital signatures, their working principle, and applications	**[L2, CO4]**	**10M**
9	**a)**	Explain the working of the NIST Digital Signature Algorithm with a neat diagram.	**[L3, CO4]**	**5M**
	b)	Discuss the security properties of the Digital Signature Algorithm (DSA).	**[L2, CO4]**	**5M**
10		Discuss X.509 certificates in detail, including their format, version, and applications.	**[L2, CO4]**	**10M**

Course Code: 23CS0525 **R23**

UNIT –IV

USER AUTHENTICATION

1	**a)**	List any two principles of remote user authentication.	**[L1,CO5]**	**[2M]**
	b)	Define Kerberos? Mention its primary purpose.	**[L1,CO5]**	**[2M]**
	c)	What does PGP stand for? State its key security features (any two).	**[L1,CO5]**	**[2M]**
	d)	What is meant by combining Security Associations?	**[L1,CO5]**	**[2M]**
	e)	Name the two phases of IKE.	**[L1,CO5]**	**[2M]**
2		Evaluate different remote authentication mechanisms (Password, Biometrics, Token-based, Multi-factor) based on security, usability, and deployment challenges.	**[L3,CO5]**	**[10M]**
3		List and explain the typical attacks remote authentication protocols must resist.	**[L2,CO5]**	**[10M]**
4	**a)**	Illustrate how Kerberos authenticates a client to a service in a network domain.	**[L3,CO5]**	**[5M]**
	b)	Analyze how Kerberos ensures security against eavesdropping and replay attacks.	**[L4,CO5]**	**[5M]**
5	**a)**	Explain the complete architecture of PGP including key rings, packet flow, and trust model.	**[L2,CO5]**	**[5M]**
	b)	Compare PGP and S/MIME on cryptographic approach, key management, trust model, and interoperability.	**[L4,CO5]**	**[5M]**
6	**a)**	Design IPsec-based secure network architecture for enterprise communication.	**[L3,CO5]**	**[5M]**
	b)	Evaluate advantages and limitations of IPsec in end-to-end security.	**[L3,CO5]**	**[5M]**
7	**a)**	Explain IP Security Policy including SPD processing, selectors, and actions.	**[L2,CO5]**	**[5M]**
	b)	Summarize the difference between ESP authentication and AH authentication.	**[L4,CO5]**	**[5M]**
8	**a)**	Describe ESP packet format in detail and explain its security coverage.	**[L2,CO5]**	**[5M]**
	b)	Evaluate the security impact of combining AH and ESP in different modes.	**[L3,CO5]**	**[5M]**
9	**a)**	Describe why multiple SAs are needed for combining security services.	**[L2,CO5]**	**[5M]**
	b)	Given a security requirement set, show how multiple SAs are combined to achieve it.	**[L4,CO5]**	**[5M]**
10.		How IKE Phase-1 and Phase-2 differ in goals, exchange methods, cryptographic operations, and outputs.	**[L4,CO5]**	**[10M]**

Course Code: 23CS0525 **R23**

UNIT –V

Transport Level Security

1	**a)**	Explain the functions of Transport Layer Security.	**[L2, CO6]**	**5M**
	b)	List the security services provided by TLS.	**[L2, CO6]**	**5M**
2		Discuss web security requirements in detail and explain the threats addressed by each requirement.	**[L2, CO6]**	**10M**
3		Explain Transport Layer Security (TLS), its protocol components, and security services	**[L2, CO6]**	**10M**
4		Explain HTTPS and describe how it provides secure web communication	**[L2, CO6]**	**10M**
5		Explain the authentication and encryption mechanisms used in SSH.	**[L2, CO6]**	**10M**
6	**a)**	what is a firewall?	**[L1, CO6]**	**2M**
	b)	Describe the characteristics and functions of firewalls.	**[L2, CO6]**	**8M**
7		Explain in detail about different Types of Fire walls	**[L2, CO6]**	**10M**
8		How can firewall policies be set to allow or deny traffic?	**[L2, CO6]**	**10M**
9		What are the key parameters to consider when configuring a firewall?	**[L2, CO6]**	**10M**
10		Describe the steps to configure a firewall in a small office network.	**[L2, CO6]**	**10M**

Prepared by –

V SAMBASIVA, Assistant Professor, CSE Department

R. SUREKA, Assistant Professor, CSE Department

S. SHILPA, Assistant Professor, CSE Department

N. ANITHA, Assistant Professor, CSIT Department