H1 **1100CST393122102** **Pages: 2**

Reg No.:_______________ Name:_______________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Fifth Semester B.Tech (Hons.) Degree Examination December 2022 (2020 Admn.)

Course Code: CST 393

Course Name: CRYPTOGRAPHIC ALGORITHMS

Max. Marks: 100 Duration: 3 Hours

PART A

(Answer all questions; each question carries 3 marks) Marks

1 Comment on Passive and active attacks on the encryption schemes. 3

2 Write the rules of play fair ciphering technique. 3

3 Explain the generation of round keys in DES. 3

4 Brief the construction of S-box. 3

5 Mention the three uses of an encryption scheme. 3

6 Define one-way function and trap-door one way function. 3

7 State a method to identify the errors that may happen during transmission of key values. 3

8 If the key values are compromised, what are the steps to be taken by Alice to prevent further issues? 3

9 Define message digest. 3

10 Draw a neat a sketch of using MAC for authentication. 3

PART B

(Answer one full question from each module, each question carries 14 marks)

Module -1

11 a) Draw the basic model of network security and explain each term. 10

b) Compare stream cipher and block cipher with example. 4

OR

12 a) Encrypt the text "***I only regret that I have but one life to give for my country***" using transposition cipher with the key (3,2,1,4,5). Show decryption of the ciphertext to recover the original text back. 6

b) Encrypt the message "***the house is being sold tonight***" using the following ciphers. Ignore the space between words. 8

i. Vigenere cipher with key = "***largest***".
ii. Autokey system of Vigenere cipher with key = "***largest***".

		Module -2	
13	a)	Explain the encryption and decryption of triple DES using 2 keys and 3 keys.	5
		Summarize the primitive operations in RC4 algorithm.	9
		OR	
14	a)	Illustrate Linear and differential cryptanalysis.	10
	b)	Sketch the diagram for Fiestel structure.	4
		Module -3	
15	a)	Discuss Elliptic curve cryptography.	10
	b)	Write the equation for the addition of two points on the elliptic curve.	4
		OR	
16	a)	Explain Diffie Hellman Key Exchange. User A and B use the Diffie-Hellman key exchange technique with a common prime q=17 and primitive root α =7. If user A has private key X_A=3, and user B has private key X_B = 6, what is the secret key shared?	8
	b)	How does a man-in-the-middle attack happen to DH key exchange?	6
		Module -4	
17	a)	Explain the different PKIX management protocols.	6
	b)	Explain the concept of symmetric key distribution using asymmetric keys.	8
		OR	
18		With neat diagram, explain Public Key Infrastructure (PKI).	14
		Module -5	
19	a)	Illustrate Message Authentication Code (MAC) and HMAC.	8
	b)	Specify the format for X.509 certificate. Explain the steps required to obtain user's certificate.	6
		OR	
20		Explain SHA-512 algorithm.	14

***