U.S.N.										

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

Autonomous Institute Affiliated to VTU

June / July 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.

			UNIT - I	CO	PO	Marks
1	a)		Explain active and passive attacks in cryptography.	CO1	-	**07**
	b)		Encrypt the plaintext "do not wait for" using Hill cipher with the key . $\begin{pmatrix} 7 & 4 \\ 17 & 3 \end{pmatrix}$	CO2	PO1	**07**
	c)		Using rail fence method, key= 4, Encrypt: namma Bengaluru is silicon valley of India.	CO2	PO1	**06**
			OR			
2	a)		With diagram explain network access security model.	CO1	-	**06**
	b)		Using play fair method, decrypt UGRMKCSXHMUFMKBTOXGCMVATLUIV using the key = MONARCHY.	CO2	PO1	**06**
	c)		Use double transposition cipher to encrypt and decrypt the text "attack post postponed until pm meeting " with the encryption key being 5213647	CO2	PO1	**08**
			UNIT - II			
3	a)		Explain S-DES key generation with diagram.	CO1	-	**06**
	b)		Derive an expression for Fermat's theorem.	CO2	PO1	**07**
	c)		Solve using CRT $X\equiv6(\text{mod } 7), X\equiv4(\text{mod } 8), X\equiv3(\text{mod } 5)$.	CO3	PO2	**07**
			OR			
4	a)		Explain the details of single round in DES with diagram.	CO1	-	**07**
	b)		In S-DES Obtain the cipher text for the given 8 bit plain text	CO3	PO2	**07**

			(1 0 1 0 0 1 1 1) ,consider following data, 10 bit key (1 0 1 0 1 0 0 0 1 1), IP= (2,6,3,1,4,8,5,7) , E/P =(4,1,2,3,2,3,4,1), P4 = (2,4,3,1) , IP^{-1} = (4,1,3,5,7,2,8,6), P10 = (3 5 2 7 4 10 1 9 8 6) and P8 = (6 3 7 4 8 5 10 9) 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)	Explain stream cipher using diagram.	*CO1*	-	**06**
			UNIT - III			
	5	a)	With diagram explain Counter mode operations and its advantages.	*CO1*	-	**08**
		b)	With diagram explain general structure of AES.	*CO1*	-	**06**
		c)	With diagram explain triple DES with two keys.	*CO1*	-	**06**
			OR			
	6	a)	With diagram explain single round AES.	*CO1*	-	**07**
		b)	Explain mix column transformation and add round key transformation in AES.	*CO1*	-	**07**
		c)	Explain Electronic code book with diagram.	*CO1*	-	**06**
			UNIT - IV			
	7	a)	Consider a Diffie – Hellman scheme with a common prime q = 192 and primitive root α = 7. If user A has private key X_A=11 and user B has private key X_B =13, compute the secret key of user A & user B.	*CO3*	*PO2*	**08**
		b)	Explain expression for message authentication, confidentiality, where authentication is tied to cipher text with diagram.	*CO1*	-	**06**
		c)	Explain MAC with diagram.	*CO1*	-	**06**
			OR			
	8	a)	Perform encryption and decryption using RSA algorithm for the following P=7, q = 11, e=17, and M=8.	*CO3*	*PO2*	**07**
		b)	Explain and derive and expression for man in middle attack in Diffie – Hellman key exchange.	*CO2*	*PO1*	**07**
		c)	With diagram explain public key cryptosystem for secrecy and authentication.	*CO1*	-	**06**
			UNIT - V			
	9	a)	With diagram explain PRNG and PRF.	*CO1*	-	**06**
		b)	With relevant equation and derive an expression for Blum Blum Shub generator.	*CO1*	-	**06**

		c)	Derive an expression for Linear Congruential Generator and generate sequence of random number for following data , a = 9, c = 0, m = 64 and X_o=1	*CO2*	*PO1*	**08**
			OR			
	10	a)	What are the requirement of PRNG?	*CO1*	-	**06**
		b)	With diagram explain PRNG using OFB.	*CO1*	-	**06**
		c)	With relevant diagram explain RC4 stream cipher.	*CO1*	-	**08**

****