VIT

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

Final Assessment Test(FAT) - Apr/May 2025

Programme	**B.Tech.**	Semester	**Winter Semester 2024-25**
Course Code	**BCSE309L**	Faculty Name	**Prof. Balasaraswathi**
Course Title	**Cryptography and Network Security**	Slot	**B2+TB2**
		Class Nbr	**CH2024250501877**
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

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. An old woman goes to the market, and a horse steps on her basket and crushes the eggs. The rider offered to pay for the damages and asked her how many eggs she had brought. She does not remember the exact number, but 2 eggs were left when she took them out five at a time. There were 3 eggs left when she picked them out seven at a time, but they came out 10 when she took them eleven at a time. Find the smallest number of eggs she could have had.

[10] (CO1/K3)

02. i) An important property which makes DES secure is that the S-boxes are nonlinear. Prove this property by computing the output of S_1 for several pairs of inputs. That is, show that $S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$, where "$\oplus$" denotes bitwise XOR, for: [6 marks]

a) x_1=000000, x_2=000001
b) x_1=111111, x_2=100000
c) x_1=101010, x_2=010101

Table of S-box S1

S1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	00	09	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

ii) A secure messaging application needs to generate a random session key for encrypting messages between users. In order to use the application, Mr. Ram is testing two linear congruential generators (LCGs) to generate pseudo-random sequences with a full period.

LCG1: $X_{n+1} = (9x_n) \bmod 13$

LCG 2: $X_{n+1} = (4x_n) \bmod 13$

Generate the pseudo random sequences, if the initial seed $x_0 = 2$. Also, help Mr. Ram to identify which one appears more random. [4 Marks]

[10] (CO2/K3)

03. Ms. Inarve is the Chief Security Officer of a multinational corporation that deals with highly sensitive trade secrets. To ensure the confidentiality of internal communications, the company implements RSA public-key cryptography for secure message exchange. A senior executive, Mr. Mark, needs to securely send a confidential message M=90 to Ms. Inarve from potential eavesdroppers with the following parameters: p=19, q=11, and public key = 103. Illustrate the steps performed by Mr. Mark and Ms. Inarve to ensure confidential communication. Suppose an attacker intercepts the encrypted message, without knowing Ms. Inarve's private key, explain why it is computationally infeasible for the attacker to decrypt the message.

[10] (CO2/K3)

04. Ryan, Olivia, and Noah are three cybersecurity specialists working for a space research organization. They need to establish a secure communication channel to discuss a classified project without anyone intercepting their messages. Since they are in different locations, they decide to use the Diffie-Hellman key exchange to generate a common secret key for encrypting their communication. To achieve this, they agree on a public prime number q=23 and a primitive root g=5. Each expert privately selects a secret key: Ryan chooses X_A=6, Olivia chooses X_B =15 and Noah chooses X_C =10.

a) Compute the public keys for Ryan, Olivia, and Noah. [3 marks]

b) Compute the final shared secret key they all share. [7 marks]

[10] (CO2/K6)

05. A secure communication system employs the MD5 hash function with a 16-bit word instead of the full 32-bit version to authenticate short messages. Consider the message M_0=0xCDEF and key K_0=0x5A82. Perform one buffer operation for the third round of the MD5 algorithm with <<<7(left rotation by 7 bits). Show your step-by-step workings and provide the final values of the 4 buffers A, B, C, D. Assume the initial values of the 4 buffers as: A = 0x0123; B = 0x89AB; C = 0xFEDC; D = 0x7654.

[10] (CO3/K3)

06. FinSecure Bank processes thousands of sensitive financial transactions daily, including fund transfers and account updates. To protect customer data, it implements message confidentiality and authentication tied to ciphertext ensuring data integrity and authenticity during sensitive transactions. Consider a transaction where:

- Message: 0x8376
- Key K1: 0x4892 (used for encryption)
- Key K2: 0x536240 (used for generating the Message Authentication Code)

Demonstrate how can FinSecure ensure that any modification to the encrypted message is detected while maintaining both confidentiality and authenticity? Assume bitwise XOR operation for both encryption and MAC.

[10] (CO3/K2)

07. Mr. Arun is an IT administrator at a large university who manages a secure network for students, faculty, and administrative staff. To enhance security and prevent unauthorized access, the university implements the Kerberos authentication protocol for all internal systems, including email, library access, and student portals. One day, a professor, Dr. Lisa, tries to log into the university's research database from her office computer. She enters her username and password, and the system authenticates her successfully. However, later in the day, she notices that she can still access the system without re-entering her credentials. Meanwhile, a suspicious login attempt from an unauthorized device is flagged in the network logs.

Elucidate how Kerberos ensures secure authentication when Dr.Lisa logs into the research database, detailing the steps involved inpreventing unauthorized access and ensuring mutual authentication between her workstation and the database server. List the additional security measures canMr. Arun implement to strengthen the Kerberos authentication system against cyber threats.

[10] (CO3/K2)

08. A multinational company, SecureCorp, wants to establish a secure communication channel between its headquarters and a branch office over the internet. The IT team must ensure that the data remains confidential, tamper-proof, and that only authorized devices can communicate. To achieve this, they decide to implement IPSec.

a) Identify the IPSec mode should be used, and why? [2 marks]

b) Should the IT team implement Authentication Header, Encapsulating Security Payload, or a combination of both? Justify your choice. [2 marks]

c) How will Security Associations (SAs) and the Security Association Database (SAD) help in managing secure communication? [2 marks]

d) Explain the role of Security Policies in ensuring that only specific traffic is protected under IPSec. [4 marks]

[10] (CO4/K4)

09. Assume that you work in a company that handles sensitive client information. Your manager asks you to send a confidential email to a client using S/MIME to ensure the message is encrypted and digitally signed. The client has provided their public S/MIME certificate, and you have your own S/MIME certificate installed in your email client. Illustrate the steps you would take to send this email securely and what happens on the client's end when they receive it.

[10] (CO4/K1)

10. CyberShield Ltd, is setting up a multi-layered firewall architecture to protect its internal network from cyber threats. You are the network security engineer responsible for implementing and optimizing firewall rules.
Network Setup & Security Requirements:

- Branch Office Network: Employees need to access web applications (HTTP/HTTPS), email servers (IMAP/SMTP), and a cloud-based VPN.
- Main Data Center: Hosts sensitive financial applications and a private database (SQL Server). Only internal systems should communicate with it.
- External Threats: Recent security logs show an increase in brute force login attempts and malware-infected traffic targeting the company's web servers.

Analyze the effectiveness of each firewall type in the given setup. Which security threats does each mitigate, and what are their potential weaknesses?

[10] (CO4/K2)

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

⇔⇔⇔