REG.NO.:

VIT®
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: E1 + TE1

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 : **20.03.25**
Exam Duration : **90 minutes** **Maximum Marks: 50**

Answer Key

Q. No	Question	M	CO	BL
1.	A logistics company specializing in secure supply chain management is implementing elliptic curve cryptography to protect data integrity in shipment tracking. The system uses the elliptic curve equation E : $y^2 = x^3 + 7x + b \ (mod\ 11)$ a) The company wants to determine the value of coefficient 'b' for the point P = (4,5) and verify whether this point 'P' lies on the curve. (2 marks) b) Generate a set of points on the given elliptic curve E. (2 marks) c) Given a point P = (4,5), compute the result of 6P, and -P. (6 marks) **Solution:** (a) Given P = (4,5), then x = 4 and y = 5 $y^2 mod\ 11 = x^3 + 7x + b\ mod\ 11$ $5^2 mod 11 = 4^3 + 7(4) + b(mod 11)$ b ≡ 3−4(mod11) b = 10 (b) Consider the given equation with b value; Y^2 mod 11 = X^3 + 7X + 10 mod 11 List of points in the curve: (3,5), (3,6), (4,5), (4,6), (5,4), (5,7), (6,2), (6,9) (c) P = (4,5) $\lambda = [(3x^2+a)/(2y)] \bmod p$ $x_3 = \lambda^2 - x - x \bmod p$ $y_3 = \lambda (x - x_3) - y \bmod p$ 2P = (3,6), 3P = (5,7),4P=(6,2), 5P=(6,9), **6P=(5,4)** **-P** = (4,-5) mod 11 = **(4,6)**	10	2	3
2.	A military intelligence unit needs to securely transmit confidential mission coordinates using ElGamal encryption to prevent enemy interception. The unit commander, Alex, is responsible for decrypting messages. a) Alex chooses a private key of 26 and utilizes a publicly agreed generator (g) = 7 and prime number (p) = 71. Determine Alex's public key and show your calculations. (2 marks)	10	2	3

	$X^3 + 7X + 10$ mod 11	Y^2 mod 11
0	10	0
1	7	1
2	10	4
3	3	9
4	3	5
5	5	3
6	4	3
7	6	5
8	6	9
9	10	4
10	2	1

	b) Suppose the message to be sent is 30. An intelligence officer randomly selects k = 2 for encryption. Compute the encrypted message and provide the necessary workings. (4 marks) c) If Alex must choose a different value of k so that the encoding of message 30 is C = (59, C2), what is the integer C2? (4 marks) **Solution:** a) Public key: $e \equiv g^d \bmod p = 7^{26} \bmod 71 = \mathbf{3}$ b) $C1 = g^k \bmod p = 7^2 \bmod 71 = 49$ $C2 = (m * e^k) \bmod p = (30 * 3^2) \bmod 71 = 57$ **(C1,C2) = (49,57)** c) Given, (C1=59,C2=?) $C1 = g^k \bmod p$ $59 = 7^k \bmod 71 \Rightarrow \mathbf{k = 3}$ $C2 = (m * e^k) \bmod p = (30 * 3^3) \bmod 71 = 29$ **C2 = 29**			
3.	A financial institution is implementing MD5 hashing to ensure the integrity of transaction messages. As part of a security audit, analysts are required to examine how MD5 processes a given transaction message. Given that the message is processed into 1009 blocks, and the padding size (excluding the length field) is 43 bytes, determine the following: a) Calculate the total size of the padded message in bits. (2 marks) b) Determine the original message size before padding was added. (2 marks) c) How are the logical functions applied to the leftmost digits of the following buffers in each round operation? Given: B = 0xDEE0, C = 0x7792, D = 0xA8CC. (6 marks) **Solution:** a) Total padding (padding + length field) = 43 + 8 = 51 bytes = 408 bits. b) Total message size after padding = 1009×64=64576 bytes Original message size=Total size−Total padding = 64576−51 =64525 bytes c) $B= (1101\ 1110\ 1110\ 0000)_2$, $C= (0111\ 0111\ 1001\ 0010)_2$, $D= (1010\ 1000\ 1100\ 1100)_2$ $F = (B \wedge C) \vee ((\neg B) \wedge D) = 0x768C$ $G= (B \wedge D) \vee (C \wedge (\neg D)) = 0xDFD1$ $H= B \oplus C \oplus D = 0x01BE$ $I=C \oplus (B \vee (\neg D)) = 0xA861$	10	3	3
4.	a) Assume a security system uses the SHA-1 hash function. Using the birthday paradox, estimate the approximate number of random hashes required to have a 50% probability of finding a collision. $N \approx 1.2 \times \sqrt{2^n}$, where $n = 160$. **Step 1: Compute the Square Root** $\sqrt{2^{160}} = 2^{80}$ Since $2^{80} \approx 1.21 \times 10^{24}$, **Step 2: Apply the Birthday Bound Formula** $N \approx 1.2 \times 2^{80}$ $N \approx 1.2 \times 1.21 \times 10^{24}$ $N \approx 1.45 \times 10^{24}$	5	3	3

	b) At VIT, the VTOP Intranet portal maintains detailed system logs that record every user action, such as grade submissions, fee payments, and attendance updates. Each log entry is associated with the user's ID and timestamped to provide a record of activities. However, the system does not implement any mechanism to verify whether the data transmitted or stored has been altered. Does this system ensure integrity, non-repudiation, or both? Justify your answer with respect to security principles. **Solution:** This system ensures non-repudiation because system logs provide a record of user activities, making it difficult for a user to deny performing an action. However, it does not ensure integrity, as an attacker with sufficient privileges could modify stored logs or alter data in transit. To ensure both integrity and non-repudiation, cryptographic techniques such as hashing (e.g., SHA-256) and digital signatures should be used to detect any unauthorized data modifications.	5		
5.	Use the RSA Digital Signature scheme. Given the prime numbers p=11 and q=13, and the public key exponent e=7, perform the following tasks: (a) How do you know the choice of e is valid? (2 marks) (b) Compute the private key exponent d. (2 marks) (c) Generate the digital signature for the given hash code w = 25. (3 marks) (d) Verify the signature to confirm the integrity and non-repudiation of the source. (3 marks) **Solution:** (a) n=143, $\Phi(n)=120$ gcd(e, $\Phi(n)$) = 1 and $1 < e < \Phi(n)$. (b) $e*d = 1 \bmod \Phi(n)$ d = 103 (c) $S = W^d \bmod n = 25^{103} \bmod 143 = 38$ (d) $M' = S^e \bmod n = 38^7 \bmod 143 = 25$ Hence verified.	10	3	3

****