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: 19ET5PE1CY **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.

<table>
<tr><th></th><th></th><th>UNIT - I</th><th><i>CO</i></th><th><i>PO</i></th><th>Marks</th></tr>
<tr><td>1</td><td>a)</td><td>Explain different types of security attacks with relevant diagrams</td><td><i>CO1</i></td><td></td><td>06</td></tr>
<tr><td></td><td>b)</td><td>Encrypt the plaintext <b>FRIDAY</b> using Hill Cipher with the key $\begin{bmatrix}7 &amp; 8\\19 &amp; 3\end{bmatrix}$
Show the appropriate calculations and thereby deduce the ciphertext.</td><td><i>CO2</i></td><td><i>PO1</i></td><td>06</td></tr>
<tr><td></td><td>c)</td><td>Use double transposition cipher to encrypt and decrypt the text “<b>attack postponed until pm meeting</b> ” with the encryption key <b>5 2 1 3 6 4 7</b></td><td><i>CO2</i></td><td><i>PO1</i></td><td>08</td></tr>
<tr><td></td><td></td><td>OR</td><td></td><td></td><td></td></tr>
<tr><td>2</td><td>a)</td><td>Using the Playfair matrix given below, Encrypt the message:
<b>I only regret that I have but one life to give for my country</b>
<table>
<tr><td>J/K</td><td>C</td><td>D</td><td>E</td><td>F</td></tr>
<tr><td>U</td><td>N</td><td>P</td><td>Q</td><td>S</td></tr>
<tr><td>Z</td><td>V</td><td>W</td><td>X</td><td>Y</td></tr>
<tr><td>R</td><td>A</td><td>L</td><td>G</td><td>O</td></tr>
<tr><td>B</td><td>I</td><td>T</td><td>H</td><td>M</td></tr>
</table></td><td><i>CO2</i></td><td><i>PO1</i></td><td>08</td></tr>
<tr><td></td><td>b)</td><td>Alice meets Bob and says <b>yqqf yq pgduzs iadwuzs tagd. iq iuxx pueogee ftq bxmz</b>. If she is using a key of <b>12</b>, what does she want to convey.</td><td><i>CO2</i></td><td><i>PO1</i></td><td>06</td></tr>
<tr><td></td><td>c)</td><td>Analyze the network security model.</td><td><i>CO1</i></td><td></td><td>06</td></tr>
</table>

			UNIT - II			
	3	a)	Solve using CRT **x ≡ 4 (mod 10)** **x ≡ 6 (mod 13)** **x ≡ 4 (mod 7)** **x ≡ 2 (mod 11)**	*CO2*	*PO1*	**06**
		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$^{\sim1}$ = (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*	*PO1*	**08**
		c)	Using Fermat's theorem, find **4^{225} mod 13**	*CO2*	*PO1*	**06**
			OR			
	4	a)	Derive expression for Fermat's theorem.	*CO1*		**06**
		b)	Explain with diagram single round DES	*CO1*		**08**
		c)	Derive expression for CRT.	*CO1*		**06**
			UNIT - III			
	5	a)	Explain substitute bytes transformation, shift rows transformation, mix column in AES	*CO1*		**10**
		b)	With diagram explain CFB operations with relevant equations and its advantages	*CO1*		**10**
			OR			
	6	a)	Analyze the concept of AES Single round	*CO1*		**12**
		b)	Explain Counter (CTR) mode and its advantages	*CO1*		**08**
			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*	**12**
		b)	With diagram explain different approach of Message authentication in cryptographic hash functions	*CO1*		**08**
			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$_A$?	*CO2*	*PO1*	**12**

			ii. If user B has a private key **X_B = 57**, what is B’s public key Y_B? What is the shared secret key?			
		b)	Derive an expression for man in middle attack with diagram	*CO2*	*PO1*	**08**
			UNIT - V			
	9	a)	Analyze the concept of RC4.	*CO1*		**10**
		b)	Analyze the various PRNG requirements.	*CO1*		**10**
			OR			
	10	a)	Analyze the concept of Blum Blum Shub Generator	*CO1*		**10**
		b)	With relevant equation and example, explain linear congruential generator	*CO1*		**10**

******