Code No: R1941051 **R19** **Set No. 1**

IV B.Tech I Semester Regular Examinations, November – 2022
CRYPTOGRAPHY AND NETWORK SECURITY(COMMON TO CSE & IT)
(Computer Science and Engineering)

Time: 3 hours **Max. Marks: 75**

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

UNIT-I

1	a)	Draw a matrix that shows the relationship between security mechanisms and attacks.	[7]
	b)	Make comparisons between the monoalphabetic ciphers and polyalphabetic ciphers.	[8]
		(OR)	
2	a)	Consider an Automated Teller Machine (ATM) in which users provide a Personal Identification Number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement.	[7]
	b)	Discuss the Symmetric Cipher Model.	[8]

UNIT-II

3	a)	Explain the Block Cipher Modes of Operations.	[7]
	b)	Discuss the Blowfish algoritham with a neat diagram.	[8]
		(OR)	
4	a)	How encryption and decryption are done in DES? Explain	[7]
	b)	What are relative prime numbers? Describe their role in fermat's theorem and Euler's theorem.	[8]

UNIT-III

5	a)	Briefly explain the Public key Cryptography Principles in detail.	[7]
	b)	Explain the Secure Hash Function Algorithm in detail.	[8]
		(OR)	
6	a)	For SHA-512, show the equations for the values of W_{16},W_{17}, W_{18}, W_{19} and Calculate the hash function for the 48 letter message " I leave 20 million dollars to my friendly cousin bill".	[7]
	b)	Mention three variations of digital signatures and briefly state the purpose of each.	[8]

UNIT-IV

7	a)	Why Kerberos is needed? What problem was Kerberos designed to address?	[5]
	b)	List and explain the PGP services and explain how PGP message generation is done with a neat diagram.	[10]

(OR)

8 a) Distinguish between transport mode AH and tunnel mode AH. [7]
b) Elaborate on Combining Security Associations and Key Management. [8]

UNIT-V

9 a) Write the differences between a packet-filtering router and a stateful inspection firewall. [7]
b) Explain the significance of the Dual signature and its purpose, how is it constructed in SET. [8]

(OR)

10 a) Explain various web security threats. Briefly explain SSL. [10]
b) Give a brief note on Secure Shell (SSH). [5]

Code No: R1941051 **R19** **Set No. 2**

IV B.Tech I Semester Regular Examinations, November – 2022
CRYPTOGRAPHY AND NETWORK SECURITY(COMMON TO CSE & IT)
(Computer Science and Engineering)

Time: 3 hours **Max. Marks: 75**

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

UNIT-I

1		Consider a desktop publishing system used to produce documents for various organizations. a. Give an example of a type of publication for which confidentiality of the stored data is the most important requirement. b. Give an example of a type of publication in which data integrity is the most important requirement. c. Give an example in which system availability is the most important requirement.	[15]
		(OR)	
2	a)	Discuss the Buffer Overflow& Format String Vulnerabilities.	[8]
	b)	Explain the TCP session hijacking with a neat diagram .	[7]

UNIT-II

3	a)	If n is composite and passes the Miller-Rabin test for base a, then n is called a strong pseudo prime to base a. Show that 2047 is a strong pseudo prime to the base 2.	[7]
	b)	Do you agree with the statement that an increase in the key size of 1 bit doubles the security of DES? Justify your answer.	[8]
		(OR)	
4	a)	List and explain the strengths of DES.	[7]
	b)	AES consists of four functions in three layers. Which of the functions are primarily for confusion and which are primarily for diffusion? Which of the layers are for confusion and which are for diffusion? Justify your answers.	[8]

UNIT-III

5	a)	How keys are exchanged in the Diffie-Hellman algorithm? Explain	[7]
	b)	List the Application of Cryptographic Hash Functions.	[8]
		(OR)	
6	a)	Discuss the Message Authentication Functions.	[7]
	b)	Explain the steps involved in SHA-512.	[8]

UNIT-IV

7	a)	Give the architecture of IP Security	[7]
	b)	What are the main three parts of Kerberos? Give their significance.	[8]

(OR)

8 a) Explain the X.509 certificate formats. What is one-way authentication? [7]
b) In PGP, what is the probability that a user with N public keys will have at least one duplicate key ID? [8]

UNIT-V

9 a) What are the three types of Firewalls? Compare and contrast them.. [7]
b) What are the functions performed by the firewall and how those functions are performed? Explain [8]

(OR)

10 a) How SSL record protocol provides confidentiality and message integrity for SSL connections? Explain [7]
b) Give a brief note on Web Security Requirements. [8]

Code No: R1941051 **R19** **Set No. 3**

IV B.Tech I Semester Regular Examinations, November – 2022
CRYPTOGRAPHY AND NETWORK SECURITY(COMMON TO CSE & IT)
(Computer Science and Engineering)

Time: 3 hours **Max. Marks: 75**

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

UNIT-I

1	a)	Describe the Block Cipher Design Principles.	[7]
	b)	List and explain the Web Based Attacks.	[8]
		(OR)	
2	a)	Describe the components of Symmetric cipher model with a neat diagram	[7]
	b)	Give the classification of security attacks. How security services are related to security mechanisms?	[8]

UNIT-II

3	a)	What is the purpose of the Extended Euclidean algorithm? Illustrate with an example.	[7]
	b)	Explain the Chinese remainders theorem.	[8]
		(OR)	
4	a)	Use Euler's Theorem to find a number "***a"*** between 0 and 9 such that a is congruent to 7^{1000}modulo 10.	[7]
	b)	Compare the rounds of DES algorithm with that od AES algorithm.	[8]

UNIT-III

5		Perform encryption and decryption using the RSA algorithm for the following: a. p = 3; q = 11, e = 7;M = 5 b. p = 5; q = 11, e = 3;M = 9 c. p = 7; q = 11, e = 17;M = 8	[15]
		(OR)	
6	a)	Explain the essential characteristics of public key cryptography.	[7]
	b)	Discuss the Elliptic Curve Cryptography is used for data encryption.	[8]

UNIT-IV

7	a)	With the help of a neat diagram, explain the IP security architecture.	[7]
	b)	Discuss the encapsulating security payload.	[8]

(OR)

8 a) In the PGP scheme, what is the expected number of session keys generated before a previously created key is produced? [7]

b) Discuss the Remote User Authentication Principles. [8]

UNIT-V

9 Compare SSL and TLS. Explain in detail how payment processing is done in SET. [15]

(OR)

10 a) Why do we need security in the Transport layer? Is TLS symmetric or asymmetric. [7]

b) Consider any commercial hardware firewall and explain it in detail. [8]

Code No: R1941051 **R19** **Set No. 4**

IV B.Tech I Semester Regular Examinations, November – 2022
CRYPTOGRAPHY AND NETWORK SECURITY(COMMON TO CSE & IT)
(Computer Science and Engineering)

Time: 3 hours **Max. Marks: 75**

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

UNIT-I

1	a)	List and briefly define categories of Security Services & Mechanisms.	[7]
	b)	Discuss the UDP Session Hijacking.	[8]
		(OR)	
2	a)	Compare TCP session Hijacking with UDP session Hijacking.	[7]
	b)	Draw and explain the common attacks and vulnerabilities.	[8]

UNIT-II

3	a)	Use Fermat's Theorem to find a number x between 0 and 28 with x^{85} congruent to 6 modulo 29.	[7]
	b)	What are the integer arithmetic operations related to security? Explain .	[8]
		(OR)	
4	a)	How do you find the relative prime of a number? Discuss	[7]
	b)	Let K = (k0,k1,k2, ... k55) be a 56-bit DES key. List the 48 bits of each DES subkey K1, K2, ... ,K16. Make a table that contains the number of subkeys in which each bit ki is used. Can you design a DES key schedule algorithm in which each key bit is used an equal number of times?	[8]

UNIT-III

5	a)	Explain Message Authentication Requirements and What are the attacks related to message communication?	[7]
	b)	Consider a Diffie- Hellman key with a common prime q=11 and primitive root α = 2.If the user has a public key Y_a= 9 what is A's private key X_A?	[8]
		(OR)	
6	a)	List and explain the applications of public key cryptography.	[7]
	b)	Explain the weakness of Hash and MAC functions.	[8]

UNIT-IV

7		What are teh benefits of IPSec? Describe the three protocols used in IP Security.	[15]

(OR)

8 a) How Kerberos V5 differs from Kerberos V4? [5]
b) Discuss the security services offered byPretty Good Privacy. [10]

UNIT-V

9 Compare the various generations of firewalls. Comment on the security achieved and the ease of implementation of the various generations of firewalls. [15]

(OR)

10 a) Is it possible in SSL for the receiver to record SSL record blocks that arrive out of order? If so, explain how it can be done. If not, why not? [7]
b) How to prevent false alarms in IDS? Discuss in detail. [8]