SIDDHARTHINSTITUTEOFENGINEERING&TECHNOLOGY

(AUTONOMOUS)
(Approved by AICTE, New Delhi & Affiliated to JNTUA, Ananthapuramu)
(Accredited by NBA for Civil, EEE, Mech., ECE & CSE)
(Accredited by NAAC with 'A+' Grade)
Puttur-517583,Tirupati District,A.P.(India)

QUESTIONBANK(DESCRIPTIVE)

Subject with Code	CRYPTOGRAPHY AND DATA SECURITY-23CS1207	**Course & Branch**	B.Tech– CSE-CCC
Year & Sem	III & II	**Regulation**	R23

UNIT-I
INTRODUCTION TO SECURITY CONCEPTS
A MODEL FOR CRYPTOGRAPHY CONCEPTS AND TECHNIQUES

1	**a)**	Define Disclosure with one example	**[L1][CO1]**	**[2M]**
	b)	What is meant by Disruption?	**[L1][CO1]**	**[2M]**
	c)	Define Destruction with one example.	**[L1][CO1]**	**[2M]**
	d)	Define Snooping in security attacks.	**[L1][CO1]**	**[2M]**
	e)	Explain Sniffing with one example in security threats.	**[L1][CO1]**	**[2M]**
2		Explain in detail about passive attacks and active attacks.	**[L2][CO3]**	**[10M]**
3	**a)**	Classify possible types of attacks in cryptography?	**[L2][CO1]**	**[5M]**
	b)	Compare Encryption and Decryption Process.	**[L4][CO1]**	**[5M]**
4		A student shares his password with a friend. Which security principle is compromised?	**[L3][CO1]**	**[10M]**
5	**a)**	Explain how authentication ensures secure communication.	**[L2][CO1]**	**[5M]**
	b)	Summarize the major security approaches used in organizations.	**[L2][CO1]**	**[5M]**
6	**a)**	Explain the difference between plaintext and cipher text with an example.	**[L2][CO1]**	**[5M]**
	b)	Evaluate the effectiveness of access control lists (ACLs) vs role-based access control (RBAC).	**[L5][CO1]**	**[5M]**
7	**a)**	Define cryptography.	**[L1][CO1]**	**[2M]**
	b)	List any two substitution techniques.	**[L1][CO1]**	**[2M]**
	c)	Define symmetric key cryptography.	**[L1][CO1]**	**[2M]**
	d)	What is key size explain with example?	**[L2][CO1]**	**[2M]**
	e)	What is the main purpose of security services?	**[L1][CO1]**	**[2M]**
8	**a)**	Indicate any three Symmetric key cipher techniques.	**[L3][CO1]**	**[5M]**
	b)	Infer the Principles of security in data security?	**[L2][CO1]**	**[5M]**
9	**a)**	Illustrate different types of transposition techniques in detail.	**[L3][CO1]**	**[5M]**
	b)	Discuss Playfair cipher in Detail.	**[L2][CO1]**	**[5M]**
10		Analyze how transposition differs from substitution in terms of security.	**[L4][CO6]**	**[10M]**
11		Analyze why encryption alone cannot provide complete security.	**[L4][CO6]**	**[10M]**

UNIT-II
CONVENTIONAL ENCRYPTION

1	**a)**	List the five main classical encryption techniques.	**[L1][CO2]**	**[02M]**
	b)	State the formula for the Affine cipher encryption and decryption.	**[L1][CO2]**	**[02M]**
	c)	Explain the difference between stream cipher and block cipher?	**[L2][CO2]**	**[02M]**
	d)	What does DES stand for and what is its block size?	**[L1][CO2]**	**[02M]**
	e)	What is Triple DES? Why was it developed?	**[L2][CO2]**	**[02M]**
2	**a)**	Illustrate Conventional encryption model.	**[L3][CO2]**	**[5M]**
	b)	List the five main classical encryption techniques.	**[L1][CO2]**	**[5M]**
3		Describe Hill cipher and Mono alphabetic ciphers in detail	**[L2][CO2]**	**[10M]**
4		Explain Transposition ciphers with examples	**[L2][CO2]**	**[10M]**
5	**a)**	State the formula for the Affine cipher encryption and decryption.	**[L2][CO2]**	**[5M]**
	b)	Derive Ceasar cipher algorithm, encrypts the message using the key "POLYMORPHIC" and Key k=3.	**[L3][CO2]**	**[5M]**
6	**a)**	Explain the number of rounds used in DES encryption.	**[L2][CO2]**	**[02M]**
	b)	What is Triple DES? Explain Why was it developed?	**[L4][CO2]**	**[02M]**
	c)	Define conventional encryption and list its two main components.	**[L1][CO2]**	**[02M]**
	d)	What is the Caesar cipher? Explain its basic mechanism.	**[L1][CO2]**	**[02M]**
	e)	Define cryptanalysis and list its four types.	**[L1][CO2]**	**[02M]**
7	**a)**	Establish Affine cipher Encryption and Decryption process using the keyword "MONARCHY" and keys a=3, b=5.	**[L3][CO2]**	**[5M]**
	b)	Compare conventional key with public key encryption.	**[L5][CO2]**	**[5M]**
8		Examine the general structure of DES with neat sketch.	**[L4][CO2]**	**[10M]**
9		Analyze a real-world scenario where DES was compromised and discuss the Lessons learned.	**[L4][CO6]**	**[10M]**
10	**a)**	Differentiate between mono alphabetic and poly alphabetic substitution ciphers.	**[L2][CO2]**	**[5M]**
	b)	Analyze the security weaknesses of the Caesar cipher and propose improvements.	**[L4][CO6]**	**[5M]**
11	**a)**	Write short notes on block cipher principles? Explain the block cipher modes of operation.	**[L1][CO2]**	**[10M]**
	b)	Infer the Principles of Stream Cipher and Block cipher.	**[L2][CO2]**	**[5M]**

UNIT-III

ASYMMETRIC KEY CIPHERS

1	**a)**	Define RSA and state the mathematical problem on which its security is based.	**[L1][CO3]**	**[02M]**
	b)	List the key sizes typically used in RSA encryption.	**[L1][CO3]**	**[02M]**
	c)	What is the purpose of the Diffie-Hellman key exchange protocol?	**[L2][CO3]**	**[02M]**
	d)	List the parameters required for DSA signature generation.	**[L1][CO4]**	**[02M]**
	e)	Define Blowfish cipher. What is its key size range?	**[L2][CO3]**	**[02M]**
2		Compute Cipher text for Plain text="DECRYPTION", P=11, D=3, E1=2, R=4(Random Integer) plain text=7, using Elgamal Cryptography.	**[L3][CO3]**	**[10M]**
3	**a)**	Illustrate the structure of Diffie-Hellman Key Exchange and Calculate Diffie-Hellman Key Exchange algorithm using keys q=7, X_a=3, X_b=4, α=2.	**[L4][CO5]**	**[6M]**
	b)	Establish Digital Signature Algorithm using RSA.	**[L3][CO4]**	**[4M]**
4		Generalize the structure of DSA and its algorithms.	**[L2][CO4]**	**[10M]**
5	**a)**	Infer the concept of Elgamal Cryptography algorithm.	**[L2][CO3]**	**[5M]**
	b)	Compare ElGamal encryption with RSA in terms of cipher text expansion.	**[L3][CO3]**	**[5M]**
6		Discuss any one Asymmetric Key cipher algorithms with example. List out the advantages and disadvantages.	**[L3][CO4]**	**[10M]**
7	**a)**	What does IDEA stand for? Mention its key and block size.	**[L1][CO3]**	**[02M]**
	b)	What is AES? State its block size and possible key lengths.	**[L1][CO3]**	**[02M]**
	c)	Define X448 key exchange. What is its key size?	**[L1][CO3]**	**[02M]**
	d)	What are the main steps involved in RSA key generation?	**[L1][CO5]**	**[02M]**
	e)	State the discrete logarithm problem and its significance in Diffie-Hellman.	**[L1][CO3]**	**[02M]**
8	**a)**	Analyze the computational complexity of RSA encryption vs decryption. Which is faster and why?	**[L4][CO6]**	**[5M]**
	b)	Examine the vulnerabilities of RSA with small encryption exponent (e=3). What Attacks are possible?	**[L4][CO6]**	**[5M]**
9		Demonstrate the Structure of AES and its transformations.	**[L2][CO3]**	**[10M]**
10		Discuss about key scheduling and round transformation of IDEA.	**[L2][CO3]**	**[10M]**
11	**a)**	Evaluate the structure of blow fish algorithm and list out the merits and Demerits.	**[L3][CO3]**	**[5M]**
	b)	Describe how stream ciphers use key stream generation for encryption.	**[L2][CO3]**	**[5M]**

UNIT-IV
INTRODUCTION TO DATA SECURITY & IDS SECURITY

1	**a)**	Define data security. What are its primary objectives?	**[L1][CO4]**	**[02M]**
	b)	What is the difference between a threat, vulnerability, and an attack?	**[L2][CO4]**	**[02M]**
	c)	List the three main security goals (CIA Triad). Define each briefly.	**[L1][CO4]**	**[02M]**
	d)	Define a hash function. What are its essential properties?	**[L1][CO4]**	**[02M]**
	e)	Name two simple hashing functions commonly used for basic integrity checking.	**[L1][CO4]**	**[02M]**
2		What is security attack? Explain different Types of Security attacks?	**[L2][CO3]**	**[10M]**
3		Examine the types, process & tools of Vulnerability assessment?	**[L4][CO4]**	**[10M]**
4	**a)**	Explain Vulnerability and its types?	**[L2][CO4]**	**[5M]**
	b)	Enumerate security goals and its methods.	**[L1][CO4]**	**[5M]**
5	**a)**	Explain the Man-in-the-middle attacks with example	**[L2][CO4]**	**[5M]**
	b)	Define firewall? Examine the need for firewalls and role of firewalls in protecting Networks.	**[L4][CO4]**	**[5M]**
6	**a)**	Explain the concept of a salami attack with example?	**[L3][CO3]**	**[5M]**
	b)	Evaluate the types and characteristics of Data Integrity.	**[L5][CO4]**	**[5M]**
7	**a)**	Infer in detail about Time-of-check to Time-of-use (TOCTTOU) Errors.	**[L2][CO4]**	**[5M]**
	b)	Apply TOCTTOU attack principles on a sample file access scenario.	**[L2][CO4]**	**[5M]**
8	**a)**	Explain Vulnerability and its types?	**[L2][CO4]**	**[5M]**
	b)	Explain the concept of a salami attack with example?	**[L3][CO4]**	**[5M]**
9		Classify various types of viruses in IDS Security.	**[L4][CO4]**	**[10M]**
10	**a)**	Define firewall? Examine the need for firewalls and role of firewalls in protecting Networks.	**[L4][CO6]**	**[5M]**
	b)	Assess the impact of man-in-the-middle attacks on online banking security.	**[L5][CO3]**	**[5M]**
11	**a)**	What are the advantages of ECC over RSA?	**[L2][CO4]**	**[5M]**
	b)	What is Elliptic Curve Cryptography (ECC)? On what mathematical structure is it based?	**[L2][CO4]**	**[5M]**

UNIT–V
IP SECURITY & DIGITAL SIGNATURES

1	**a)**	Define IPSec and list its two main protocols.	**[L1][CO5]**	**[02M]**
	b)	List the two modes of operation in IPSec.	**[L1][CO5]**	**[02M]**
	c)	Name the three main components of IPSec architecture.	**[L1][CO5]**	**[02M]**
	d)	What is the purpose of Security Association Database (SAD) in IPSec.	**[L1][CO5]**	**[02M]**
	e)	Define a digital signature.	**[L1][CO5]**	**[02M]**
2		Sketch neatly and summarize IP security Architecture in detail.	**[L3][CO5]**	**[10M]**
3		Generalize Authentication header and its modes of operation in detail.	**[L6][CO5]**	**[10M]**
4	**a)**	Justify briefly about combining Security Associations.	**[L5][CO5]**	**[6M]**
	b)	Distinguish between Digital Signature and Digital Certificate.	**[L4][CO4]**	**[4M]**
5	**a)**	Discuss Model of Digital Signature and Encryption with Digital Signature.	**[L2][CO4]**	**[5M]**
	b)	Differentiate between SHA1 and SHA2	**[L4][CO5]**	**[5M]**
6	**a)**	Illustrate the steps involved in DSA Algorithm.	**[L3][CO4]**	**[5M]**
	b)	Examine the Proof of Digital signature algorithm.	**[L3][CO5]**	**[5M]**
7	**a)**	Describe the steps taken to ensure security, signing the Digest in Digital Signature Algorithm.	**[L2][CO4]**	**[5M]**
	b)	Examine Secure Hash Algorithm and applications.	**[L4][CO5]**	**[5M]**
8	**a)**	What is the output size of SHA-1 algorithm?	**[L1][CO5]**	**[02M]**
	b)	Explain how digital signatures provide authentication.	**[L2][CO6]**	**[02M]**
	c)	Describe the relationship between hash functions and digital signatures.	**[L1][CO5]**	**[02M]**
	d)	What does AH stand for in IPSec?	**[L1][CO5]**	**[02M]**
	e)	Define IPSec and list its two main protocols.	**[L1][CO5]**	**[02M]**
9	**a)**	Explain the difference between Authentication Header (AH) and Encapsulating Security Payload (ESP).	**[L2][CO6]**	**[5M]**
	b)	Describe how transport mode differs from tunnel mode in IPSec.	**[L2][CO6]**	**[5M]**
10	**a)**	Explain the purpose of Security Association Database (SAD) in IPSec.	**[L2][CO5]**	**[5M]**
	b)	What is the role of Security Policy Database (SPD) in IPSec architecture?	**[L2][CO5]**	**[5M]**
11		How would you implement IPSec to secure communication between two branch offices? Specify the mode and protocols.	**[L3][CO6]**	**[10M]**

Prepared by: Mr.T.Anil Kumar
Dept.of CCC-CIA-CIC