DEPARTMENT OF CSE and CSE-AIML

III SEMESTER B. TECH

MID-TERM QP

SUBJECT: Principles of Cryptography (PC) CSE3121

SET-1 (Mid-term)					
Q. No.	**Questions**	**M**	**CO (CLO)**	**LO**	**BL**
1	Akshay sends a message 'hi' to Akash at 6pm. However, when Akshay and Akash meet in real at 8pm, Akshay denies that he had sent the message to Akash. Make use of the described scenario, the attacker and the security goal being breached are respectively: (A) Akshay, Authentication (B) Akash, Accountability, (C) Akshay, Accountability (D) Akash, Authentication	0.5	CO1	C1	3
Ans	(c) Akshay, Accountability				
2	If x = remainder obtained by dividing 7^{886} by 300, then evaluate the value of x: - (A) x = 7 (B) x = 49 (C) x = 1 (D) x = 343	0.5	CO3	C3	5
Ans	(B) x=49				
3	For a 7-bit to 7-bit Substitution Block Cipher (Ideal Block Cipher), select how many sets of transformations are possible from Plaintext Blocks to Ciphertext Blocks? (A) 128! (B) 7! (C) 128 (D) None of These	0.5	CO2	C2	5
Ans	(A) 128!				
4	If x = Order of 44 (mod 19), then evaluate the value of x:- (A) x = 9 (B) x = 25 (C) x = 4 (D) x = 1	0.5	CO2	C2	6
Ans	(A) =9				

5	If GCD (651, 168) = 651*x+168*y (x, y ∈ Z), then (x, y)= (A) (4,-1) (B) (-1,4) (C) (-4,1) (D) None of These	0.5	C03	C3	5
Ans	(B) (-1,4)				
6	Which among the following Statements is True? (A) 11 is a primitive root of 18 (B) 49 doesn't have any primitive root (C) 4 is primitive root of 16 (D) 7 is a primitive root of 9	0.5	CO3	C3	1
Ans	(A) 11 is a primitive root of 18				
7	Choose the plaintext corresponding to the ciphertext '**QJDFFOFWRHDQTSPY**' using Vigenere Cipher which uses only alphabets as the character set (by ignoring the case, and mapping with their default numerical equivalents) with the key '**MODULO**' is (A) EVALUATIONSRIGHT (B) EVALUATIONSDONE (C) EVALUATIONMARKS (D) None of These	0.5	CO1	C1	6
Ans	(D)None of These				
8	Select the minimum length of the key required to define all possible 5-bit to 5-bit mappings in an ideal block cipher: (A) 32 Bits (B) 20 Bytes (C) 5! Bits (D) 5! Bytes	0.5	CO3	C3	1
Ans	(B)20 Bytes				
9	Which of the security mechanisms defined by X.800 is sufficient to counter any passive attack? (A) Notarization (B) Authentication Exchange (C) Traffic Padding (D) Digital Signature	0.5	CO1	C1	1
Ans	(C) Traffic Padding				
10	A Plaintext '**HI**' has been encrypted to a Ciphertext '**EE**' with a key '**SOFTWARE**' using	0.5	CO1	C1	6

	Vigenere Cipher (Assume that only alphabets by ignoring the case has been used for encryption). If the attacker captures the Ciphertext and has a knowledge that Vigenere Cipher has been used for encryption, compute the maximum number of keys he/she would have to try for a successful Brute Force Attack. (A) 26^8 (B) 8^{26} (C) 26 (D) 676				
Ans	(D) 676				
11	Explain the following security services defined by X.800 for data storages and data communications:- (a) Data Origin Authentication, (b) Access Control, (c) Non-Repudiation, (d) Peer Entity Authentication	2	CO1	C1	2
Ans	1) (a) Data Origin Authentication:- (Verification of the source of the data, and that it is from a legitimate communicating entity.) **OR** (In a connectionless transfer, provides assurance that the source of received data is as claimed.) **OR** (any similar answer) ***(0.5 Marks)*** (b) Access Control:- (Mechanisms and Policies which are defined to manage and restrict access to resources and data.) **OR** (This service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do.) **OR** (any similar answer) ***(0.5 Marks)*** (c) Non-Repudiation:- (Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.) **OR** (any similar answer) ***(0.5 Marks)*** (d) Peer Entity Authentication:- (Verification of the identities of the communicating entities.) **OR** (Used in association with a logical connection to provide confidence in the identity of the entities connected.) **OR** (any similar answer) ***(0.5 Marks)***				
12	List and explain any 4 design features to be considered in Feistel Cipher	2	CO3	C3	3
Ans	Design Features are Block Size, Key Size, Number of Rounds, Sub Keys generation algorithm, Round Function, Fast software encryption/decryption, and Ease of analysis of analysis.				

	Explain any 4 of these or similar design features ***(0.5 Marks each for mentioning and explaining any 4 features)***				
13	Calculate Multiplicative Inverse of **$(x^4 + 1)$** mod **$(x^5 + x^2 + 1)$** in **GF(2^5)** by applying Extended Euclidean Algorithm (EEA) for Polynomials. (Show Long Division steps for all the iterations while calculating the quotients and remainders)	3	CO2	C2	5
Ans	Iteration 1:- $a(x) = x^5 + x^2 + 1$; $b(x) = x^4 + 1$; $q(x) = x$; $r(x) = x^2 + x + 1$; $v1(x) = 0$; $v2(x) = 1$; $v(x) = x$ ***(0.5 Marks)*** Iteration 2:- $a(x) = x^4 + 1$; $b(x) = x^2 + x + 1$; $q(x) = x^2 + x$; $r(x) = x + 1$; $v1(x) = 1$; $v2(x) = X$; $v(x) = x^2 + x + 1$ ***(0.5 Marks)*** Iteration 3:- $a(x) = x^2 + x + 1$; $b(x) = x + 1$; $q(x) = x$; $r(x) = 1$; $v1(x) = x$; $v2(x) = x^3 + x + 1$; $v(x) = x^4 + x^3$ ***(0.5 Marks)*** Iteration 4:- $a(x) = x + 1$; $b(x) = 1$; $q(x) = x + 1$; $r(x) = 0$; $v1(x) = x^3 + x^2 + 1$; $v2(x) = x^4 + x^3$; $v(x) = (x^5 + x^2 + 1) \bmod (x^5 + x^2 + 1) = 0$ ***(1 Mark)*** Iteration 5:- $a(x) = 1$; $b(x) = 0$; $v1(x) = x^4 + x^3$; $v2(x) = 0$ Therefore, $MI(x^4 + 1) \bmod (x^5 + x^2 + 1) = x^4 + x^3$ ***(0.5 Marks)***				
14	Assume that Feistel Cipher uses 16 rounds. The output of the **14^{th}** Round during Encryption is **0xAB**; **K_{15} = 0xD, K_{16} = 0xE**. The round function **F(x,y) = XOR(1-bit circular left shift of x, 1-bit circular right shift of y)**, where y is the Round Key (K_i). Evaluate the value of Ciphertext (CT).				
ANS	LE14 = 0xA RE14 = 0xB LE15 = RE14 = 0xB ***(0.5 Marks)*** RE15 = LE14 $\oplus$ F(RE14, K15)				

	RE15 = 0xA ⊕ F(0xB, 0xD) ***(0.5 Marks)*** RE15 = 0xA ⊕ (0x7 ⊕ 0xE) RE15 = 0x3 ***(0.5 Marks)*** LE16 = RE15 = 0x3 RE16 = LE15 ⊕ F(RE15, K16) ***(0.5 Marks)*** RE16 = 0xB ⊕ F(RE15, K16) RE16 = 0xB ⊕ (0x6 ⊕ 0x7) RE16 = 0xA ***(0.5 Marks)*** CT = RE16||LE16 = 0xA3 ***(0.5 Marks)***				
16	When x (x ∈N) is divided by **32** and **55**, the remainders obtained are **7** and **14** respectively. Apply Chinese Remainder Theorem (CRT) to write the corresponding Linear Congruence equations and evaluate the value of x.	3	CO3	C3	3
Ans	x ≡ 7 (mod 32) x ≡ 14 (mod 55) a1 = 7, m1 = 32, a2 = 14, m2 = 55; M = m1 * m2 = 1760 M1 = M/m1 = 55 M2 = M/m2 = 32 ***(0.5 Marks)*** N1 = MI(M1) mod m1 calculations with Extended Euclidean Algorithm (EEA) ***(1 Mark)*** N2 = MI(M2) mod m2 calculations with Extended Euclidean Algorithm (EEA) ***(1 Mark)*** x = (a1*M1*N1 + a2*M2*N2) mod M = 839 ***(0.5 Marks)***				
15	Calculate Multiplicative Inverse of **$(x^3 + 1)$** mod **$(x^4 + x + 1)$** in **GF(2^4)** by applying Extended Euclidean Algorithm (EEA) for Polynomials. (Show Long Division steps for all the iterations while calculating the quotients and remainders)	2	CO3	C3	5
Ans	Iteration 1 (With Long division steps for quotient and remainder):-				

	$a(x) = x^4 + x + 1$; $b(x) = x^3 + 1$; $q(x) = x$; $r(x) = 1$; $v1(x) = 0$; $v2(x) = 1$; $v(x) = x$ ***(1 Mark)*** <u>Iteration 2 (With Long division steps for quotient and remainder):-</u> $a(x) = x^3 + 1$; $b(x) = 1$; $q(x) = x^3 + 1$; $r(x) = 0$; $v1(x) = 1$; $v2(x) = x$; $v(x) = 0$; <u>Iteration 3:-</u> $a(x) = 1$; $b(x) = 0$; $v1(x) = x$; $v2(x) = 0$ $MI(x^3 + 1) \bmod (x^4 + x + 1) = x$ ***(1 Mark)***				
16	When x (x ∈N) is divided by **32** and **55**, the remainders obtained are **7** and **14** respectively. Apply Chinese Remainder Theorem (CRT) to write the corresponding Linear Congruence equations and evaluate the value of x.				
Ans	$x \equiv 7 \pmod{32}$ $x \equiv 14 \pmod{55}$ a1 = 7, m1 = 32, a2 = 14, m2 = 55; M = m1 * m2 = 1760 M1 = M/m1 = 55 M2 = M/m2 = 32 ***(0.5 Marks)*** N1 = MI(M1) mod m1 calculations with Extended Euclidean Algorithm (EEA) ***(1 Mark)*** N2 = MI(M2) mod m2 calculations with Extended Euclidean Algorithm (EEA) ***(1 Mark)*** x = (a1*M1*N1 + a2*M2*N2) mod M = 839 ***(0.5 Marks)***				
17	A Plaintext (PT) was encrypted using Triple-Stage Columnar Transposition Cipher with the key '**ENDSEM**'(Using only alphabets by ignoring the case and by using the padding '**X**' if necessary). The Ciphertext (CT) corresponding to the PT is '**TTOTESYIIHUXDRERITXSSMXM**'. Evaluate PT by discarding the padding '**X**' (if any, after final stage decryption).	3	CO3	C3	6
Ans	Key Permutation: 2, 5, 1, 6, 3, 4 First Stage deciphered Text = EITSIDSTTMHRYXOXUEISTMXR ***(1 Mark)***				

	Second Stage Deciphered Text = IUETTYDEIMMXSITXHOTSSRRX ***(1 Mark)*** Third Stage Deciphered Text = THISISYOURMIDTERMTESTXXX Therefore, the PT after discarding the 'X's is 'THISISYOURMIDTERMTEST' ***(1 Mark)***				
18	State and Prove Fermat's Theorem for prime numbers. Apply Fermat's Theorem to calculate the remainder obtained when $\mathbf{48^{783}}$ is divided by **79**.	3	CO3	C3	6
Ans	1) Stating Fermat's theorem:- $a^{p-1} \equiv 1 \pmod p$; where a ∈N, GCD(a,p)=1, and p is a prime. ***(0.5 Marks)*** Proof:- Consider the set of positive integers less than P: {1,2,.....,p-1} and multiply each element by a modulo p, to get the set X = {a mod p, 2*a mod p,.....,(p - 1)*a mod p}. ***(0.5 Marks)*** None of the elements of X is equal to zero because p does not divide a. Furthermore, no two of the integers in X are equal. To see this, assume that $j*a \equiv k*a \pmod p$) ------>>> (1), where $1 \le j < k \le p-1$. Since GCD(a,p) = 1, we can eliminate a from both sides of the equation 1 resulting in $j \equiv k \pmod p$. The last equality $j \equiv k \pmod p$ is impossible, because j and k are both positive integers less than p. ***(0.5 Marks)*** Therefore, we know that the (p- 1) elements of set X are all positive integers with no two elements equal. We can conclude the X consists of the set of integers {1,2,.....,p-1} in some order. ***(0.5 Marks)*** Multiplying the numbers in both sets (P and X) and taking the result mod p yields a * 2*a *.....* (p-1)*a ≡ [(1 * 2 *.....* (p- 1)](mod p) ----------->>>> (2) i.e. $a^{p-1}*(p-1)! \equiv (p-1)! \pmod p$ ------->> (3) Dividing both sides of equation (3) by (p-1)!, we get $a^{p-1} \equiv 1 \pmod p$ ***(0.5 Marks)*** 48^{783} mod 79:- 48^{78} mod 79 = 1 48^{783} mod 79 = [$(48^{78})^{10}$ mod 79) * (48^3 mod 79)] = (1*71) mod 79 = 71 ***(0.5 Marks)***				
19	A Plaintext (PT) was encrypted using Hill Cipher with a Key Matrix (K) as displayed in Figure 1. The	4	CO3	C3	6

	character set consists of only alphabets by ignoring the case (the alphabets are mapped with their default numerical equivalents). The Ciphertext (CT) corresponding to the PT is '**CPSAPOQLNZIU**'. Calculate the Inverse Key Matrix (K^{-1} mod 26). Also, Calculate the Plaintext (PT). $\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$ **Figure 1:- Key Matrix (K) for Hill Cipher**				
Ans	Determinant (K) = 441 Cofactor matrix (K) = $\begin{bmatrix} 70 & 5 & -99 \\ -343 & 70 & 378 \\ 224 & -47 & -216 \end{bmatrix}$ ***(1 Mark)*** Adjoint(K) = $\begin{pmatrix} 70 & -343 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -216 \end{pmatrix}$ ***(0.5 Marks)*** MI(441) mod 26 = 25 calculations with EEA ***(0.5 Marks)*** K^{-1} mod 26 = $\begin{pmatrix} 70 & -343 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -216 \end{pmatrix}$ * 25 (mod 26) = $\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$ ***(0.5 Marks)*** P = C*K^{-1} (mod 26) with right arrangement of ciphertext characters ***(0.5 Marks)*** P = $\begin{bmatrix} 7 & 8 & 11 \\ 11 & 2 & 11 \\ 8 & 12 & 1 \\ 8 & 13 & 6 \end{bmatrix}$ ***(0.5 Marks)***				

	PT = HILLCLIMBING ***(0.5 Marks)***