CSE555

USN	1	M	S							

RAMAIAH
Institute of Technology

(Autonomous Institute, Affiliated to VTU)
(Approved by AICTE, New Delhi & Govt. of Karnataka)
Accredited by NBA & NAAC with ‘A+’ Grade

SEMESTER END EXAMINATIONS – FEBRUARY 2024

Program	:	**B.E. - Computer Science and Engineering**	**Semester**	:	**V**
Course Name	:	**Cryptography and Network Security**	**Max. Marks**	:	**100**
Course Code	:	**CSE555**	**Duration**	:	**3 Hrs**

Instructions to the Candidates:

- Answer one full question from each unit.

UNIT - I

1.	a)	Draw the taxonomy of security goals. Illustrate the security goals with an example.	CO1	(08)
	b)	Write the Extended Euclidean algorithm to find the multiplicative inverse of a number. Apply the same to compute multiplicative inverse of 7 in Z_{180}.	CO1	(08)
	c)	Analyze which security mechanism(s) are provided in each of the following cases? i. A school demands student identification and a password to let students log into the school server. ii. A school server disconnects a student if she is logged into the system for morethan two hours. iii. A professor refuses to send students their grades by e-mail unless they providestudent identification they were preassigned by the professor. iv. A bank requires the customer’s signature for a withdrawal.	CO1	(04)
2.	a)	Using Euclidean Algorithm, determine the GCD for the following pair of integers: i. 1760 and 2740 ii. 25 and 60.	CO1	(06)
	b)	Distinguish between active attack and passive attacks. Give few examples for passive and active attacks.	CO1	(07)
	c)	Illustrate set of residues, congruence and residue classes with suitable examples.	CO1	(07)

UNIT - II

3.	a)	Explain the common types of cryptanalysis attack.	CO2	(08)
	b)	Identify four types of transformations used by AES.	CO2	(08)
	c)	Distinguish between a steam cipher and block cipher.	CO2	(04)
4.	a)	Describe the key generation in DES with a suitable diagram.	CO2	(08)
	b)	Use the Playfair cipher to encipher the message “The key is hidden under the door pad” using the secret key “GUIDANCE”.	CO2	(06)
	c)	With an example explain key expansion in AES-128.	CO2	(06)

UNIT - III

5.	a)	Illustrate the general design of AES Encryption cipher with a neat block diagram.	CO3	(08)
	b)	With the help of neat diagram, explain the optimal asymmetric encryption padding in detail.	CO3	(06)
	c)	Assume that a=[3, 7, 12, 30, 60,115] and s = 82 . Find tuple x using inv_knapsack sum.	CO3	(06)

6.	a)	Show the AES structure of each round at the encryption site with a neat diagram.	CO3	(08)
	b)	Bob chooses 13 and 11 as p and q and calculates n value. Find the value of φ(n). Find the two exponents e and d. Now assume that Alice wants to send the plain text 13 to Bob. Find the cipher text and decrypt it on receiving side to get plaintext using RSA algorithm.	CO3	(06)
	c)	Draw the taxonomy of potential attacks on RSA. Illustrate any three attack forms.	CO3	(06)

UNIT- IV

7.	a)	Identify the various types of attacks identified in message authentication requirements.	CO4	(10)
	b)	Discuss the general format and elements of X.509 certificate.	CO4	(06)
	c)	Briefly discuss about Message Authentication Code (MAC). What are the requirements for Message Authentication Code?	CO4	(04)
8.	a)	Explain the general schemes for the distribution of public keys with a neat diagram.	CO4	(12)
	b)	Summarize the possible types of attacks with Digital Signature.	CO4	(08)

UNIT - V

9.	a)	Identify the various Transport Layer Security (TLS) session state and connection state parameters.	CO5	(10)
	b)	Explain the limitations of the Kerberos Version 4 with respect to environmental shortcomings and technical deficiencies.	CO5	(10)
10.	a)	Illustrates confidentiality and encryption with the Simplified S/MIME Functional Flow process diagram.	CO5	(10)
	b)	Summarize the Message Exchanges of Kerberos version 5.	CO5	(10)

****