VIT®

Vellore Institute of Technology

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

Reg. No. :

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. ROLLA SUBRAHMANYAM	Slot	F1+TF1
		Class Nbr	CH2023240501437
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