Reg. No.: 22BCE5181

Name :

VIT

Vellore Institute of Technology

Continuous Assessment Test-II March 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. Ankit is the IT security head of a financial institution. His team is implementing a Rivest-Shamir-Adleman cryptographic scheme to ensure secure communication between the bank's servers and customers. A customer, Riya, wants to send a sensitive request to the bank's server, asking for a loan approval. She needs to ensure that only the bank can read her message and that it remains confidential during transmission. **10**

(a) If an attacker intercepts the encrypted message, why is it computationally infeasible for them to retrieve the original message? **(2 Marks)**

(b) How does the difficulty of prime factorization in large numbers contribute to Rivest-Shamir-Adleman's security? **(2 Marks)**

(c) If the encryption exponent e is small, under what conditions could an attacker potentially decrypt the ciphertext without knowing the private key? **(2 Marks)**

(d) In modern cybersecurity, what is the minimum key size recommended for Rivest-Shamir-Adleman encryption. **(2 Marks)**

(e) To improve efficiency, should the bank implement a hybrid cryptographic system for data transmission? Identify the suitable hybrid cryptographic system for secure data transmission. **(2 Marks)**

2. Ms. Priya and Mr. Raj are working on a classified AI-powered threat detection system for a government cybersecurity agency. To ensure secure communication, they decide to use the Elliptic Curve Cryptography (ECC) key exchange mechanism to derive a common secret key for AES encryption. They agree to use the elliptic curve Ep(a, b) = (2, 3) over a finite field GF(29). The chosen base point is (3,6). **10**

- Ms. Priya's private key: 3
- Mr. Raj's private key: 2

Help them compute the shared secret key using the ECC Diffie-Hellman key exchange process.

3. i) Ms. Saina is a cybersecurity expert working for a financial institution. To ensure message authenticity, she uses the ElGamal digital signature scheme to sign transactions securely. Her private key K_{pr} is 16 and her public key K_{pub}=(p, α, Y_s) is (71, 7, 19). She signs two transaction messages:

- Transaction1: M_1=15, with signature (S_1,S_2)=(11,49)
- Transaction2: M_2=31, with signature (S_1,S_2)=(56,65)

A security analyst, Mr. Arun, receives these signed transactions and wants to verify their authenticity. Illustrate the verification steps and conclude whether both messages are authentic or not. **(8 marks)** 10

ii) How many valid signatures are there for each message x in ElGamal digital signature scheme? Give reason for your answer. **(2 marks)**

4. A cybersecurity analyst, Mr. Rohan, is investigating how MD5 processes message blocks. He wants to analyze one step of Round 3.

- Message Block (M) = 9F1A2B3C
- Key (K) = CDEFAB12
- Number of shifts (S) = 3 bits
- Buffer Values:
  A = 11223344 10
  B = 55667788
  C = 99AABBCC
  D = DDEEFF00

Calculate the updated value of B after one operation in Round 3 of the MD5 compression function.

5. Identify the message authentication algorithm used here and walk through the steps to derive the final hexadecimal value using the below-mentioned parameters. The key is the binary equivalent of the last two digits of your student ID, which we'll say is 42. The message is a 16-bit string: "IT" (in ASCII). The block size is the same as the message length. The hash function (16-bit) is defined as the Exclusive OR of the message blocks. The input padding is a constant value: 0x55.The output padding is a different constant value: 0x7C. 10