U.S.N.										

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

Autonomous Institute Affiliated to VTU

January / February 2025 Semester End Main Examinations

Programme: B.E. **Semester: V**

Branch: Electronics & Telecommunication Engineering **Duration: 3 hrs.**

Course Code: 23ET5PECPY **Max Marks: 100**

Course: CRYPTOGRAPHY

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

Important Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

			UNIT - I	CO	PO	Marks
1	a)		Explain different types of security attacks with relevant diagrams.	CO1	-	**06**
	b)		Encrypt the plaintext **PAYMOREMONEY** using Hill cipher with the key $\begin{pmatrix} 17 & 7 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$	CO2	PO1	**06**
	c)		Use double transposition cipher to encrypt and decrypt the text "**attack postponed until pm meeting**" with the encryption key **5 2 1 3 6 4 7**	CO2	PO1	**08**
			OR			
2	a)		Using the Playfair matrix given below, Encrypt the message: **I only regret that I have but one life to give for my country**	CO2	PO1	**08**
	b)		Alice meets Bob and says **yqqf yq pgduzs iadwuzs tagd. iq iuxx pueogee ftq bxmz**. If she is using a key of **12**, what does she want to convey?	CO2	PO1	**06**
	c)		Analyze the network security model.	CO1	-	**06**
			UNIT - II			
3	a)		Derive the CRT theorem.	CO2	PO1	**06**

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

		b)	In S-DES Obtain the cipher text for the given 8 bit plain text **(1 0 1 0 0 1 0 1)** , K_1 **= 10100100** and K_2**= 01000011** to generate cipher 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)**. S0= $\begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix}$ S1= $\begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$	*CO3*	*PO2*	**08**
		c)	Using Fermat's theorem, find 4^{225} **mod 13**	*CO3*	*PO2*	**06**
			OR			
	4	a)	Derive expression for Fermat's theorem.	*CO2*	*PO1*	**06**
		b)	Solve using CRT, the following : **x ≡ 4 (mod 10)** **x ≡ 6 (mod 13)** **x ≡ 4 (mod 7)** **x ≡ 2 (mod 11)**	*CO3*	*PO2*	**07**
		c)	Explain with diagram single round DES.	*CO1*	-	**07**
			UNIT - III			
	5	a)	Analyze the concept of AES Single round.	*CO1*	-	**08**
		b)	With relevant expression and diagram explain Triple DES with Two keys.	*CO1*	-	**06**
		c)	Explain Counter (CTR) mode and its advantages.	*CO1*	-	**06**
			OR			
	6	a)	Explain substitute bytes transformation, shift rows transformation, mix column in AES.	*CO1*	-	**08**
		b)	With an appropriate diagram, explain the structure of AES.	*CO1*	-	**06**
		c)	With diagram explain CFB operations with relevant equations and its advantages.	*CO1*	-	**06**
			UNIT - IV			
	7	a)	Perform encryption and decryption using RSA algorithm for the following data; **p=17, q=23, e=17, M=75**	*CO2*	*PO1*	**08**
		b)	With a diagram explain general structure of secure hash code.	*CO1*	-	**06**
		c)	Analyze with relevant diagram the Man in the middle attack.	*CO2*	*PO1*	**06**
			OR			
	8	a)	User A and User B use the Diffie-Hellman key exchange technique. A common prime **q = 467** and a primitive root **α = 2**. i. If user A has a private key X_A **= 228**, what is A's public key Y_A?	*CO3*	*PO2*	**08**

			ii. If user B has a private key $\mathbf{X_B = 57}$, what is B's public key Y_B? What is the shared secret key?			
		b)	Analyze the concept of MAC with respect to authentication tied to plaintext and ciphertext.	*CO1*	-	**06**
		c)	Analyze the following with respect to Message Encryption: i. Internal and External Error control ii. Public key encryption	*CO1*	-	**06**
			UNIT - V			
	9	a)	Analyze the concept of RC4.	*CO2*	*PO1*	**10**
		b)	With relevant equation and example, explain linear congruential generator.	*CO2*	*PO1*	**10**
			OR			
	10	a)	Analyze the concept of Blum Blum Shub Generator.	*CO2*	*PO1*	**10**
		b)	With diagram explain PRNG and TRNG requirements.	*CO1*	-	**10**

****