U.S.N.										

B.M.S. College of Engineering, Bengaluru-560019

Autonomous Institute Affiliated to VTU

September / October 2023 Supplementary Examinations

Programme: B.E. **Semester: V**
Branch: Electronics and Telecommunication Engineering **Duration: 3 hrs.**
Course Code: 19ET5PE1CY **Max Marks: 100**
Course: CRYPTOGRAPHY **Date: 20.09.2023**

Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may suitably assumed.

UNIT - I

1	a)	With diagram explain network security model		**06**
	b)	Encrypt the plaintext "white space characteristic" using Hill cipher with the key $\begin{pmatrix} 17 & 18 & 18 \\ 10 & 15 & 17 \\ 12 & 8 & 3 \end{pmatrix}$		**08**
	c)	Using Rail fence technique with depth of 6 generate cipher text for the following plain text "project demonstrated basic knowledge on c"		**06**

OR

2	a)	Using play fair method, key= PROJECT, Decrypt: "OZDPHZUDWGRORHOPQYQIKYPOZPAZ"		**06**
	b)	Using rotation cipher, Encrypt the following plain text, use K= 8 "If he had anything confidential to say, write it in cipher"		**04**
	c)	Explain active attacks and passive attacks		**06**
	d)	Use double transposition to Decrypt the cipher text "PUAAPSTTACNWKPNTTEDMTOOLTOAOST " with block size 6 and the decryption key being 521364		**04**

UNIT - II

3	a)	Explain and derive an expression for Fermat's theorem		**06**
	b)	In S-DES Obtain the plain text for the given 8 bit cipher text (0 0 0 1 1 1 0 1) ,consider following data, 10 bit key (1 0 1 0 0 0 1 0 1 0) generate plain text, Consider IP= (2,6,3,1,4,8,5,7) , E/P =(4,1,2,3,2,3,4,1), P4 = (2,4,3,1) and IP^{-1} = (4,1,3,5,7,2,8,6).		**08**

S0= $\begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix}$ S1= $\begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$

c) Solve $Z \equiv 4 \pmod{29}$ $Z \equiv 7 \pmod{30}$ $Z \equiv 8 \pmod{31}$ using CRT **06**

UNIT - III

4 a) Explain with diagram single round in AES **08**

b) With diagram explain triple DES with two keys **06**

c) With diagram explain cipher feedback **06**

UNIT - IV

5 a) Perform encryption and decryption using RSA algorithm for the following data; p=17, q=7, e=17, C = 37 **08**

b) Explain Diffie- Hellman key exchange and prove the obtained key are equal **06**

c) Explain with diagram internal and external error control in message authentication **06**

OR

6 a) Consider a Diffie – Hellman scheme with a common prime q = 191 and primitive root α =13. If user A has private key X_A=36 and user B has private key X_B =58, compute the secret key of user A & user B **08**

b) Explain and derive an expression for RSA algorithm **06**

c) Derive an expression for message authentication, confidentiality, where authentication is tied to plain text and cipher text with diagram **06**

UNIT - V

7 a) With relevant equation derive an expression for linear congruential generator **05**

b) With relevant equation derive an expression for Blum Blum Shub generator **05**

c) With relevant diagram explain ANSI X9.17 Pseudorandom Number Generator **05**

d) Explain PRNG requirements **05**

******