REG.NO.:

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

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
WINTER SEMESTER 2024-2025

SLOT: E2 + TE2

Programme Name & Branch	**:** B.Tech. & Computer Science and Engineering	
Course Code and Course Name	**:** BCSE309L & Cryptography and Network Security	
Faculty Name(s)	**:** Applicable to all	
Class Number(s)	**:** Applicable to all	
Date of Examination	**:** 20-March-2025	
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 – Analyze, 5 – Evaluate, 6 – Create)
- **Course Outcomes**
  CO2 - To understand concept of various cryptographic techniques.
  CO3 - To apprehend the authentication and integrity process of data for various applications.

Q. No.	Question	M	CO	BL
1.	Emma, a security consultant, wants to securely send a confidential message, "INTELLIGENT," to her colleague Liam using RSA encryption. She decides to use a public-key cryptosystem where the modulus is n=17680 and the encryption exponent is e=3. To ensure that only Liam can decrypt the message, Emma encrypts it using the 00-26 encoding scheme. Meanwhile, Liam, who holds the secret decryption key, must compute the private exponent, d to retrieve the original message. Show the ciphertext of the message sent to Liam and compute d, the private exponent required to decrypt the ciphertext. **ANSWER**: $n = 17680$, $e = 3$, $m =$ 'INTELLIGENT' Encode the message: I → 08 I → 08 N → 13 G → 06 T → 19 E → 04 E → 04 T → 19 L → 11 The plaintext is 08131904111108060413 19 Encrypting the message: Create 4 digit blocks so that the value of each block be less than 'n' $C = m^e \bmod n$	10	2	3

$P_1 = 0813 \Rightarrow C_1 = 813^3 \bmod 17680 = 1877$

$P_2 = 1904 \Rightarrow C_2 = 1904^3 \bmod 17680 = 15504$

$P_3 = 1111 \Rightarrow C_3 = 1111^3 \bmod 17680 = 16791$

$P_4 = 0806 \Rightarrow C_4 = 0806^3 \bmod 17680 = 13416$

$P_5 = 0413 \Rightarrow C_5 = 0413^3 \bmod 17680 = 7877$

$P_6 = 19 \Rightarrow C_6 = 19^3 \bmod 17680 = 6859$

Find Private Key for Decryption

$d \equiv e^{-1} \bmod \phi(n)$

$d \equiv 3^{-1} \bmod \phi(17680)$

Euler totient Function $\phi(17680)$ } $n \Rightarrow$ Cannot be splited into two prime numbers

$n = 17680 = 2^4 \times 5 \times 13 \times 17$

$\phi(17680) = 17680 \times (1-1/2)(1-1/5)(1-1/13)(1-1/17)$

$\phi(17680) = 6144$

$d \equiv 3^{-1} \bmod 6144$ does not exist.

∴ The private Component 'd' Cannot be Computed.

2.	Given a prime number p=233 and a primitive root g=5, Alice chooses a secret key a=191 and Bob chooses a secret key b=211. However, an attacker Eve performs a Man-in-the-Middle (MITM) attack by intercepting and replacing the public keys exchanged between Alice and Bob. Instead of forwarding the correct values, Eve sends her own public keys to both parties. Eve selects her secret key as e_1=181 and e_2=157 for Alice and Bob respectively. a. Compute the public keys that Eve sends to Alice and Bob. [4] b. Compute shared secret keys between Alice and Eve, and between Bob and Eve. [4] c. Show that Alice and Bob end up with different secret keys due to the attack. [2] **Answer**	10	2	3

$p = 233, g = 5, a = 191, b = 211, e_1 = 181, e_2 = 157$

Compute Alice's public key

$A = g^a \bmod p$

$= 5^{191} \bmod 233$

$\boxed{A = 213}$

Compute Bob's public key

$B = g^b \bmod p$

$= 5^{211} \bmod 233$

$\boxed{B = 68}$

Compute public key Sent to Alice by Eve

$E_A = g^{e_1} \bmod p$

$= 5^{181} \bmod 233$

$\boxed{E_A = 172}$

Compute public key Sent to Bob by Eve

$E_B = g^{e_2} \bmod p$

$= 5^{157} \bmod 233$

$\boxed{E_B = 211}$

Compute Shared key b/w Alice & Eve

$S_{AE} = [E_A]^a \bmod p$

$= [172]^{191} \bmod 233$

$S_{AE} = 125$

Compute Shared key b/w Bob & Eve

$S_{BE} = [E_B]^b \bmod p$

$= [211]^{211} \bmod 233$

$\boxed{S_{BE} = 106}$

C) In a normal Diffie-Hellman exchange, Alice and Bob would compute the same shared secret key.

But Alice receives the public key [E_A = 172] sent by Eve.

Bob also receives the public key [E_B = 211] sent by Eve.

However, due to Eve's attack, the shared secrets are:

S_{AE} = 125 and S_{BE} = 106

$S_{AE} \neq S_{BE}$

Thus, Alice and Bob end up with different secret keys as a direct result of Eve's interference in the public key exchange, illustrating the impact of the man-in-the-middle attack.

REG.NO.:

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

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
WINTER SEMESTER 2024-2025

SLOT: E2 + TE2

3.	a. David, a cybersecurity researcher, is analysing the security of a hashing algorithm used in digital forensics. As part of his research, he needs to compute a specific word in the SHA-512 message schedule expansion for a given set of 16-bit hexadecimal words. He has been provided with the following words: W_0=0x1234, W_1=0xFEDC, W_2=0x0011, W_3=0x8899, W_9=0x5555, W_{14}=0x1111 Using SHA-512's word expansion and addition modulo 2^{16}, David must compute the value of W_{16}.	8	3	4

ANSWER:

$W_0 = 1234$, $W_1 = FEDC$, $W_2 = 0011$, $W_3 = 8899$, $W_9 = 5555$

$W_{14} = 1111$

$W_{16} = \sigma_1(W_{14}) + W_9 + \sigma_0(W_1) + W_0$

Find $\sigma_1(W_{14})$: $W_{14} = (0001\ 0001\ 0001\ 0001)_2$

$\sigma_1(W_{14}) = ROTR^{19}(W_{14}) \oplus ROTR^{61}(W_{14}) \oplus SHR^6(W_{14})$

$ROTR^{19}(W_{14}) = 0010\ 0010\ 0010\ 0010 \rightarrow A$

$ROTR^{61}(W_{14}) = 1000\ 1000\ 1000\ 1000 \rightarrow B$

$SHR^6(W_{14}) = 0000\ 0000\ 0100\ 0100 \rightarrow C$

$A \oplus B$:
0010 0010 0010 0010
1000 1000 1000 1000
1010 1010 1010 1010 → D

$D \oplus C$:
1010 1010 1010 1010
0000 0000 0100 0100
1010 1010 1110 1110

$\sigma_1(W_{14}) = (1010\ 1010\ 1110\ 1110)_2 = (AAEE)_{16}$

Find $\sigma_0(w_1)$: $w_1 = (1111\ 1110\ 1101\ 1100)_2$

$\sigma_0(w_1) = ROTR^1(w_1) \oplus ROTR^8(w_1) \oplus SHR^7(w_1)$

$ROTR^1(w_1) = 0111\ 1111\ 0110\ 1110 \rightarrow A$

$ROTR^8(w_1) = 1101\ 1100\ 1111\ 1110 \rightarrow B$

$SHR^7(w_1) = 0000\ 0001\ 1111\ 1101 \rightarrow C$

$A \oplus B$:

$0111\ 1111\ 0110\ 1110$
$1101\ 1100\ 1111\ 1110$
$1010\ 0011\ 1001\ 0000 \rightarrow D$

$D \oplus C$:

$1010\ 0011\ 1001\ 0000$
$0000\ 0001\ 1111\ 1101$
$1010\ 0010\ 0110\ 1101$

$\sigma_0(w_1) = (1010\ 0010\ 0110\ 1101)_2 = (A26D)_{16}$

$W_{16} = (AAEE + 5555 + A26D + 1234) \bmod 2^{16}$

Convert Hexadecimal to Decimal

$= (43758 + 21845 + 41581 + 4660) \bmod 65536$

$= 111844 \bmod 65536$

$= (46308)_{10}$

$W_{16} = (B4E4)_{16}$

b.	Compute and show the result of the function which is used in SHA-512 round operations and acts on the first three buffers (64bits each). a = 510E527FADE682D1 e = 6A09E667F3BCC908 b = 9B05688C2B3E6C1F f = BB67AE8584CAA73B c = 1F83D9ABFB41BD6B g = 3C6EF372FE94F82B d= 5BE0CD19137E2179 h = A54FF53A5F1D36F1	2	3	4

	ANSWER: A = 01010001000011100101001001111111101011011110011010000001011010001 B = 10011011000001010110100010001100001010110011111001101100000011111 C = 00011111100000111101100110101011111110110100000110111101011011011 **Maj(A,B,C)=(**A∧B)⊕(A∧C)⊕(B∧C) (A AND B) = 00010001000001000100000000001100001010010010011000000000000010001 (A AND C) = 00010001000000100101000000101011101010010100000010000000010000001 (B AND C) = 00011011000000001010010001000100000101011000000000011011000000101 1 (A∧B)⊕(A∧C)⊕(B∧C) 00011011000001110101100010101111101010110110011010110000000000101 **Maj(A,B,C)=1B0758AFAB66B005**			
4.	a. HMAC is used for message authentication in a banking system. If an attacker can observe the HMAC output but not the key: i. Can they forge a valid message? Justify. [2] ii. How does HMAC resist preimage attacks? [3] **ANSWER**: **(i) Can an attacker forge a valid message? Justify** No, an attacker cannot forge a valid message if they do not know the secret key. **Reason:** • **HMAC relies on a secret key (KKK)**: Unlike regular hashing, which only depends on the message, HMAC requires a **shared secret key**. • **Collision resistance**: Even if an attacker can generate hash collisions in the underlying hash function (e.g., SHA-256), **they still need the secret key** to create a valid HMAC. • **One-way property**: Given an HMAC output, an attacker cannot reverse-engineer the key or the message. **Example Scenario:** • Suppose a bank sends **HMAC(Message, Key)** = abcd1234 for "Transfer $100 to Bob". • If an attacker changes the message to "Transfer $1000 to Mallory", they must also generate a valid HMAC for it. • Since the key is unknown, generating a new valid HMAC is **computationally infeasible**. **Conclusion:** Without knowing the secret key, an attacker cannot forge a valid message-HMAC pair**.** **(ii) How does HMAC resist preimage attacks?** A preimage attack occurs when an attacker tries to find a message that produces a given hash value. HMAC resists this attack due to: **(a) Use of a Secret Key**	5	3	2

- A regular hash function (e.g., SHA-256) only depends on the message, making it vulnerable to preimage attacks.
- HMAC includes a secret key:
  - HMAC = Hash (Key ⊕ opad || Hash (Key ⊕ ipad || Message))
  - Since the attacker does not know the key, they cannot generate valid HMACs, even if they find hash collisions.

(b) Nested Hashing Mechanism

- HMAC applies two layers of hashing:
  1. Inner hash: Hashes the message combined with the key.
  2. Outer hash: Hashes the output again with the key.
- This ensures that even if an attacker finds a preimage for the inner hash, they still cannot compute the final HMAC without knowing the key.

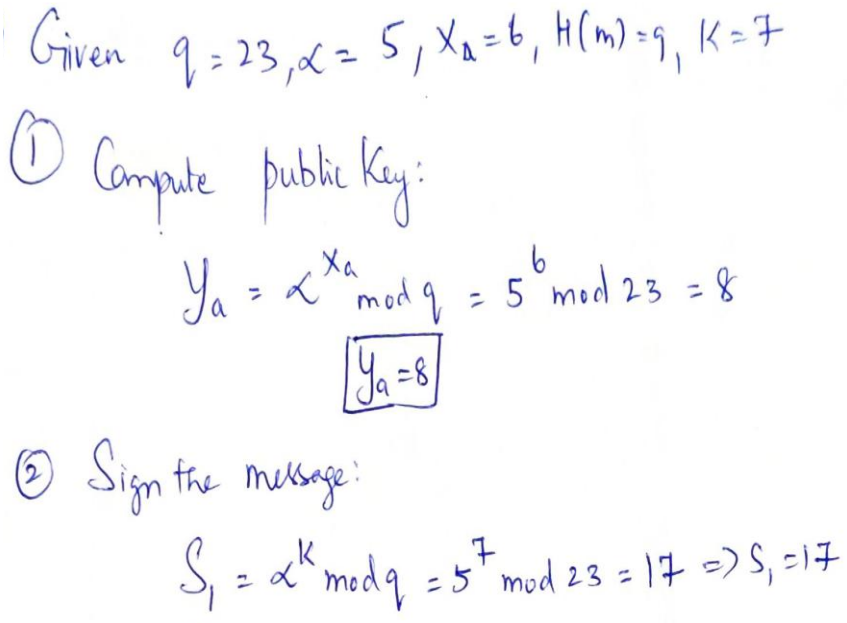
(c) Security of Modern Hash Functions

- If the hash function (e.g., SHA-256) is strong, it is already resistant to preimage attacks.
- Since HMAC uses the hash function twice with a secret key, it is even more secure.

Conclusion: HMAC resists preimage attacks because the attacker does not know the key, and the structure makes it infeasible to reverse-engineer the original message.

b.	Alice wants to sign a message using the ElGamal signature scheme with small values for easy computation. She chooses a prime modulus q=23, a generator α=5, and her secret key X_a=6. She needs to sign a message with hash value h(M)=9 using a randomly chosen integer k=7. Illustrate the steps involved in signing process and the verification process.	5	3	2

ANSWER



$S_2 = k^{-1}(H(m) - X_a S_1) \bmod (q-1)$

$= [7^{-1}(9 - (6 \times 17))] \bmod 22$

$= [7^{-1}(-93)] \bmod 22 \qquad [7^{-1} \bmod 22 = 19]$

$= [19 \times (-93)] \bmod 22$

$\boxed{S_2 = 15}$

(3) Verify the message:

$V_1 = H(m) \bmod q = 5^9 \bmod 23 = 11$

$V_2 = (Y_a)^{S_1} (S_1)^{S_2} \bmod q = 8^{17} \cdot 17^{15} \bmod 23$

$= (13 \times 15) \bmod 23 = 11$

$V_1 = V_2 \Rightarrow$ Valid signature.

5.	Bob wants to generate a digital signature using DSA with the prime modulus p=67, subgroup order q=11, and h=3. i. Compute the value of g and check whether it is prime or not. [4] ii. Assume if Bob selects the per message secret integer as 7, the pseudo random integer, k as 5 and the hash of the message as 13, what would be the signer digital signature component. [4] iii. How does the receiver verify the signature component sent by Bob? [2] **ANSWER**:	10	3	3

$p = 67, \quad q = 11, \quad h = 3$

i) Compute the value of g: ⟶ (4 Marks)

$g = h^{(p-1)/q} \bmod p$

$= 3^{(66)/11} \bmod 67 \quad = 3^6 \bmod 67$

$\boxed{g = 59}$ ⟶ (2 Marks)

ii) Use Rabin-Miller (or) equivalent methods to verify the primality of $g = 59$ ⟶ (3 Marks)

ii) Secret integer $x = 7$, $H(M) = 13$, ~~$K = 5$~~ $k = 5$

Find y: $y = g^x \bmod p$

$= 59^7 \bmod 67 = 15$

$\boxed{y = 15}$

Generating Signature

$r = (g^k \bmod p) \bmod q$

$= (59^5 \bmod 67) \bmod 11$

$\boxed{r = 7}$

$S = [k^{-1}\{H(M) + x * r\}] \bmod q$

$= [5^{-1}\{13 + (7*7)\}] \bmod 11$

$= (5^{-1} \times 62) \bmod 11 = (9 \times 62) \bmod 11 \quad [\because 5^{-1} \bmod 11 = 9]$

$\boxed{S = 8}$

Signature $= (7, 8)$

iii) Verify the Signature;

$w = (S)^{-1} \bmod q = 8^{-1} \bmod 11 = 7$

$u_1 = (H(M) \times w) \bmod q = (13 \times 7) \bmod 11 = 3$

$u_2 = (r \times w) \bmod q = (7 \times 7) \bmod 11 = 5$

$v = ((g^{u_1} \times y^{u_2}) \bmod p) \bmod q = ((59^3 \times 15^5) \bmod 67) \bmod 11$

$= 62 \bmod 11$

$\boxed{v = 7}$

Test, $V = r \Rightarrow 7 = 7$:

The Signature is valid.

****