Roll No												

PRESIDENCY UNIVERSITY
BENGALURU

School Of Computer Science and Engineering & Information Science

End-Term Examinations, Aug 2024

Odd Semester: 2023 - 24
Course Code: CSE3078
Course Name: Cryptography and Network Security
Department: CSE

Date: 09.08.2024
Time: 9.30AM -12.30PM
Max Marks: 100
Weightage: 50%

Instructions:
(i) Read the all questions carefully and answer accordingly.
(ii) Do not write any matter on the question paper other than roll number.

Q.No	Questions	Marks	CO	RBT
1	a. Let message = "graduate", key="word", find ciphertext using playfair cipher.	4	CO1	L1
	b. Describe the various security services.	6	CO1	L2
	c. Demonstrate encryption and decryption process in hill cipher. Consider message="sh" and key="hill"..	10	CO1	L3
	OR			
2	a. Encrypt the plaintext "tobeornottobe" using the vigenere cipher for the key value "Now".	4	CO1	L1
	b. Differentiate between i) Active and Passive attack Ii) Block Cipher and Stream Cipher	6	CO1	L2
	c. Solve using playfair cipher. Encrypt the word "Semester Result" with the keyword "Examination". Discuss the roles to be followed	10	CO1	L3
3	a. Describe: i) Railfence cipher ii) Columnar transposition.	4	CO2	L1
	b. Find GCD (1970, 1066) using Euclid's algorithm.	6	CO2	L2
	1. Describe DES algorithm with neat diagram and explain the steps.	10	CO2	L3
	OR			
4	a. State Fermat's theorem and Euler's theorem.	4	CO2	L1
	b. Determine GCD(4655, 12075) using Euclid's algorithm	6	CO2	L2

	c. Describe in detail the key generation in AES algorithm and its expansion format.	10	CO2	L3

5	a. Explain concept of Public key cryptography with diagram.	4	CO3	L1
	b. With neat diagram explain Diffie-Hellmann Key exchange.	6	CO3	L2
	c. Write the steps of RSA algorithm and find public and private key for prime numbers p=17 and q=11.	10	CO3	L3

OR

6	a. Explain Man-in-the-middle attack.	4	CO3	L1
	b. With a neat diagram explain concept of Digital Signature.	6	CO3	L2
	c. Bring out the steps of Secure Hash Algorithm with neat diagram.	10	CO3	L3

7	a. What are the requirements for Kerberos.	4	CO4	L 1
	b. Explain the PKI architectural model.	6	CO4	L 2
	c. Elaborate PGP operations with neat diagram.	10	CO4	L 3

OR

8	a. What are S/MIME functions.	4	CO4	L1
	b. With diagram explain fields of Encapsulating Security Payload.	6	CO4	L2
	c. Elaborate the working and protocols involved in SSL.	10	CO4	L3

9	a. Using the Vigenère cipher, encrypt the word "explanation" using the key leg.	4	CO1	L1
	b. Explain OSI Security Architecture model with neat diagram	6	CO1	L2
	c. Encrypt the message "PAYMOREMONEY" using the Hill cipher with the key 17 17 5 21 18 21 2 2 19	10	CO1	L3

OR

10	a. Using Fermat's theorem, check whether 19 is prime or not? Consider a is 7.	4	CO2	L1
	b. Using the extended Euclidean algorithm, find the multiplicative inverse of i) 550 mod 1769 ii) 1234 mod 4321	6	CO2	L2
	c. State Chinese Remainder theorem and find the value of X for the given set of congruent equations using Chinese Remainder theorem. $X \equiv 1 (\text{mod } 5)$ $X \equiv 2 (\text{mod } 7)$ $X \equiv 3 (\text{mod } 9)$ $X \equiv 4 (\text{mod } 11)$	10	CO2	L3