Name :

VIT

Vellore Institute of Technology

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

Continuous Assessment Test-I January 2025

Programme	:	B.Tech CSE	Semester	:	Winter 2024 – 2025
Course	:	Cryptography and Network Security	Code	:	BCSE309L
			Class Nbr	:	CH2024250501852 CH2024250501853 CH2024250501847 CH2024250501856 CH2024250501877
Faculty	:	Dr. N G BHUVANESWARI Dr. MARY SHAMALA L Dr. LEKI CHOM THUNGON Dr. SOBITHA AHILA S Dr. BALASARASWATHI	Slot	:	B2+TB2
Time	:	1 ½ Hours	Max. Marks	:	50

Answer all Questions

1. i) Calculate 11^{-1} (mod 80). Hence solve the congruence $11x \equiv 4 \pmod{80}$. **(5 Marks)**

   ii) Compute $21^{4599} \pmod{47}$ using a suitable theorem. **(5 Marks)**

2. i) Find the greatest common divisor g of the numbers 1819 and 3587, and then find integers x and y to satisfy $1819x + 3587y = g$. **(6 Marks)**

   ii) Given 3 as a primitive root of 17, construct a table of the discrete logarithm and use it to solve the congruence $11 \equiv 3^x \bmod 17$. **(4 Marks)**

3. i) XYZ bank uses DES encryption to protect account information sent between its servers. A transaction request containing sensitive details (e.g., account number and amount) is encrypted using DES before being transmitted. The encrypted message (ciphertext) is received by the server, which then decrypts it to process the transaction. Explain the steps the server must follow to decrypt the received ciphertext using DES and retrieve the original plaintext. **(6 Marks)**

   ii) Jithin and Ram want to generate a simple sequence of numbers using the recurrence relation: $X_{n+1}=(a^{X_n}) \bmod m$. They choose the following parameters:

   - Modulus m=9
   - Base: a=2
   - Initial seed: $X_0=3$

   Generate the first 4 numbers (X_1, X_2, X_3, X_4) in the sequence generated by this method.

(4

Marks)

4. Encrypt the message "ME" using Hill cipher with a 2x2 key matrix $\begin{bmatrix} F & H \\ C & D \end{bmatrix}$. Each alphabet letter is mapped to a number (A = 0, B = 1, ..., Z = 25). Additionally, Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext.

(10 Marks)

5. Assume you are part of a cybersecurity team responsible for securing communications between two remote offices of a global company. The company uses Output Feedback mode with the Vernam cipher and key 0x36CC encrypting sensitive business documents before they are sent over the internet. One of the documents containing confidential financial data 0xAA0918BB (in hexadecimal digits) needs to be encrypted. Compute the ciphertext if the block size is 16 bits (4 hexadecimal digits in a block) and the nonce value is 0x728C. **(10 Marks)**