Course Code: 19CI0605 **R19**

SIDDHARTH GROUP OF INSTITUTIONS:: PUTTUR
(AUTONOMOUS)
Siddharth Nagar, Narayanavanam Road – 517583

QUESTION BANK (DESCRIPTIVE)

Subject with Code: Cryptography & Network Security(19CI0605) **Course & Branch**: B.Tech-CSIT
Year &Sem: IV-B.Tech & I-Sem **Regulation:** R19

UNIT –I
SECURITY CONCEPTS AND CRYPTOGRAPHY CONCEPTS AND TECHNIQUES

1	**a**	Specify the components of encryption algorithm	[L4][CO1]	**[6M]**
	b	Explain about steganography.	[L2][CO2]	**[6M]**
2	**a**	What are the principles of security .	[L1][CO1]	**[6M]**
	b	Describe the various security mechanisms.	[L2][CO1]	**[6M]**
3	**a**	What is security mechanism	[L1][CO1]	**[6M]**
	b	Explain about a model for network security.	[L2][CO2]	**[6M]**
4	**a**	Explain the substitution encryption techniques in detail?	[L2][CO1]	**[6M]**
	b	What are security services.	[L1][CO2]	**[6M]**
5	**a**	Explain the OSI security architecture?	[L2][CO1]	**[6M]**
	b	List and briefly define categories of passive and active security attacks.	[L1][CO1]	**[6M]**
6	**a**	What is the purpose of security.	[L1][CO1]	**[6M]**
	b	Explain the Transposition encryption techniques in detail?	[L2][CO1]	**[6M]**
7	**a**	Explain about symmetric key cryptography.	[L2][CO1]	**[6M]**
	b	Distinguish Threat and Attack	[L2][CO1]	**[6M]**
8	**a**	Illustrate different types of Security Attacks and Services in Detail	[L2][CO3]	**[6M]**
	b	List and briefly define the fundamental security design principles.	[L1][CO1]	**[6M]**
9	**a**	Explain about asymmetric key cryptography.	[L2][CO1]	**[8M]**
	b	Explain the following terms i. Encryption ii. Decryption iii. plain text iv. Cipher text	[L2][CO1]	**[4M]**
10	**a**	Compare Substitution and Transposition techniques.	[L2][CO1]	**[4M]**
	b	Explain about security approaches	[L2][CO3]	**[8M]**

Course Code: 19CI0605 **R19**

UNIT –II
SYMMETRIC KEY CIPHERS AND ASYMMETRIC KEY CIPHERS

1	**a**	What is the difference between block cipher and stream cipher ?	[L1][CO1]	**[6M]**
	b	What requirements must a public key cryptosystem to fulfill to a secured algorithm?	[L1][CO1]	**[6M]**
2	**a**	Extend the Diffie-Hellman Key Exchange.	[L2][CO1]	**[6M]**
	b	What are the principle elements of a public key cryptosystem?	[L1][CO1]	**[6M]**
3	**a**	Descover the working principles of simple DES with an example.	[L3][CO2]	**[6M]**
	b	List out the attacks to RSA and define each.	[L1][CO1]	**[6M]**
4	**a**	List the steps in RSA algorithm.	[L1][CO2]	**[6M]**
	b	Consider and Evaluate a Diffie-Hellman scheme with a common prime q=11 and a primitive root α=2 a. Show that 2 is a primitive root of 11. b. If user A has public key Ya = 9, what is A's private key Xa? c. If user B has public key Yb = 3, what is the secret key K shared with A?	[L5][CO1]	**[6M]**
5	**a**	Design principles of block cipher.	[L6][CO1]	**[6M]**
	b	Formulate the decryption and encryption using RSA algorithm with p=3 q=11 e=7 and N=5.	[L6][CO2]	**[6M]**
6	**a**	Explain the block cipher modes of operations	[L2][CO1]	**[5M]**
	b	Explain about IDEA with neat diagram	[L2][CO1]	**[7M]**
7	**a**	What is the strength of DES.	[L1][CO1]	**[2M]**
	b	Examine users A and B use the Diffie-Hellman key exchange technique with a common prime q=11 and a primitive root α=7. a. If user A has private key Xa = 3, what is A's public key Ya ? b. If user B has private key Xb=6, what is B's public key Yb ? c. What is the shared secret key?	[L4][CO1]	**[10M]**
8	**a**	Explain Knapsack Algorithm	[L2][CO2]	**[6M]**
	b	Explain in detail about AES key expansion	[L2][CO1]	**[6M]**
9	**a**	Illustrate about RC5 Encryption algorithm	[L3][CO1]	**[6M]**
	b	Interpret working of AES with example.	[L3][CO2]	**[6M]**
10	**a**	Illustrate about Blowfish algorithm.	[L3][CO1]	**[6M]**
	b	Design and develop Triple DES algorithm and explain with neat diagram.	[L6][CO1]	**[6M]**

Course Code: 19CI0605 **R19**

UNIT –III
CRYPTOGRAPHIC HASH FUNCTIONS AND KEY MANAGEMENT AND DISTRIBUTION

1	**a**	Differentiate MAC and Hash function?	[L2][CO1]	**[6M]**
	b	What are the applications of cryptographic hash function?	[L1][CO1]	**[6M]**
2	**a**	Describe Secure hash Algorithm in detail.	[L2][CO3]	**[6M]**
	b	What are the requirements for message authentication	[L1][CO2]	**[6M]**
3	**a**	Describe any one method of efficient implementation of HMAC.	[L2][CO1]	**[6M]**
	b	What types of attacks are addressed by message authentication?	[L1][CO1]	**[6M]**
4	**a**	Explain in detail ElGamal Digital Signature scheme with an example.	[L2][CO3]	**[8M]**
	b	What characteristics are needed in a secure hash function?	[L1][CO1]	**[4M]**
5	**a**	Explain in detail about different ways of distribution of public keys	[L2][CO2]	**[6M]**
	b	Discuss about symmetric key distribution using symmetric encryption	[L2][CO2]	**[6M]**
6	**a**	Define digital signature? Explain its role in network security.	[L1][CO2]	**[8M]**
	b	List out the comparison of SHA parameters	[L1][CO2]	**[4M]**
7	**a**	What is a message authentication code?	[L1][CO1]	**[2M]**
	b	Consider prime field q=19, it has primitive roots { 2,3,10,13,14,15}, if suppose α=10. Then write key generation by she choose XA=16. And also sign with hash value m=14 and alice choose secret no K=5. Verify the signature using Elgamal digital Signature Scheme	[L5][CO4]	**[10M]**
8	**a**	Explain X.509 Authentication Services	[L2][CO2]	**[6M]**
	b	Explain the public key infrastructure.	[L2][CO3]	**[6M]**
9	**a**	What is a key distribution center?	[L1][CO3]	**[4M]**
	b	What is Kerberos?Define the requirements of a Kerberos.	[L1][CO1]	**[8M]**
10	**a**	Explain about symmetric key distribution using symmetric encryption	[L2][CO3]	**[6M]**
	b	Identify cryptography hash function.	[L1][CO3]	**[6M]**

Course Code: 19CI0605 **R19**

UNIT –IV
TRANSPORT LEVEL SECURITY AND WIRELESS NETWORK SECURITY

1	**a**	What are the parameters in TLS ?	[L1][CO4]	**[6M]**
	b	Explain about wireless security.	[L2][CO4]	**[6M]**
2	**a**	Evaluate the different protocols of SSL. Explain Handshake protocol in detail.	[L5][CO4]	**[6M]**
	b	What is the difference between a TLS connection and a TLS session?	[L1][CO1]	**[6M]**
3	**a**	What protocols comprise TLS	[L1][CO4]	**[6M]**
	b	List and briefly define the SSH protocols.	[L1][CO1]	**[6M]**
4	**a**	Elaborate different level of awareness of a connection in HTTPS.	[L6][CO4]	**[6M]**
	b	What steps are involved in the TLS Record Protocol transmission?	[L1][CO1]	**[6M]**
5	**a**	Explain the SSH protocols.	[L1][CO4]	**[6M]**
	b	What services are provided by the TLS Record Protocol?	[L1][CO5]	**[6M]**
6	**a**	What is the basic building block of an 802.11 WLAN?	[L1][CO5]	**[6M]**
	b	List some security threats related to mobile devices.	[L1][CO1]	**[6M]**
7	**a**	Describe transport level security in detail	[L6][CO5]	**[7M]**
	b	Explain about web security considerations	[L6][CO5]	**[5M]**
8	**a**	List and briefly define IEEE 802.11 services.	[L5][CO5]	**[6M]**
	b	Describe the five IEEE 802.11i phases of operation.	[L2][CO1]	**[6M]**
9	**a**	What are the security areas are addressed by IEEE 802.11i?	[L1][CO4]	**[6M]**
	b	How is the concept of an association related to that of mobility?	[L1][CO4]	**[6M]**
10	**a**	List out the wireless network threats.	[L1][CO4]	**[6M]**
	b	Discuss about transport layer security.	[L2][CO4]	**[6M]**

Course Code: 19CI0605 **R19**

UNIT –V
E-MAIL SECURITY AND CASE STUDIES ON CRYPTOGRAPHY AND SECURITY

1	**a**	Explain in detail about the security services for E-mail	[L2][CO1]	**[6M]**
	b	Explain the operation description of PGP	[L2][CO2]	**[6M]**
2	**a**	What is Cross site Scripting Vulnerability	[L1][CO6]	**[6M]**
	b	List out the four principal services provided by S/MIME?	[L1][CO6]	**[6M]**
3	**a**	Why is base64 conversion useful for an email application?	[L4][CO4]	**[6M]**
	b	Explain about internet key exchange.	[L2][CO5]	**[6M]**
4	**a**	Explain about authentication header.	[L2][CO6]	**[4M]**
	b	Explain the IP Security architecture.	[L2][CO4]	**[8M]**
5	**a**	How IPSec ESP does provide transport and Tunnel Mode operation? Explain with a neat sketch.	[L2][CO5]	**[10M]**
	b	Discuss the benefits of IPsec	[L2][CO1]	**[2M]**
6	**a**	What is ESP?	[L1][CO1]	**[4M]**
	b	What is PGP? Show the message format of PGP	[L1][CO5]	**[8M]**
7	**a**	Elaborate different categories of IPsec documents.	[L6][CO6]	**[6M]**
	b	List and briefly define different categories of IPsec documents	[L1][CO1]	**[6M]**
8	**a**	Discuss in detail about S/MIME	[L2][CO6]	**[6M]**
	b	Why does ESP include a padding field?	[L4][CO1]	**[6M]**
9	**a**	Identify the benefits of IPsec	[L3][CO6]	**[6M]**
	b	What is the difference between transport mode and tunnel mode?	[L1][CO1]	**[6M]**
10	**a**	Describe the Encapsulating security payload.	[L5][CO6]	**[6M]**
	b	List and briefly describe some benefits of IPsec.	[L1][CO1]	**[6M]**

Preparedby:
Mrs. D.Viswasahithya
Assistant Professor/CSIT