Roll No											

PRESIDENCY UNIVERSITY
BENGALURU

SET A

SCHOOL OF ENGINEERING
END TERM EXAMINATION - JAN 2024

Semester : Semester V - 2021
Course Code : CSE3078
Course Name : Cryptography and Network Security
Program : B.Tech.

Date : 10-JAN-2024
Time : 9:30AM - 12:30 PM
Max Marks : 100
Weightage : 50%

Instructions:
(i) Read all questions carefully and answer accordingly.
(ii) Question paper consists of 3 parts.
(iii) Scientific and non-programmable calculator are permitted.
(iv) Do not write any information on the question paper other than Roll Number.

PART A

ANSWER ALL THE QUESTIONS **4 X 5M = 20M**

1. As part of their final project in a course on Cryptography, a group of students is tasked with demonstrating the use of the Rail Fence Cipher. They are given a specific plaintext message "CRYPTOGRAPHY IS FUN" and instructed to encrypt it using the Rail Fence Cipher with 3 rails. (CO 1, Undestand)

1. Encrypt the given plaintext using the Rail Fence Cipher with the specified number of rails. Clearly show how you arrange the text and how you derive the ciphertext.
2. Write down the resulting ciphertext.

(CO1) [Knowledge]

2. You are working as a cybersecurity analyst at a security firm. Your team has intercepted a message that was encrypted using the Data Encryption Standard (DES). To analyze this message, you need to understand the workings of the DES algorithm, particularly the role of the S-boxes in the encryption process. One of the intercepted segments of the encrypted message corresponds to the input for S-box 4 in the DES algorithm. Your task is to decipher this part of the message. During the analysis, you find that the input for S-box 4 is '101011'. Explain the role of S-boxes in the DES algorithm. How do they contribute to the security of the encryption? Given the input '101011' for S-box 4 in the DES algorithm, determine the output.
(CO 3, Apply)

S[4]

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

(CO2) [Knowledge]

3. Kaul and Sanjay want to securely exchange messages using a shift cipher, and they decide to employ the Diffie-Hellman key exchange method for secure key generation. They agree on using the prime number q=11 for their cyclic group $Z11^*$, and the generator α=7. In this scenario, Kaul chooses the secret value a=6, while Sanjay selects the secret value b=9. Apply the Diffie-Hellman key exchange algorithm to compute the intermediate values and the final shared secret key between Kaul and Sanjay based on their chosen secret values. (CO 3, Apply)

(CO3) [Knowledge]

4. As a cybersecurity consultant for FinSecure, explain the role and function of each component in a Public Key Infrastructure system. Describe how PKI will facilitate secure communication between the company and its clients. Specifically, focus on how the Certificate Authority, Registration Authority, Certificate Database, and Certificate Store contribute to the overall security and integrity of digital transactions.Consider the importance of both public and private keys in this process. Conclude your explanation by outlining the benefits and challenges FinSecure might face when implementing and managing a PKI system

(CO 4, Understand)

(CO4) [Knowledge]

PART B

ANSWER ALL THE QUESTIONS **5 X 10M = 50M**

5. a. You are an aspiring cryptanalyst working with a team of historians who have recently discovered a series of old manuscripts. One of the documents contains a message that appears to be encrypted using the Playfair Cipher. The historians are eager to understand the content of this message, believing it could provide valuable insights into historical events. The cipher text provided in the document is "KBSIEQKEZMBCIEPZ". It's known that the person who wrote this message used the phrase "HISTORICAL FINDS" as the key for the Playfair Cipher. For spaces and letters that required a filler, the letter 'X' was used.

(CO 1, Apply)

1. Create the 5x5 Polybius square matrix utilized in the Playfair Cipher.
2. Decrypt the cipher text "KBSIEQKEZMBCIEPZ" to reveal the plaintext message.
3. Present your solution in a tabular format, showing each cipher text digraph alongside its corresponding plaintext digraph.

b. As part of a cybersecurity project, you, a final-year B.Tech student, are tasked with demonstrating the encryption process using the Hill cipher. Your project supervisor has provided you with a plaintext message " DCDF" that needs to be encrypted and a specific key matrix “TEXT”.

(CO 1, Understand)

1. Assume that the alphabet A-Z is represented by numbers 0-25 (e., A=0, B=1, ..., Z=25).
2. If necessary, use 'X' (23) as padding at the end of the plaintext to make it a multiple of the key matrix's size.
3. Prepare the plaintext for encryption, including any necessary steps such as padding. Explain your process.
4. Perform the encryption using the Hill cipher and the given key matrix. Show all steps of your calculation.

(CO1) [Comprehension]

6. a. As the chief cryptography engineer at SecureCom Inc., you are tasked with developing a cutting-edge block cipher for the company's new secure communication platform. Your design is based on the Feistel network structure, renowned for its balance of security and efficiency. (CO 2, Understand)

1. Prepare an insightful presentation for your team, highlighting the foundational principles of block cipher design. Focus on explaining the concepts of confusion, diffusion, and the avalanche effect, and how these principles contribute to the security of the cipher.
2. Develop a comprehensive tutorial for the software development team, detailing the encryption and decryption processes in a Feistel cipher. Use clear, step-by-step instructions and include diagrams to illustrate the flow of data and transformations within the Feistel structure.

b. You are a computer security analyst working on an encryption project using the Data Encryption Standard (DES). As part of your project, you need to demonstrate a clear understanding of the DES algorithm's functioning by providing a detailed walkthrough of the initial stages of the encryption process. (CO 2, Apply)
Given Data:
Plaintext (M) in hexadecimal format: 0123456789ABCDEF
K_1 = 000110 110000 001011 101111 111111 000111 000001 110010

1. Convert the hexadecimal plaintext M into its binary equivalent. Explain the conversion process.
2. Describe the process of initial permutation (IP) on the binary form of M and state the resulting L_0 and R_0.
3. Explain how the round 1 key (K_1) is used in the first round of the DES encryption process.
4. Describe the expansion function applied to R0 to obtain $E(R_0)$ and expand R_0.
5. Demonstrate the operation between K_1 and $E(R_0)$

IP Table

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(CO2) [Comprehension]

7. a. ABC Bank, a prominent financial institution, is in the process of modernizing its operations and aims to enhance the security of online transactions. As a cybersecurity expert, you have been consulted to implement a robust digital signature system. (CO 3, Understand)

1. Explain the process of implementing a digital signature system for securing online transactions at ABC Bank to ensure data integrity, non-repudiation, and authentication
2. Outline the key components of a digital signature infrastructure, including the generation of public and private keys, certificate authorities, and the role of hashing algorithms.

b. XYZ Corporation, a multinational company, is concerned about the rising threat of cyberattacks, particularly Man-in-the-Middle attacks, compromising sensitive business communications. As a cybersecurity expert, you have been hired to assess and mitigate the risks associated with MitM attacks. (CO 3, Understand)

1. Identify specific scenarios where MitM attacks could occur, such as during email exchanges, remote access sessions, or financial transactions.
2. Explain the methods that attackers might employ to execute successful MitM attacks in these scenarios.

(CO3) [Comprehension]

8. a. You are working on an encryption algorithm that requires generating large prime numbers and solving complex modular equations. (CO 3, Apply)

1. Use Fermat's Little Theorem to check if the number 29 is prime, taking a=6 as a base. Explain the theorem and your method.
2. Solve the following system of linear congruences using the Chinese Remainder Theorem: $x \equiv 3 \pmod 4$, $x \equiv 5 \pmod 6$, and $x \equiv 7 \pmod 9$. Detail each step of your methodology.

(CO4) [Comprehension]

9. You are a junior mathematician working in a software development company that specializes in cryptographic algorithms. Your team is currently working on designing a new encryption system that will use the mathematical structures of groups, rings, and fields. You have been asked to provide a detailed explanation of these structures to help your team understand how they can be applied in cryptography. (CO 3, Apply)

1. Explain what a group is in the context of abstract algebra. Provide an example of a group that might be used in cryptography, explaining its operations and the properties that make it a group (Closure, Associativity, Identity, and Inverse).
2. Describe the concept of a ring in mathematics. Illustrate with an example relevant to cryptographic systems. Explain the additional structures a ring has compared to a group and how these can be leveraged in cryptographic algorithms.
3. Define a field in abstract algebra and provide an example that is typically used in cryptography. Discuss how the properties of a field (such as the existence of additive and multiplicative inverses for every element) are advantageous in developing cryptographic algorithms.

(CO2,CO3) [Comprehension]

PART C

ANSWER ALL THE QUESTIONS **2 X 15M = 30M**

10. a. You are a junior cryptographer working on a project that involves encrypting sensitive information. Your team has decided to use the Vigenère cipher for one of the encryption tasks. The word "CRYPTOGRAPHY" needs to be encrypted using the keyword “LUCKY”. Encrypt the word "cryptography" with the Vigenère cipher. Show each step of your working. (CO 1, Understand)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

b. As part of an Advanced Encryption Standard (AES) encryption process, the Mix Columns transformation is employed to enhance the security of the data. Consider a scenario where the sequence of bytes "09 AD 0E 0B" is subjected to the Mix Columns transformation in an AES encryption. Your task is to demonstrate the transformation and identify the byte at position r0,1 in the resulting column. (CO 3, Apply)

1. Perform the Mix Columns transformation on the original state matrix represented by the bytes "09 AD 0E 0B" and show the resulting column matrix.
2. State the value at position r0,1 in the transformed column after applying the Mix Columns transformation to the given sequence of bytes.

Current State		**RConstant**					**New State**
09		**02**	**03**	**01**	**01**		
AD		**01**	**02**	**03**	**01**		
0E		**01**	**01**	**02**	**03**	=	
0B		**03**	**01**	**01**	**02**		

(CO2,CO1) [Application]

11. You are a cybersecurity analyst participating in a controlled exercise designed to test the strength of cryptographic systems. Your task is to crack an RSA encrypted message as part of the drill. The RSA system under test encrypted a secret message *M* into the ciphertext C=65. The public key used in this encryption is given by *n*=221 and *e*=47. (CO 3, Apply)

1. What are the key parameters that comprise the public key in the RSA encryption system? Explain the role of each component and identify the components that form the private key in the RSA system.
2. Outline the steps necessary to derive the private key from the given public key parameters in the RSA system. Perform these steps to compute the private key components needed for decryption.
3. Apply the RSA decryption algorithm using the derived private key to decrypt the given ciphertext C=65 and retrieve the original message M

b. As a cybersecurity consultant for FinSecure, explain the role and function of each component in a Public Key Infrastructure system. (CO 4, Understand)

1. Describe how PKI will facilitate secure communication between the company and its clients. Specifically, focus on how the Certificate Authority, Registration Authority, Certificate Database, and Certificate Store contribute to the overall security and integrity of digital transactions. Consider the importance of both public and private keys in this process.
2. Conclude your explanation by outlining the benefits and challenges FinSecure might face when implementing and managing a PKI system

(CO4,CO3) [Application]