Reg. No.: 22BCE5181

Name : Sharon Byju

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	:	CH2024250502097 CH2024250501819 CH2024250501825 CH2024250501834
Faculty	:	Dr. SUBBULAKSHMI P Dr. VATCHALA S Dr. KARTHIKA V Dr. BALASARASWATHI V R	Slot	:	B1+TB1
Time	:	1 ½ Hours	Max. Marks	:	50

Answer all Questions

1.	i)	Use a suitable theorem to simplify and find the value of x in the given congruence: $x^{4567} \equiv 13$ mod 17. **(6 marks)**
	ii)	Find the last 2 decimal digits of 2^{100}. **(4 marks)**
2.	i)	Find all solutions x, if they exist, to the system of equivalences: **(8 marks)** $2x \equiv 6 \bmod 14$ $3x \equiv 9 \bmod 15$ $5x \equiv 20 \bmod 60$
	ii)	Three alarms ring at different intervals: • Alarm 1 rings every 8 minutes. • Alarm 2 rings every 14 minutes. • Alarm 3 rings every 18 minutes. All alarms last rang together 5 minutes ago. Write relevant congruences for the same to describe it better. **(2 marks)**
3.	i)	Sunil is a cryptographer working on securing a communication channel between two parties, Alice and Bob. The two parties want to use a key exchange protocol to share a secret key over an insecure channel securely. Alice and Bob are using a key exchange protocol with the following parameters: prime modulus p=19, generator g=2. **(6 Marks)** (a) Determine Alice's private key a, such that: $g^a \equiv 12 (\text{mod } p)$ (b) Determine Bob's private key b, such that: $g^b \equiv 18$ (mod p)
	ii)	Calculate the order of each invertible element in mod 7. **(4 marks)**

4. i) Assume that you are working as a cryptography engineer for a government organization that needs to protect classified communications. The organization chooses the Advanced Encryption Standard (AES)-128 encryption standard to achieve this. The AES-128 requires an initial key of 128 bits; divided into 4 words to generate round keys for encryption. Generate the first five words, i.e., w0 to w5 using the following initial key:

54 68 61 74 73 20 6D 79 20 4B 75 6E 67 2F 46 75

The S-box values are given as follows:

54	68	61	74	73	20	6D	79	20	4B	75	6E	67	2F	46	75
20	45	EF	92	8F	B7	3C	B6	B7	B3	9D	9F	85	4E	5A	9D

(8 marks)

ii) Compute the output of the shift rows transformation for the following sequence of input bytes: 54 77 6F 20 4F 6E 65 20 4E 69 6E 65 20 54 77 6F **(2 Marks)**

5. Alice and Bob decided to use a toy version of RC4 for secure communication. Instead of the full 256-byte state array used in the standard RC4, they used a smaller version with 3x2 bits to simplify the process. In this version, the state array S can take values from 0 to 5.

(a) Perform the initial permutation of the state array S using the key K= [3,1,4]. **(3 Marks)**

(b) Given the plaintext P= [5,2,4,0], generate the key stream and compute the ciphertext. **(7 Marks)**