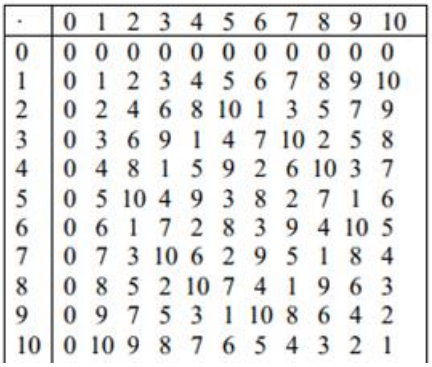
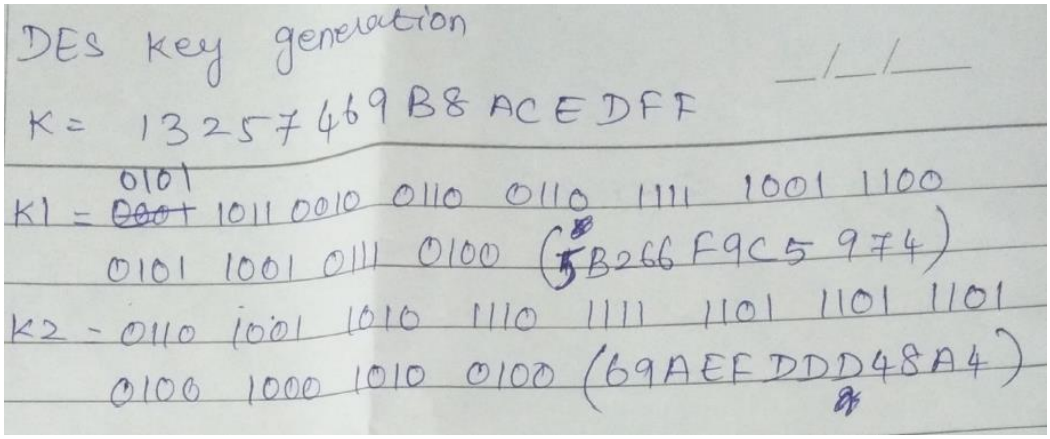
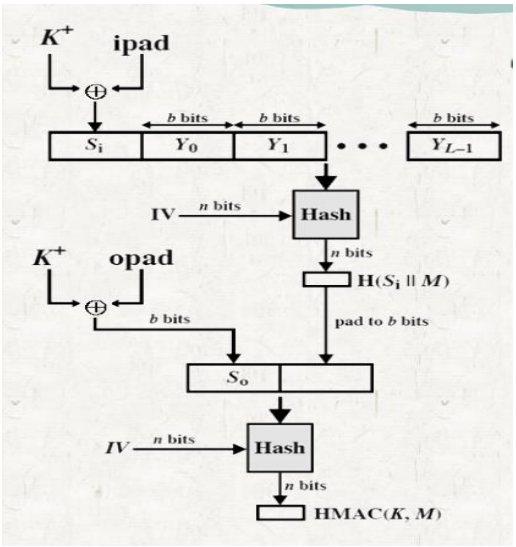
Question Paper Setter Information

Name of Examination	**Final Assessment Test** (FAT), **Fall 2023-24 Semester**		
Slot: C2+TC2			Class number : 3540
Course Code:	CSE4003	Course Title:	Cyber Security

Part	Q. No.	Sub-division	Question Text	Marks
	1.	a)	Consider the group n, where n=11. Determine whether the given group is a multiplicative group. Answer: Since, n=11, group contains 11 elements from 0 to 10. To determine whether given group is a multiplicative group, we have to check whether it satisfies four axioms. (1) closure property (2) associativity (3) identity element (4) inverse element  Satisfies all 4 axioms. By considering values from the group, students must show that all 4 axioms are satisfied. For 4th axiom, inverse element table is given above.	5
		b)	Given two polynomials $f(x) = x^2 + 1$ and $g(x) = x^2 + x + 1$ taken from $GF(2^3)$, perform arithmetic addition and multiplication operations for the irreducible polynomial $m(x) = x^3 + x^2 + 1$. Addition – 2 marks $f(x) + g(x) = x$ Multiplication – 3 marks $f(x) \times g(x) = 1$	5
	2.		A hoard of gold pieces comes into the possession of' a band of 15 pirates. When they come to divide up the coins, they find that three are left over. Their discussion of what to do with these extra coins becomes animated, and by the time some semblance of order returns there remain only 7 pirates capable of making an effective claim on the hoard. When, however, the hoard is divided between these seven it is found that two pieces are left over. There ensues an unfortunate repetition of the earlier disagreement, but this does at least have the consequence that the 4	10

·	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

			pirates who remain are able to divide up the hoard evenly between them. What is the minimum number of gold pieces which could have been in the hoard? Students must apply CRT and computer the result. Answer: X = 408 Step by step computation is required.	
	3.		In DES key generation, let the 64-bit key input 'K' (in hexadecimal) be "13257469B8ACEDFF". Perform necessary computations and generate the 48-bit subkeys K1 (Round-1 subkey) and K2 (Round-2 subkey). Step by step solution is expected. Required tables are given below: **Permuted Choice One (PC-1)** 57 49 41 33 25 17 9 1 58 50 42 34 26 18 10 2 59 51 43 35 27 19 11 3 60 52 44 36 63 55 47 39 31 23 15 7 62 54 46 38 30 22 14 6 61 53 45 37 29 21 13 5 28 20 12 4 **Permuted Choice Two (PC-2)** 14 17 11 24 1 5 3 28 15 6 21 10 23 19 12 4 26 8 16 7 27 20 13 2 41 52 31 37 47 55 30 40 51 45 33 48 44 49 39 56 34 53 46 42 50 36 29 32 **Schedule of Left Shifts** Round Number 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 Bits Rotated 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1 Answer:  	10
	4.		In ECC, consider the elliptic curve $E_{29}(2,3)$. Find the discrete logarithm 'n' for the equation P = n * G where P = (23,23) and G = (16,19). Step by step computation is expected. Answer: n = 4. If n=1, LHS = (23, 23) RHS = (16,19). LHS not equal to RHS If n=2, LHS = (23, 23) RHS = (22,9). LHS not equal to RHS If n=3, LHS = (23, 23) RHS = (26,17). LHS not equal to RHS If n=4, LHS = (23, 23) RHS = (23,23). LHS equal to RHS. So, n=4.	10

	5.		Suppose Alice chooses p = 167, q = 83, a = 8 and g = 5 which is a primitive root. She calculates α and β. Assume that she chooses k = 13 and the hash of message she wants to sign is 39. Compute the signature of the message and do the verification if Alice uses Digital Signature Standard algorithm. Answer: α = 31 β = 54 Sender side, Signature = (31,54) Receiver side, verification is successful. Student has to show all computations with proper steps in both sender and receiver side.	10
	6.		Discuss HMAC algorithm in detail. Exemplify its design objectives. Explaining HMAC algorithm steps with structure diagram – 7 marks Design objectives – 3 marks HMAC  Design objectives: • To use, without modification, available hash functions. In particular, hash functions that perform well in software and code is freely and widely available. • To allow for easy replaceability of the embedded hash function in case faster or more secure hash function are found or required. • To preserve the original performance of the hash function without incurring a significant degradation. • To use and handle key in a simple way. • To have a well understood cryptographic analysis of the strength of the authentication mechanism based on reasonable assumption about the embedded hash function.	10

	7.		Identify and discuss in detail any 5 cybercrimes in which computer is used as a tool to commit criminal activity. From your own perspective, suggest appropriate counter measures for each of those cybercrimes in order to mitigate. Answer: For each cybercrime with counter measure – 2 marks Students can identify and explain any 5 cybercrimes in which computer is used as tool. For each crime, they must suggest counter measures to mitigate. Example: Cyber Stalking, Cyber pornography and so on	10
	8.		Write notes on social engineering. Discuss any 4 types of human-based and computer-based social engineering attacks. Answer: Social engineering – 2 marks Any 4 types of human-based – 4 marks Any 4 types of computer-based – 4 marks	10
	9.		Write brief notes on the following cyber threat/attack. i) Tautology attack ii) Buffer overflow attack iii) Adware iv) Keyboard overlays v) Identity cloning Answer: Each carries 2 marks. Student has to write brief notes on each.	10
	10		Suggest (any 5) internet and email security policies to be followed by the organizations in India. Elucidate and explain the steps for achieving policy enforcement and compliance. Answer: Any 5 internet security policy – 2.5 marks Any 5 email security policy – 2.5 marks Elucidate and explain the steps for enforcement and compliance – 5 marks	10