VIT®

Vellore Institute of Technology

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

CHENNAI

22BCE5181 No

Final Assessment Test(FAT) - Apr/May 2025

Programme	B.Tech.	Semester	Winter Semester 2024-25
Course Code	BCSE309L	Faculty Name	Prof. Karthika V
Course Title	Cryptography and Network Security	Slot	B1+TB1
		Class Nbr	CH2024250501825
Time	3 hours	Max. Marks	100

Instructions To Candidates

- Write only your registration number in the designated box on the question paper. Writing anything elsewhere on the question paper will be considered a violation.

Course Outcomes

On completion of this course, students should be able to:

CO1: To know the fundamental mathematical concepts related to security.

CO2: To understand concept of various cryptographic techniques.

CO3: To apprehend the authentication and integrity process of data for various applications

CO4: To know fundamentals of Transport layer security, web security, E-Mail Security and IP Security

Answer all Questions (10 × 10 Marks)

01. i) Assume a forensic team is investigating a cyberattack involving ransomware encryption. The malware uses a RSA-like modular inversion process for its key obfuscation. Analysts must compute the inverse for the following equation to begin the decryption of affected files:

$$67589W \equiv 1 (\text{mod} 3121)$$

Without W, thousands of critical corporate files will remain locked. Solve for W. [7 Marks]

ii) Compute the value of 5^{264} mod 299 using suitable theorem. [3 Marks]

[10] (CO1/K2)

02. You are a cybersecurity analyst investigating an incident where a critical message was altered in transit. The organization uses CFB mode encryption with custom symmetric algorithm (XOR each byte of plaintext with a flipped version of the key byte) to protect sensitive communication. The plaintext message "ATTACKNOW" is encrypted using the key 0x133457799BBCDFF1 and Initial Value 0xAABBCCDDEEFF0011, producing the ciphertext. During transmission, an attacker flips a single bit in the first ciphertext block (C_1). Upon decryption, the recipient reports that the first block of plaintext is completely corrupted, while the second block contains a minor, localized error. Answer the following questions.

i) Encrypt the given plaintext using CFB mode to obtain C_1. [5 marks]

ii) Explain why modifying C_1 results in full corruption of P_1 and a partial error in P_2. [2 marks]

iii) How can the organization prevent such tampering attacks while continuing to use CFB mode? [3 marks]

[10] (CO2/K3)

03. i) Bob randomly generated N = 119 for his public RSA key. Find out the smallest possible choice for e? (2 Marks)

ii) Mr. Dany is an intelligence officer who needs to send a highly confidential code to his headquarters securely. The agency uses ElGamal public-key encryption for secure communication. The headquarters has published the following parameters: prime number, q=59; generator, g=23; private key = 7; random integer, k=6. Mr. Dany wants to encrypt the secret message, M = 45 and send it securely to headquarters. List the steps involved in the communication process and perform encryption and decryption. If an attacker intercepts (C_1, C_2), why is it computationally hard to determine the original message without knowing the private key? (8 Marks)

[10] (CO2/K4)

04. Ann and Besty use the Diffie-Hellman key exchange with the following public parameters: prime number q =71, primitive root a = 7. Ann selects a private key X_A=5, and Besty selects a private key X_B = 12. However, an attacker, Eve, intercepts their communication and performs a Man-in-the-Middle attack by choosing her own private keys X_{EA}=9, X_{EB}=14.

a) Compute Ann's public key Y_A, Besty's public key Y_B, Eve's fake public keys Y_{EA} and Y_{EB}. (4 marks)
b) Determine the shared secret key between Ann and Besty. (2 marks)
c) Determine the shared secrets between Ann and Besty as computed by Eve. (2 marks)
d) What measures should be taken to overcome a Man-in-the-Middle attack? (2 marks)

[10] (CO2/K4)

05. Assume you are a cybersecurity analyst and implementing SHA-512 to hash file content before transmission to ensure data integrity. Analyze the below given file content "crypt" through SHA-512's block preparation and compression phases.

a. Convert the file content "crypt" into its binary form using ASCII values (ASCII of a is 97), and then represent this binary message in hexadecimal. [2 marks]

b. Specify the number of bits occupied by the file content, the padding, and the length field in the block. [2 marks]

c. Compute the Conditional Function Ch(e, f, g) in SHA-512's Compression Phase and represent the value in hexadecimal. The buffer values are given below e= 0xAAAABBBBCCCC1234 f= 0xAAAABBBBCCCC5678 g= 0x5555444433334321 [6 marks]

[10] (CO3/K4)

06. **SafeVault** is a cloud-based platform that manages and secures sensitive financial records, including transaction histories, account statements, and investment portfolios. Given the highly confidential nature of this data, SafeVault enforces strict security protocols to ensure data protection and regulatory compliance:

- All financial records are encrypted to prevent unauthorized access.
- Only verified financial analysts and auditors can access or modify financial records, ensuring strict access control.
- Digital signatures are utilized to authenticate and validate the integrity of financial reports and transaction approvals.

Consider a record where **Message = 7**, prime factors **P = 7** and **Q = 11**, and the public key **e = 17**. How does SafeVault address these security challenges while ensuring compliance with financial regulations?

[10] (CO3/K3)

07. A multinational healthcare organization, HealthSecure Inc., operates across 15 countries and manages sensitive patient data. To ensure secure communication and data access for its 50,000 employees, the organization decides to implement an X.509-based authentication service as part of its public key infrastructure (PKI) system. The system must support secure login to internal servers, email encryption, and verification of employee identities across its global network.

i) Analyze the role of the Certificate Authority (CA) in the X.509 authentication process and explain how it establishes trust among HealthSecure Inc.'s employees in this scenario. (4 marks)

ii) Evaluate the potential vulnerabilities in the X.509 certificate lifecycle (issuance, usage, and revocation) that an attacker could exploit to compromise HealthSecure Inc.'s sensitive patient data, and propose one mitigation strategy for each vulnerability. (4 marks)

iii) Given HealthSecure Inc.'s global operations and large workforce, predict one challenge that might arise in maintaining the scalability of the X.509 authentication system and suggest a practical solution to address it. (2 marks)

[10] (CO3/K4)

08. **ShopEase,** a widely used e-commerce platform, processes thousands of transactions daily, where customers provide sensitive information such as credit card details, shipping addresses, and login credentials. To secure these communications, ShopEase uses **Transport Layer Security (TLS)** to encrypt data exchanged between the client's browser and the server. Explain about the Transport Layer Security for the above scenario in detail with neat architecture

[10] (CO4/K2)

09. i) How can the principles of Secure Electronic Transactions (SET) be applied to enhance consumer trust in online payment systems, and what potential challenges might arise in implementing these principles across different regions with varying regulatory frameworks? [5 Marks]

ii) How might different stakeholders (e.g., consumers, businesses, regulators) perceive the implementation of Secure Electronic Transactions (SET), and what conflicting interests could arise as a result? [5 Marks]

[10] (CO4/K4)

10. An MNC company security manager identified an intruder in the system. Now, the company wants to deploy a mechanism to detect intruders. Identify the different types of detection mechanisms available and list the various advantages and disadvantages of such mechanisms.

[10] (CO4/K2)

BL-Bloom's Taxonomy Levels - (K1-Remembering,K2-Understanding,K3-Applying,K4-Analysing,K5-Evaluating,K6-Creating)