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

III B. Tech II Semester Regular/Supplementary Examinations, May/June-2024
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 is the need of security? Explain about various security threats.	[7M]
	b)	Explain Simple substitution ciphers with an example.	[7M]
		(OR)	
2.	a)	What is Cryptography? What are the main challenges and risks?	[7M]
	b)	The coded message MXOQCY IFUDT YDWIE CKSXJ YCUED JXYI was received. It is known that the code was a shift code with equation c = p – 10. Decode the message. Be sure to put in appropriate spaces.	[7M]

UNIT-II

3.	a)	What is symmetric encryption scheme? What are the Five elements of it? Explain.	[7M]
	b)	What are the mathematical concepts used in symmetric cryptographic algorithms? Explain how is algebra used in cryptography?	[7M]
		(OR)	
4.	a)	What is Cipher text? Explain with an example about Caesar cipher	[7M]
	b)	What is an Algorithm? Discuss about any one Symmetric encryption algorithm.	[7M]

UNIT-III

5.	a)	What is Asymmetric encryption? What problems does it solve?	[7M]
	b)	Explain MILLER-RABIN algorithm for testing a large number for primality	[7M]
		(OR)	
6.	a)	Discuss RSA algorithm for Asymmetric Cryptography.	[7M]
	b)	Given two prime numbers P = 17 and Q = 29, find out N E and D in a RSA encryption process.	[7M]

UNIT-IV

7.	a)	Describe the properties of digital signatures.	[7M]
	b)	Write and explain the Digital Signature Algorithm (DSA).	[7M]
		(OR)	
8.	a)	What is authentication? Explain the different types of authentication.	[7M]
	b)	What are the characteristics of acceptable hash functions in Cryptography? Justify?	[7M]

UNIT-V

9.	a)	What is PGP? Draw and explain the general PGP packet structure.	[7M]
	b)	What is SSL? Write short notes on the keys used in SSL.	[7M]
		(OR)	
10.	a)	Give the architecture of e-mail system with a neat sketch.	[7M]
	b)	Compare and contrast IPSec and SSL.	[7M]

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

III B. Tech II Semester Regular/Supplementary Examinations, May/June-2024
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 is a Cryptographic Attack? What are the different types of attacks?	[7M]
	b)	Which Tools are used by attackers to attack web sites? Explain	[7M]
		(OR)	
2.	a)	What are the mathematical methods used in cryptography? Give their significance.	[7M]
	b)	What is Fermat's theorem? Explain how it is used in security?	[7M]

UNIT-II

3.	a)	What is Symmetric Encryption? How does it work & Why use it?	[7M]
	b)	Explain DES algorithm with an example.	[7M]
		(OR)	
4.	a)	What are the two basic ways of transforming a plain text into a cipher text? Explain.	[7M]
	b)	Use any method to decode the following encoded with a Caesar Cipher. Adhziypsspn, hukaolzspaofavclz . Write the original Plain - Text	[7M]

UNIT-III

5.	a)	What is Asymmetric- Key Cryptography? Discuss the advantages and disadvantages of it.	[7M]
	b)	What is Primality test? Explain how it is used in Asymmetric- Key Cryptography.	[7M]
		(OR)	
6.	a)	Discuss the 'Elliptical Wave Theory' algorithm for Asymmetric Cryptography. What is the security?	[7M]
	b)	If A wants to send a message securely to B, Explain What are the typical steps involved?	[7M]

UNIT-IV

7.	a)	What is Digital Signature? Explain the benefits of Digital signatures.	[7M]
	b)	Describe with an example how the process involved in digital signatures.	[7M]
		(OR)	
8.	a)	What is authentication? Explain how authentication is performed in Kerberos.	[7M]
	b)	What is Hash Function? What are the applications of it in authentication?	[7M]

UNIT-V

9.	a)	Explain how does PGP perform trust processing	[7M]
	b)	Discuss how SSL provides secure communication	[7M]
		(OR)	
10.	a)	Discuss about some application avenues of IPSec.	[7M]
	b)	Compare and contrast IPSec and SSH.	[7M]

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

III B. Tech II Semester Regular/Supplementary Examinations, May/June - 2024
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 is Network Security? What are the Four Goals of Network Security? Explain with examples.	[7M]
	b)	What tricks attackers use to hack online banking accounts? How to prevent them?	[7M]
		(OR)		
2.	a)	Elaborate on attacks threatening confidentiality.	[7M]
	b)	What are the two basic ways of transforming a plain text into a cipher text?	[7M]

UNIT-II

3.	a)	What is symmetric and asymmetric encryption? Explain the various components of the encryption.	[7M]
	b)	Elaborate on components of a modern block cipher.	[7M]
		(OR)	
4.	a)	What is Caesar cipher? Explain how Caesar cipher can be cracked?	[7M]
	b)	A plaintext was encrypted with a Caesar cipher with a shift of 7. The resulting cipher text is: Kvu'aqbknlhivvrifpazjvcly What was the original plain-text?	[7M]

UNIT-III

5.	a)	How does Fermat theorem is used in finding multiplicative inverses? Explain.	[7M]
	b)	What are the different types of primality testing algorithms? Explain	[7M]
		(OR)	
6.	a)	Discuss The 'Diffie-Hellman algorithm' for Asymmetric Cryptography.	[7M]
	b)	In RSA, given N = 187 and the encryption key(E) as 17 find out the corresponding private key D.	[7M]

UNIT-IV

7.	a)	A cryptographic hash function must satisfy three criteria. What are they? Explain them.	[10M]
	b)	What happens if a k value used in creating a DSA signature is compromised?	[4M]
		(OR)	
8.	a)	What is authentication? Explain how authentication is performed in multiple Kerberos.	[7M]
	b)	What is hash Function? Explain HMAC algorithm. What is to be done to speed up HMAC algorithm?	[7M]

UNIT-V

9.	a)	Write short note on PGP Key Rings.	[7M]
	b)	Explain the various SSL Protocols and their structure and use.	[7M]
		(OR)	
10.	a)	What is IPSec? Explain why it is necessary in security of IP network.	[7M]
	b)	Compare and contrast IPSec and TLS.	[7M]

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

III B. Tech II Semester Regular/Supplementary Examinations, May/June-2024
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)	Elaborate on the security goals to be achieved.	[7M]
	b)	Explain the operational security model with a block diagram.	[7M]
		(OR)	
2.	a)	What is timing Attack? What are the possible defenses against timing attack?	[7M]
	b)	What are the elements of information security? Explain each in brief.	[7M]
		UNIT-II	
3.	a)	Write short notes on following: Commutative ring, operations on polynomials	[7M]
	b)	Give the basic structure of Feistel cipher.	[7M]
		(OR)	
4.	a)	Compare Linear cryptanalysis with differential cryptanalysis.	[7M]
	b)	A plaintext was encrypted with a Caesar cipher, resulting in the following: DOOV ZHOO WKDW HQGV ZHOO Can you work out what the plaintext was?	[7M]
		UNIT-III	
5.	a)	How fundamental theorem of factorization is used in finding GCD and LCM? Explain.	[7M]
	b)	What is key Wrapping? Explain how it is useful?	[7M]
		(OR)	
6.	a)	Discuss RSA algorithm for Asymmetric- Key Cryptography	[7M]
	b)	Consider a plain - text alphabet G. Using RSA algorithm and the values as E = 3 and d = 11 and N = 15 then Find out what this plain - text alphabet encrypts to. Verify that upon decryption it transforms back to G	[7M]
		UNIT-IV	
7.	a)	What is Random Oracle Model? Focus on the attacks on Random Oracle Model.	[7M]
	b)	Describe with an example the process involved in Digital Signature Algorithm DSA	[7M]
		(OR)	
8.	a)	Compare SSL authentication process with Kerberos	[7M]
	b)	Explain Block Cipher based MAC scheme	[7M]
		UNIT-V	
9.	a)	Discuss the various services offered by PGP to secure e-mails	[7M]
	b)	IPSec operates on two different modes. Explain them.	[7M]
		(OR)	
10.	a)	PGP uses certificates to authenticate public key. Explain them.	[7M]
	b)	Compare and contrast IPSec and SSL	[7M]