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

SEMESTER END EXAMINATIONS – JULY / AUGUST 2022

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)	In brief explain eight security mechanism recommended by ITU-T (X.500).	CO1	(08)
	b)	Find the multiplicative inverse and values for s & t for the following using Extended Euclidean algorithm: i. 23 in Z_{100} ii. 7 in Z_{180}	CO1	(08)
	c)	Differentiate between Cryptography and Steganography.	CO1	(04)
2.	a)	Describe set of residues, congruence and residue classes with suitable examples.	CO1	(08)
	b)	Discuss the taxonomy of five common Security Services.	CO1	(06)
	c)	Using Extended Euclidean's algorithm, solve for GCD of the following pairs of integers 161 and 28.	CO1	(06)

UNIT – II

3.	a)	Briefly discuss four common types of cryptanalysis attacks.	CO1	(07)
	b)	Give the relationship between the plaintext P and the ciphertext C in affine cipher. Use an affine cipher to encrypt the message "hello" with the key pair (7, 2).	CO1	(06)
	c)	Explain the process of triple DES using two keys with neat diagram.	CO2	(07)
4.	a)	Encrypt the message MONDAY using the Hill cipher with the key: $\begin{matrix} 9 & 4 \\ 5 & 7 \end{matrix}$	CO2	(06)
	b)	Explain AES key expansion.	CO2	(08)
	c)	With neat diagram explain single round of DES encryption algorithm.	CO2	(06)

UNIT – III

5.	a)	What are the different modes of operation designed to be used with modern block ciphers? Describe any two.	CO3	(08)
	b)	With the help of neat diagram, explain the optimal asymmetric encryption padding in detail.	CO3	(06)
	c)	Explain Secret communication with Knapsack Cryptosystem.	CO3	(06)
6.	a)	Draw the block diagram for encryption, decryption and key generation for Rabin cryptosystem.	CO3	(08)

b) Discuss the following types of attacks on RSA: CO3 (06)

i. Factorization.

ii. Chosen-ciphertext.

iii. Coppersmith theorem attack.

c) Write an encryption algorithm for RC4 and explain it with example. CO3 (06)

UNIT – IV

7. a) Explain the following uses of message encryption with neat diagram. CO4 (10)

i. Symmetric encryption.

ii. Public key encryption.

b) Explain the limitations of the Kerberos Version 4 with respect to environmental shortcomings and technical deficiencies. CO4 (10)

8. a) Explain with a neat diagram, the Digital signature algorithm Signing and Verifying. CO4 (08)

b) With a neat diagram, illustrate the generation of a public-key certificate. CO4 (06)

c) Briefly discuss about Revocation of Certificate. CO4 (06)

UNIT – V

9. a) List the three design goals for a firewall. Briefly explain Packet-filtering router. CO5 (06)

b) What are the two categories of malicious program? Explain each category with examples. CO5 (06)

c) Discuss the four phases a typical virus goes through its lifetime. CO5 (08)

10. a) What are intruders? Describe the different types of intruders identified as security threats. CO5 (06)

b) Lists four general techniques that firewalls use to control access and enforce the site's security policy. CO5 (08)

c) Explain different types of firewalls. CO5 (06)

****