SVKM's NMIMS
MUKESH PATEL SCHOOL OF TECHNOLOGY MANAGEMENT & ENGINEERING / SCHOOL OF TECHNOLOGY MANAGEMENT & ENGINEERING

Academic Year: 2022-23

Programme: B. Tech (CSBS) Year: IV Semester: VII

Subject: Cryptology

Date: 28 November 2022

Marks: 100
Time: 2.00 pm - 5.00 pm
Durations: 3 (Hrs)
No. of Pages: 02

Final Examination

Instructions: Candidates should read carefully the instructions printed on the question paper and on the cover of the Answer Book, which is provided for their use.

1) Question No. 1 is compulsory.
2) Out of remaining questions, attempt any 4 questions.
3) **In all 5 questions to be attempted.**
4) All questions carry equal marks.
5) **Answer to each new question to be started on a fresh page.**
6) **Figures in brackets on the right hand side indicate full marks.**
7) **Assume Suitable data if necessary.**

Question 1.		Answer briefly:	[20]
CO-1; BL-1 ; SO-1	A.	Describe Euclidean Algorithm. Calculate GCD (1071, 462) using Euclidean Algorithm.	[5]
CO-2; BL-2 ; SO-2	B.	Differentiate between Threat and Attack. Briefly describe types of active attacks.	[5]
CO-3; BL-5 ; SO-2	C.	"Elliptic Curve Cryptography offers significant computational advantages over RSA." Justify the statement.	[5]
CO-4; BL-2 ; SO-2	D.	Write short note on Post-Quantum cryptography.	[5]
Question 2 CO-1; BL-1 ; SO-2	A.	Define Security Services. Explain different security services along with their types.	[10]
CO-4; BL-5 ; SO-1	B.	The matrix G' = SGP = $\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$ is the public generating matrix for a linear [7 4 3] code. Alice encrypt the Message m = [0 1 0 1] using the vector e = [0 0 0 1 0 0 0] by McEliece Cryptosystem. Calculate the encrypted message X. Also decrypt the message given the values of	[10]

		$S^{-1} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$ and $P^{-1} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$.	
Question 3 CO-2; BL-5 ; SO-1	A.	Encrypt the plaintext message "RET" using hill cipher. Use "backupabc" as the key for encryption.	[5]
CO-2; BL-5 ; SO-1	B.	Encrypt the plain text "COMMUNICATION" with Playfair Cipher. Use "COMPUTER" as the key for encryption.	[5]
CO-2; BL-4 ; SO-2	C.	Compare different modes of operations for block ciphers in accordance to their typical applications.	[10]
Question 4 CO2-; BL-4 ; SO-2	A.	Show how hash functions can be used to provide message authentication? Explain with the help of block diagrams.	[10]
CO-3; BL-2 ; SO-6	B.	Describe zero knowledge protocol with application.	[10]
Question 5 CO-2; BL-2 ; SO-2	A.	Draw DES Encryption process. Explain DES transformation functions with suitable diagrams.	[10]
CO-2; BL-5 ; SO-1	B.	What is public Key Cryptography? Bob wants to send the message M = 13 to Alice. RSA is used for encryption and decryption of messages. Using Alice's public and private keys, calculate the ciphertext C, and the value for R when Alice recovers the message. (take P=11 and Q= 3)	[10]
Question 6 CO-2; BL-2 ; SO-2	A.	What is Pseudorandom Number? Describe the requirements for secrecy of Pseudorandom Number Generator output .	[10]
CO-2; BL-6 ; SO-2	B.	Explain the Stream Cipher Design Considerations. Design pseudocode and describe the RC4 encryption algorithm.	[10]
Question 7 CO-3; BL-2 ; SO-6	A.	Describe the security applications in electronic commerce for receiving semi-anonymous cash.	[10]
CO-2; BL-4 ; SO-2	B.	State Digital Signature Properties. Draw and compare the RSA and DSA approach of Digital Signature.	[10]

----------X----------