Code No: R2032053 **R20** SET -1

III B. Tech II Semester Regular Examinations, July -2023
CRYPTOGRAPHY AND NETWORK SECURITY
(Com. To CSE & IT)

Time: 3 hours Max. Marks: 70

Answer any **FIVE** Questions **ONE** Question from **Each unit**
All Questions Carry Equal Marks
*****

UNIT-I

1.	a)	Explain the categories of security threats.	[7M]
	b)	Explain active and passive attacks in detail.	[7M]
		(OR)	
2.	a)	Differentiate policies, mechanisms and services in network security.	[7M]
	b)	Differentiate between symmetric and asymmetric encryption.	[7M]

UNIT-II

3.	a)	Explain about the essential ingredients of symmetric cipher.	[7M]
	b)	Compare and contrast between stream cipher with block cipher.	[7M]
		(OR)	
4.	a)	List and explain block cipher modes of operation.	[7M]
	b)	Explain DES and different modes of operation in DES state its advantages and disadvantages.	[7M]

UNIT-III

5.	a)	Explain various mathematics used for asymmetric key crypotography.	[7M]
	b)	Explain round functions of Advanced Encryption Standard Algorithm	[7M]
		(OR)	
6.	a)	State the differences between diffusion and confusion .	[7M]
	b)	Brief the strength of RSA algorithm and analyze its performance.	[7M]

UNIT-IV

7.	a)	Explain HASH function and its properties in cryptography.	[7M]
	b)	Explain the classes of message authentication function.	[7M]
		(OR)	
8.	a)	Briefly explain the requirements of message authentication.	[7M]
	b)	Differentiate between MAC and Hash function..	[7M]

UNIT-V

9.	a)	Explain the operational description of PGP.	[7M]
	b)	Write a short note on S/MIME.	[7M]
		(OR)	
10.	a)	Explain the architecture of IP security.	[7M]
	b)	Write a short notes on Authentication header and ESP.	[7M]

Code No: R2032053 **R20** SET -2

III B. Tech II Semester Regular Examinations, July -2023
CRYPTOGRAPHY AND NETWORK SECURITY
(Com. To CSE & IT)

Time: 3 hours Max. Marks: 70

Answer any **FIVE** Questions **ONE** Question from **Each unit**
All Questions Carry Equal Marks
*****

UNIT-I

1.	a)	Write a brief note on integrity and non-repudiation with an example.	[7M]
	b)	Explain the network security model with neat sketch.	[7M]
		(OR)	
2.	a)	Illustrate a brief note on security goals.	[7M]
	b)	Define security attack, security mechanism and security services.	[7M]

UNIT-II

3.	a)	Explain the techniques involved for each round in DES with neat sketch	[7M]
	b)	Differentiate between cryptanalysis and brute force attack.	[7M]
		(OR)	
4.	a)	Explain about symmetric key cryptography and public key cryptography.	[7M]
	b)	Explain AES and various operations used in its round function.	[7M]

UNIT-III

5.	a)	Perform encryption and decryption using RSA for p=17, q=11, e=7, M=88	[7M]
	b)	Write about elliptic curve cryptography.	[7M]
		(OR)	
6.	a)	Explain substitute byte transformation in AES.	[7M]
	b)	Explain the primitive operations of RC5.	[7M]

UNIT-IV

7.	a)	Differentiate between internal and external error control.	[7M]
	b)	Explain the role of compression function in hash function.	[7M]
		(OR)	
8.	a)	Explain any one Hash algorithm.	[7M]
	b)	Explain the requirements of digital signature scheme.	[7M]

UNIT-V

9.	a)	Explain in detail the operation of SSL .	[7M]
	b)	Write a short notes on E-mail security.	[7M]
		(OR)	
10.	a)	Explain the services provided by PGP.	[7M]
	b)	Differentiate between SSL version 3 and TLS.	[7M]

Code No: R2032053 **R20** SET -3

III B. Tech II Semester Regular Examinations, July -2023
CRYPTOGRAPHY AND NETWORK SECURITY
(Com. To CSE & IT)

Time: 3 hours Max. Marks: 70

Answer any **FIVE** Questions **ONE** Question from **Each unit**
All Questions Carry Equal Marks
*****

UNIT-I

1.	a)	Explain different types of security services	[7M]
	b)	What are the basic mathematical concepts used in cryptography? Explain with examples.	[7M]
		(OR)	
2.	a)	Explain various types of cryptanalytic attacks and cryptanalysis and cryptology.	[7M]
	b)	What is steganography? explain the techniques in it, it from cryptography.	[7M]

UNIT-II

3.	a)	Briefly explain AES with neat sketch.	[7M]
	b)	Explain the transformation functions and key expansion for each round in AES.	[7M]
		(OR)	
4.	a)	Write about different symmetric key ciphers.	[7M]
	b)	Draw the general structure of DES and explain encryption and decryption process.	[7M]

UNIT-III

5.	a)	Explain the primitive operations of RC5.	[7M]
	b)	Differentiate between private key and public key encryption.	[7M]
		(OR)	
6.	a)	Perform decryption and encryption using RSA algorithm with p=3,q=11,e=7,N=5	[7M]
	b)	Justify your answer whether Diffie Hellman key exchange protocol is vulnerable.	[7M]

UNIT-IV

7.	a)	Differentiate between message authentication and one-way hash function.	[7M]
	b)	Write the difference between MD5 and SHA.	[7M]
		(OR)	
8.	a)	Explain secure hash algorithm in detail.	[7M]
	b)	Explain different types of attacks that are addressed by message authentication.	[7M]

UNIT-V

9.	a)	Give a brief note on IP security.	[7M]
	b)	Explain internet key management in IPSEC.	[7M]
		(OR)	
10.	a)	Explain SET with neat sketch.	[7M]
	b)	Explain the features of SET.	[7M]

Code No: R2032053 **R20** SET -4

III B. Tech II Semester Regular Examinations, July -2023
CRYPTOGRAPHY AND NETWORK SECURITY
(Com. To CSE & IT)

Time: 3 hours Max. Marks: 70

Answer any **FIVE** Questions **ONE** Question from **Each unit**
All Questions Carry Equal Marks
*****

UNIT-I

1.	a)	What kinds of services are provided for data security? Discuss in detail.	[7M]
	b)	Define plain text, cipher text, enciphering, deciphering with an example.	[7M]
		(OR)	
2.	a)	Explain the aspects required for network security model.	[7M]
	b)	Write a short note on authentication and data integrity.	[7M]

UNIT-II

3.	a)	Explain the block structures and S-Box design used in DES algorithm.	[7M]
	b)	Describe about RC4 and RC5 algorithm.	[7M]
		(OR)	
4.	a)	Explain the strength and weakness of DES algorithm.	[7M]
	b)	Describe various mathematics used for symmetric key encryption algorithm.	[7M]

UNIT-III

5.	a)	User A&B exchange the key using Diffie Hellman algorithm assume A=5, q=11, X_A=2,X_B=3 find Y_A,Y_B,K	[7M]
	b)	Explain the approaches to attack the RSA algorithm.	[7M]
		(OR)	
6.	a)	State the difference between AES decryption algorithm and the equivalent inverse cipher.	[7M]
	b)	Explain RSA algorithm in detail. Identify the possible threats for RSA algorithm and list their counter measures.	[7M]

UNIT-IV

7.	a)	Give a brief note on digital signature algorithm.	[7M]
	b)	Explain in detail about hash function.	[7M]
		(OR)	
8.	a)	Discuss about the objectives of HMAC and its security features.	[7M]
	b)	Explain MD5 with neat sketch.	[7M]

UNIT-V

9.	a)	Write a short notes on web security.	[7M]
	b)	Explain the steps involved in SET.	[7M]
		(OR)	
10.	a)	Differentiate between SSL connection and SSL session.	[7M]
	b)	Why is the segmentation and reassembly function in PGP needed explain?	[7M]