REG.NO.:

VIT

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

SCHOOL OF COMPUTER SCIENCE ENGINEERING AND INFORMATION SYSTEMS

CAT-2

WINTER SEMESTER 2025-2026

SLOT: D2+TD2

Programme Name & Branch : B.Tech – Information Technology
Course Code and Course Name : BITE401L - Network and Information Security
Faculty Name(s) : Dr. K. John Singh, Dr. S. P. Shantharajah, Dr. L. Thanga Mariappan
Class Number(s) : VL2025260502223, VL2025260502226, VL2025260502227
Date of Examination : 18-03-2026
Exam Duration : 90 minutes **Maximum Marks: 50**

General instruction(s):

- Answer All Questions
- M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)
- Course Outcomes
  CO2. Analyze and evaluate cryptographic primitives
  CO4: Design and develop security solutions.

Q. No	Question	M	CO	BL
1.	A secure communication system used by a research laboratory transmits confidential experimental results using the ElGamal public key cryptosystem. Dr. Ram wants to send a secret message to Dr. Anbu. To establish secure communication, Dr. Anbu generates his keys using the following parameters: prime number $p = 23$, primitive root $g = 5$, and private key $x = 6$. Using these values, he computes and publishes his public key. Dr. Ram intends to send the message $M = 10$ and, during the encryption process, randomly selects $k = 7$. Based on the ElGamal encryption algorithm, determine Dr. Anbu's public key, compute the ciphertext pair (C_1, C_2) produced during encryption, and demonstrate how Dr. Anbu decrypts the received ciphertext to recover the original message. Finally, discuss the security challenges of this communication system, such as the weakness caused by using very small parameter values (like $p = 23$), the risk of brute-force or discrete logarithm attacks, the importance of choosing a truly random value of k, and how improper parameter selection could compromise the confidentiality of the transmitted message.	10	CO2	BL3
2.	Alice and Bob use the Diffie–Hellman key exchange technique to securely establish a shared secret key over an insecure network. They agree on the common public parameters: prime number $q = 23$ and primitive root $\alpha = 5$. During the key exchange process, Bob publishes his public key $Y_B = 10$. Determine Bob's private key X_B such that $Y_B = \alpha^{X_B} \bmod q$. Alice publishes her public key $Y_A = 8$. Using these values, compute the shared secret key Kestablished between Alice and Bob. Also verify that 5 is a primitive root modulo 23. Finally, discuss the challenges and security issues associated with this key exchange process, such as the vulnerability to man-in-the-middle attacks, the risks of using small prime numbers, and the computational difficulties associated with solving the discrete logarithm problem that forms the basis of the protocol's security.	10	CO2	BL3
3.	Consider the elliptic curve $E_7(2,1)$, defined by the equation $y^2 = x^3 + 2x + 1$ over the finite field with modulus $p = 7$. Determine all the points that lie on the elliptic curve $E_7(2,1)$ by evaluating the equation for all possible values of $x$and $y$in the field $0 \leq x, y < 7$, and include the point at infinity. After	10	CO2	BL3

REG.NO.:

VIT

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

SCHOOL OF COMPUTER SCIENCE ENGINEERING AND INFORMATION SYSTEMS

CAT-2

WINTER SEMESTER 2025-2026

SLOT: D2+TD2

	identifying the complete set of points on the curve, discuss the significance of these points in the context of elliptic curve arithmetic and explain how such curves are used in cryptographic systems.			
4.	A multinational cloud storage provider operates a distributed platform that hosts large volumes of user data, including critical software update packages used by organizations worldwide. To ensure file integrity, the system employs a cryptographic hash function that generates a fixed-length digest for each uploaded file, which is stored in a centralized verification database along with metadata such as file ID, uploader credentials, and timestamps. Whenever a file is downloaded, the system recomputes the hash value and compares it with the stored digest to confirm that the file has not been altered during storage or transmission. During a routine cybersecurity audit, analysts discover that a widely distributed software update hosted on the platform has been secretly replaced with a malicious version containing hidden malware designed to compromise user systems. Surprisingly, the altered file successfully passes the platform's integrity. verification process because the computed hash value of the malicious file matches the original hash stored in the database. A detailed forensic investigation reveals that the attacker deliberately exploited a weakness in the hash algorithm used by the system, allowing the creation of two different files that produce the same hash value. Considering this scenario, identify which fundamental security requirement of cryptographic hash functions has been violated, explain the three main security properties required for a secure hash function, analyze how an attacker could generate two different files with identical hash values, evaluate the potential risks this attack poses to both the cloud service provider and its users, and recommend two effective security improvements that the company should implement to prevent such attacks in the future.	10	CO2	BL4
5.	A financial institution uses the Hash-based Message Authentication Code (HMAC) algorithm to ensure the integrity and authenticity of transaction messages exchanged between its ATM machines and the central banking server. Each ATM shares a secret key with the server, and before sending a transaction request, such as withdrawal or balance inquiry; the ATM computes an HMAC value using a secure hash function like SHA-512. The generated HMAC is appended to the message and sent to the server. Upon receiving the message, the server recomputes the HMAC using the same secret key and verifies whether it matches the received HMAC value. During a security audit, it is discovered that an attacker intercepted several transaction messages but was unable to modify the message contents without detection. However, the audit team raises concerns about possible replay attacks and improper key management. Explain the working principle of the HMAC algorithm in this scenario. Describe how HMAC ensures message integrity and authentication, illustrate the steps involved in generating and verifying the HMAC value, and analyze two potential security risks, such as replay attacks or weak key management that may still exist even when HMAC is used. Also suggest appropriate countermeasures to mitigate these risks.	10	CO4	BL4

****