CSE643

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

Created by trial version of DocuFreezer

SEMESTER END EXAMINATIONS – MAY 2023

Program	:	**B.E. – Computer Science and Engineering**	**Semester**	:	**VI**
Course Name	:	**Cryptography and Network Security**	**Max. Marks**	:	**100**
Course Code	:	**CSE643**	**Duration**	:	**3 Hrs**

Instructions to the Candidates:

- Answer one full question from each unit.

UNIT - I

1.	a)	Illustrate the taxonomy of security goals with suitable examples.	CO1	(06)
	b)	Distinguish between Z and Z_n. Explain how we can map an integers in Z to an integers in Z_n. Calculate the multiplicative inverse of 23 in Z_{100} using Extended Euclidean Algorithm.	CO1	(08)
	c)	Differentiate between the following with an example: i. Passive and Active attacks ii. Cryptography and Steganography iii. Repudiation and Replaying.	CO1	(06)
2.	a)	Find particular and general solution for the following linear equation. i. $9x+4 \equiv 12 \pmod 7$ ii. $25x+10y=15$.	CO1	(08)
	b)	List and explain the Security services recommended by ITU-T (X.500).	CO1	(06)
	c)	Analyze which security mechanism(s) areprovided in each of the following cases? i. A school server disconnects a student if she is logged into the system for more than two hours. ii. A professor refuses to send students grades by e-mail unless they provide student identification they were preassigned by the professor. iii. A bank requires the customer's signature for a withdrawal.	CO1	(06)

UNIT - II

3.	a)	Illustrate the various cryptanalysis attack forms with a block diagram.	CO2	(08)
	b)	Explain the steps involved in DES function with a neat diagram.	CO2	(08)
	c)	Use the multiplicative cipher with key=7 to encrypt the message "HELLO".	CO2	(04)
4.	a)	Describe the process of key expansion in AES-128 algorithm with a neat diagram.	CO2	(08)
	b)	Encrypt the message "ATTACK IS TODAY" using Autokey cipher with key=12.	CO2	(06)
	c)	Apply Vigenere cipher to encrypt the message "Let us make it happen" with the key "WORLD".	CO2	(06)

UNIT - III

5.	a)	Illustrate the process of encryption and decryption for Electronic Codebook(ECB) and Cipher block chaining(CBC) mode using modern symmetric key cipher with a neat 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)	Draw the block diagram for encryption, decryption and key generation for Rabin cryptosystem.	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)	Illustrate RC4 Encryption algorithm with an example.	CO3	(06)

UNIT- IV

7.	a)	Describe various types of attacks identified in message authentication requirements.	CO4	(08)
	b)	Illustrate the general format and elements of X.509 certificate.	CO4	(06)
	c)	Explain generic model of digital signature process and its requirements.	CO4	(06)
8.	a)	Describe the general schemes for the distribution of public keys.	CO4	(10)
	b)	Summarize the Message Exchanges of Kerberos version 4.	CO4	(10)

UNIT - V

9.	a)	Describe the following intrusion detection in detail: i. Distributed Intrusion Detection ii. Audit Records.	CO5	(08)
	b)	Illustrate four phases of virus with the structure of virus.	CO5	(08)
	c)	Explain various intruder behavior patterns.	CO5	(04)
10.	a)	Write the taxonomy of malicious program and illustrate.	CO5	(10)
	b)	What is firewall? Mention the capabilities and limitations of firewalls.	CO5	(10)

****

Created by trial version of DocuFreezer