B/E/TY

Reg. No:

Final Assessment Test – April 2025

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

Course: **BCSE309L - Cryptography and Network Security**

Class NBR(s): **1771/1774/1777/1780/1787/1793/1808/ 1812/1815/1823/1826/1832/1860/1869/1885/1892/ 1905/1923/1924/1928/1935/1942/1947/1949/1956/ 2350**

Slot: **E1+TE1**

Time: **Three Hours**

Max. Marks: **100**

- **KEEPING MOBILE PHONE/ANY ELECTRONIC GADGETS, EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE**
- **DON'T WRITE ANYTHING ON THE QUESTION PAPER**

Answer ALL Questions

(10 X 10 = 100 Marks)

1. a) Find the integer value of **x** that satisfies the following system of congruence's: **[6] BL2 CO1**

   $3x \equiv 2 \pmod{11}$
   $7x \equiv 9 \pmod{13}$
   $4x \equiv 14 \pmod{15}$

   b) Using the extended Euclidean algorithm, find the multiplicative inverse of **7465 mod 2464**. **[4]**

2. a) State and use the Fermat's theorem to find **4^{225} mod 13.** **[3] BL2 CO1**

   b) Perform **encryption** and **decryption** on the given plaintext using the **Hill Cipher** technique with the provided key matrix. **[7]**

   Plaintext: **CSE.** Map letters to numbers using **A = 0, B = 1, ..., Z = 25** and consider modulo 26.

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

3. You are given an **8-bit RC4 stream cipher** with the following parameters: **BL3 CO2**

   Key: **K=[1,0,0,2]** and Plaintext: **P=[6,1,5,4]**

   Illustrate the **key generation**, **encryption and decryption process** in step by step.

4. Given a plaintext "**VIT**", using the **SHA-512** algorithm, derive the following information. Consider the ASCII values for the plaintext: V = 86, I = 73, T = 84 **BL3 CO3**

   a) Determine the length of padding bits required. **[2]**
   b) Generate the sixteen 64-bit words (W0 to W15) in hexadecimal format. **[2]**
   c) Compute the **majority** function of the round operation using buffers A, B, and C. **[2]**
   d) Compute the **choice** function of the round operation using buffers E, F, and G. **[2]**

   Consider the following buffer values:

   A = 01100001
   B = 01100010
   C = 01100011
   E = 01100101
   F = 01100110
   G = 01100111

   e) What are the essential characteristics that ensure the security of a cryptographic hash function? **[2]**

5. Aryan and Beena use the **Diffie-Hellman Key Exchange** with p=23 and g=5. Aryan's private key is a=6, and Beena's private key is b=15. **BL4 CO2**

a. Compute the shared secret key they establish. **[3]**

Eshaan intercepts their communication and performs a **Man-in-the-Middle (MitM) attack**, using private keys e1=8 (with Aryan) and e2=10 (with Beena).

b. Compute the shared keys between Aryan-Eshaan and Beena-Eshaan. **[3]**

c. Explain why Aryan and Beena fail to secure their communication. **[2]**

d. Suggest a countermeasure against the MitM attack. **[2]**

6. The ECC cryptosystem defined by $y^2 = x^3 + x + 6$ over F_{11} and G = (2, 7). B's secret key is 3. A wishes to encrypt the message, M = (10, 9) and chooses the random value k=2. Find B's public key and determine the cipher text C. **BL3 CO2**

7. Why do some cryptographic algorithms, such as RSA, ECC, AES, and SHA-512, remain successful, while others, like MD5 and DES, have failed? Analyse the factors that contribute to the longevity or downfall of cryptosystems, including security strength, computational efficiency, and resistance to attacks. **BL4 CO3**

8. a) How do HMAC and Digital Signatures ensure message integrity and authentication? Compare their working principles, security guarantees, and real-world applications. Additionally, analyse why digital signatures provide non-repudiation while HMAC does not. **[5] BL5 CO3**

b) Illustrate the signing and verification process of the ElGamal digital signature scheme with a step-by-step example. **[5]**

9.a) Consider the following threats to Web security and describe how each is countered by a particular feature of TLS. **BL6 CO4**

- Brute-Force Attack – Exhaustive key search.
- Replay Attack – Reuse of previous TLS handshake messages.
- Man-in-the-Middle Attack – Interception during key exchange.
- Password Sniffing – Eavesdropping on credentials in transit.
- IP Spoofing – Forged IP addresses to send bogus data.
- IP Hijacking – Taking over an active, authenticated session.

OR

9.b) An organization wants to implement end-to-end security between remote branches using IPSec. However, it also needs to maintain compatibility with older network devices that do not support IPSec. Propose a hybrid security solution that integrates IPSec with other security protocols while addressing performance and interoperability challenges. **BL6 CO4**

10.a) A financial institution wants to implement a Secure Electronic Transaction (SET) protocol for online payments. However, they are concerned about the computational overhead and user experience. Design a security model that balances strong encryption with minimal performance impact, and justify your choices. **BL6 CO4**

OR

10.b) Design next-generation firewall architecture for a government intelligence agency handling classified data. Your design should integrate advanced filtering techniques, address potential insider threats, and ensure optimal security without compromising performance. Justify your design choices and propose innovative strategies to enhance security beyond conventional firewall mechanisms. **BL6 CO4**

⇔⇔⇔ **B/E/TY** ⇔⇔⇔