VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Continuous Assessment Test-I - February 2024

Programme	:	**B.Tech.**	Semester	:	**Winter 2023 – 2024**
Course Code & Title	:	**BCSE309L-Cryptography and Network Security**	Class Nbr	:	**CH2023240501434 CH2023240501437 CH2023240501459 CH2023240501465 CH2023240501442 CH2023240501446 CH2023240501472 CH2023240501480 CH2023240501452 CH2023240501485 CH2023240501492 CH2023240501499 CH2023240502478**
Faculty	:	**Dr. RENUKA DEVI S Dr. SUBRAMANIYAM Dr. SUBBULAKSHMI P Dr. BHUVANESWARI AMMA N G Dr. MARY SHAMALA L Dr. VATCHALA S Dr. SOBITHA AHILA S Dr. RAJESH R Dr. TAPABRATA ROY Dr. KARTHIKA V Dr. BALASARASWATHI Dr. KANTHIMATHI S Dr. VALARMATHI K**	Slot	:	**F1+TF1**
Time	:	**1 ½ Hours**	Max. Marks	:	**50**

Answer all Questions			
1.	i)	Assume you are a cryptographer working for a secure messaging application that uses discrete logarithms for key exchange which uses the primitive roots of 7. Determine the primitive roots of 7 and create a table presenting the discrete logarithms to the base of 5, modulo 7 ensuring the confidentiality of communication. (5 Marks)	10
	ii)	Assume you are a cybersecurity expert working for a financial institution that is implementing enhanced security measures for its online transactions. The institution has chosen to use the RSA algorithm for encryption. As part of this process, the encryption exponent (e) is selected as 407, and the modulus (n) is set to 1467. To strengthen the security of the encryption, find the multiplicative inverse of 407 modulo 1467. (5 Marks)	

2.		Imagine you are an archaeologist exploring ancient ruins. As you decipher the inscriptions, you notice that the ancient civilization used a unique system based on remainders and divisibility. The inscriptions mention that a sacred artifact is hidden at a location corresponding to a specific integer that satisfies the following conditions: $x \equiv 3 \pmod{7}$ $x \equiv 4 \pmod{9}$ $x \equiv 12 \pmod{13}$ Determine the integer that meets these conditions.	**10**
3.		For each of the following elements of DES, indicate the differences with the comparable element in AES: a. Key size b. Block size c. S-box d. Key expansion function e. Initial and final permutation	**10**
4.		Compute the cipher text for the plaintext '1C92 E112' using the counter mode of operation with the following constraints. a. Only hexadecimal values are allowed (0 to F) with each one represented as 4-bits b. Block size is 16-bit (4 hexadecimal digits in a block) c. Encryption algorithm used is (x+key) mod 16 where x is a hexadecimal digit. d. Key value is 5 e. Counter value is initialized to A01E	**10**
5.	i) ii)	In an RSA cryptosystem Lyanna uses two prime numbers p = 13 and q =17 to generate her public and private keys. Find out the private key if the public key is given as 35. And show how will the text "HAI" be encrypted and decrypted by assuming A=0, B=1 …. Z =25. (8 Marks) In what scenarios would you advise against using RSA and why? (2 Marks)	**10**