Reg. No.:

Name :

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: $x \equiv 3 \pmod 7$ $x \equiv 4 \pmod 9$ $x \equiv 12 \pmod{13}$ 220 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. 16 OE 1491 d. Key value is 5 e. Counter value is initialized to A01E E9F1 EB 8E	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

$d \leq 11$

VIT
Vellore Institute of Technology
CHENNAI

Reg. Number:	

Continuous Assessment Test(CAT) – II - APRIL 2024

Programme	:	B.Tech	Semester	:	Winter 2023-2024
Course Code & Course Title	:	BCSE309L-Cryptography and Network Security	Class Number	:	CH2023240501434 CH2023240501437 CH2023240501459 CH2023240501465 CH2023240501442 CH2023240501446 CH2023240501472 CH2023240501480 CH2023240501452 CH2023240501485 CH2023240501492 CH2023240501499 CH2023240502478
Faculty	:	Dr. RENUKA DEVI S Dr. SUBRAMANIYAM Dr. SUBBULAKSHMI P Dr. BHUVANESHWARI 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
Duration	:	11/2 Hours	Max. Marks		50

Answer all questions

Q. No	Sub Sec.	Description	Marks
1		Considering the linear congruential algorithm, generate the sequence for the following generators. $X_{n+1} = (6X_n) \bmod 13$ $X_{n+1} = (5X_n) \bmod 13$ Which of the following generators provide good randomization? Justify your answer	10
2		Choose the Elliptic curve with prime p = 11, a = 1, b = 3, Generator G= (2,7) and Message =(3,5), receiver private key is 2 and sender random integer k=3. Compute the encryption and decryption processes completely	10

3	i)	Imagine Nithila wants to authenticate messages she sends to her friend Ooviya using Hash based Message Authentication Code with a shared key "mykey". Each character in the key is represented using 5 bits by assuming a=0, b=1....z=25, and the block size is 32 bits. As Nithila frequently sends messages to her friends, she decides to optimize the process by precomputing the values of K+, S_i, and S_o for efficient implementation of message authentication algorithm. Given this scenario, help Nithila to compute the precomputed values of K+, S_i, and S_o and represent them in hexadecimal. (6 marks)	10
	ii)	Enumerate the underlying problem of the Man-in-the-Middle attack (MiM). Suggest suitable mechanisms or protocols to protect against MiM attacks (4 marks)	
4	i)	You are an IT security consultant working with a large multinational corporation that operates across multiple geographical locations. The corporation relies heavily on secure authentication mechanisms to protect its sensitive data and internal resources. Recently, there have been concerns raised about the effectiveness of the existing authentication system, prompting the company's management to explore alternative solutions. As part of your consultancy role, you've been tasked with evaluating the feasibility of implementing Kerberos authentication within the organization. As the IT security consultant, outline the benefits and limitations of implementing Kerberos authentication for the multinational corporation. Describe how Kerberos works, including its components and the authentication process involved. Discuss the potential security risks associated with Kerberos and how they can be mitigated (6 marks)	10
	ii)	Assume Alice and Bob are using SHA-512 during their conversation and the one block of their message consisting of 5 ASCII characters "hello"[ASCII value for 'a' starts with 97 and assume 8 bits binary] Handle this one block message and find out the modified length by satisfying the rules of SHA-512 (4 marks)	
5	i)	Imagine you are a security analyst at a financial institution, and you need to securely transmit a message to Bob, a colleague at another branch. You have been provided with the following values	10

		prime numbers p = 31 and q = 37 and your public key is 23. The message you need to transmit is "101000" To ensure the message's integrity and authenticity, you decide to employ a digital signature scheme based on RSA algorithm. Hashing code for the given message is generated by applying SHR3 (Shift Right by 3 bits) of the message. Generate the signature and Verify the same (7 marks)	
	ii)	Explain how homomorphic Encryption differs from Traditional encryption techniques. Detail the types of homomorphic encryption and discuss the potential applications or advantages that homomorphic encryption has over traditional methods (3 marks)	

Q	A	B	r	T_1	T_2	T
46	1080	23	22	0	1	-46
1	23	22	1	1	-46	47
22	22	1	0	-46	47	1080
	1	0		47	-1080	

↓

m.I

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of the UGC Act, 1956)

Reg. No. : 21BCE1808

Final Assessment Test (FAT) - May 2024

Programme	**B.Tech.**	Semester	**WINTER SEMESTER 2023 - 24**
Course Title	**CRYPTOGRAPHY AND NETWORK SECURITY**	Course Code	**BCSE309L**
Faculty Name	**Prof. Rajesh R**	Slot	**F1+TF1**
		Class Nbr	**CH2023240501480**
Time	**3 Hours**	Max. Marks	**100**

General Instructions:

- Write only Register Number in the Question Paper where space is provided (right-side at the top) & do not write any other details.

Answer all questions (10 X 10 Marks = 100 Marks)

01. Consider the stream cipher RC4 that uses the state vector, S of size 8 x 3 bits. You will operate on 3 bits of plaintext at a time since S can take the values 0 to 7, which is represented as 3 bits. Encrypt the plaintext P = [4 5 6 7] with the key K = [2 3 4 5]. Illustrate all the steps required to generate the ciphertext for the given plaintext. **[10]**

02. a) You are a codebreaker working on deciphering a message using an old secure communication method. Your challenge is to find a secret number 'Y' that solves the puzzle: $17Y \equiv 1 \pmod{43}$. [5 Marks] **[10]**

b) As part of your cryptographic work, you are investigating if the number 3 is the primitive root of 17. If so, build a discrete logarithm table that should use 3 as the base and operate modulo 17. [5 Marks]

03. a) Suppose Anu wants to send a secret message to her friend Binu. Hence, Anu uses a Playfair cipher encryption technique to encrypt the message with the key 'SECURITY'. Compute the encrypted message for the input message 'HELLOWORLD'. [3 Marks] **[10]**

b) Assume you are a cryptographer working for a government agency tasked with securing classified communications. Your team has been tasked with implementing the Advanced Encryption Standard (AES) algorithm for encrypting sensitive information transmitted between government officials. Detail your team about the step-by-step process of how the AES algorithm works to encrypt the messages and explain how it ensures secure communication in the scenario described. Also, discuss the key features of AES that make it suitable for securing classified communications in a high-threat environment. [7 Marks]

04. Consider that Sunil chose a widely used public-key cryptosystem that can be used for digital signatures. A digital signature ensures that the message is sent by the intended user without any tampering by any third party (attacker), and it is used to verify the authenticity of the message sent electronically. Explain the digital signature scheme used by Sunil to send a message with a digital signature when p = 17, q = 11, e = 7, and M = 88. **[10]**

a) Compute the signature. [5 Marks]

b) Verify the signature. [5 Marks]

05. As a developer at a startup focused on secure communication, you are tasked with implementing a Hash-based Message Authentication Code (HMAC) using Secure Hash Algorithm (SHA)-512 to verify the integrity and authenticity of messages exchanged in your application. A message 'HelloSecureWorld' needs to be sent securely using the key 'SecureKey2024'. Design a secure architecture to illustrate HMAC with SHA-512 for generating an authentication code for this message. Your answer should cover the process of key preparation, the role of SHA-512 in the HMAC process, and the importance of padding in generating the HMAC value. **[10]**

06. The cryptosystem parameters of the Elliptic Curve Cryptography scheme are $E_{11}(1, 6)$ and G = (2, 7). B's secret key is $n_B = 2$. **[10]**

a. Find B's public key P_B. [4 Marks]

b. A wishes to encrypt the message $P_m = (10, 9)$ and choose a random value k = 2. Determine the ciphertext C_m. [6 Marks]

07. You are a systems administrator for a large corporation implementing Kerberos authentication across your network. The CEO has tasked you with ensuring that all employees can securely access company resources, including email servers, file shares, and internal applications. However, there have been concerns raised about the security of the Kerberos authentication system, particularly regarding potential vulnerabilities and attacks. Your task is to address these concerns and answer the following to ensure secure authentication within the company's network: **[10]**

a) How does Kerberos achieve mutual authentication? [4 Marks]

b) Mention the significance of Ticket Granting Ticket in Kerberos. [2 Marks]

c) What is the purpose of the session key in Kerberos? [2 Marks]

d) Is it possible to use Kerberos in a multi-realm environment? Justify your answer. [2 Marks]

08. You are tasked with designing a secure communication system for a multinational corporation that operates in multiple countries and relies heavily on exchanging sensitive business data between its branches located worldwide. The company is concerned about the security of its communication channels, especially when transmitting financial reports, customer data, and strategic plans. The requirements of a secure communication system is given as follows: **[10]**

- The communication system should ensure confidentiality, integrity, and authenticity of the transmitted data.
- It should support communication between branches located in different countries over potentially insecure networks, including the Internet.
- The system should be scalable to accommodate the growing needs of the corporation and support a large number of simultaneous connections.
- Key management should be robust and efficient to handle the distribution and updating of cryptographic keys across different branches securely.
- Compliance with relevant international standards and regulations for data protection and privacy is essential.

Create a robust and secure communication system using the Encapsulating Security Payload protocol tailored to the specific needs and challenges faced by the multinational corporation.

09. Assume that you are a security analyst responsible for monitoring network traffic in a corporate environment. One day, you notice unusual activity on a critical server. Upon further investigation, you find that a suspicious IP address (192.168.1.100) has been attempting to **[10]**

establish connections with the server's SSH port (22) at an unusually high rate. Discuss the use of an intrusion detection system to detect and respond to this suspicious activity. Outline the steps you would take to mitigate the risk posed by this intrusion attempt.

10. As a security expert, explain to John how the Secure Electronic Transaction (SET) protocol works to secure his online transactions. Outline the key steps involved in the SET protocol, including how encryption and digital signatures are used to protect sensitive information during the transaction. Additionally, discuss any potential vulnerabilities or limitations of the SET protocol that John should be aware of to make an informed decision about his purchase. **[10]**