U.S.N.										

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

Autonomous Institute Affiliated to VTU

September / October 2024 Supplementary Examinations

Programme	**: B.E.**		**Semester: V**
Branch	**: Computer Science and Engineering**		**Duration: 3 hrs.**
Course Code:	**22CS5PCCRP**		**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.

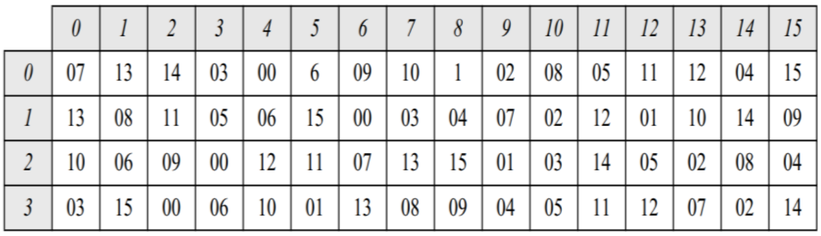
Important Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

		UNIT - I	***CO***	***PO***	**Marks**
1	a)	Demonstrate the encryption and decryption process in multiplicative cipher with an example.	CO1	PO1	**06**
	b)	Given a group G = <Z_{10}*, x >, find all the cyclic subgroups that can be made. Analyze if Z_{10}* a cyclic group. Justify your answer.	CO2	PO2	**06**
	c)	i. Use brute-force attack to decipher the following message. Assume that you know it is an affine cipher and that the plaintext “ab” is enciphered to “GL”. Ciphertext=>XPALASXYFGFUKPXUSOGEUTKCDGFXAN MGNVS ii. Analyze the given key below. Use Playfair cipher to encrypt the text “Cryptanalysis is to break ciphers” using this key.	CO2	PO2	**08**

	1	**2**	**3**	**4**	**5**
1	z	q	p	f	e
2	y	r	o	g	d
3	x	s	n	h	c
4	w	t	m	i / j	b
5	v	u	l	k	a

		OR			
2	a)	Explain Double Transposition Cipher with a figure.	CO1	PO1	**06**
	b)	Find the result of multiplying P1 = 000100110 with P2 = 1001111 using the modulus = 100011010 (nine bits). Analyze and find the number of shift-left operations and exclusive-or operations involved in multiplying P1 and P2.	CO2	PO2	**06**
	c)	i. Eve secretly gets access to Alice’s computer and using her cipher types “abcdefghij”. The screen shows “CABDEHFGIJ”. If	CO2	PO2	**08**

<table>
<tr><td></td><td></td><td></td><td>Eve knows that Alice is using a keyed transposition cipher, answer the following questions:
I. Analyze the type of attack Eve is launching
II. Analyze the size of the permutation key

ii. Consider the plaintext = "Cryptography and Network Security" (ignore spaces) and the encryption key (3, 2, 6, 1, 5, 4). Analyze and find the decryption key</td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td><b>UNIT - II</b></td><td></td><td></td><td></td></tr>
<tr><td></td><td>3</td><td>a)</td><td>Draw and explain MixColumns transformation in AES with an example</td><td>CO1</td><td>PO1</td><td><b>06</b></td></tr>
<tr><td></td><td></td><td>b)</td><td>Write the fifth design criterion of DES and analyze the same for given S-box using the following pairs of inputs.
a. 001100 and 110000
b. 110011 and 001111

<table>
<tr><th></th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th></tr>
<tr><td>0</td><td>07</td><td>13</td><td>14</td><td>03</td><td>00</td><td>6</td><td>09</td><td>10</td><td>1</td><td>02</td><td>08</td><td>05</td><td>11</td><td>12</td><td>04</td><td>15</td></tr>
<tr><td>1</td><td>13</td><td>08</td><td>11</td><td>05</td><td>06</td><td>15</td><td>00</td><td>03</td><td>04</td><td>07</td><td>02</td><td>12</td><td>01</td><td>10</td><td>14</td><td>09</td></tr>
<tr><td>2</td><td>10</td><td>06</td><td>09</td><td>00</td><td>12</td><td>11</td><td>07</td><td>13</td><td>15</td><td>01</td><td>03</td><td>14</td><td>05</td><td>02</td><td>08</td><td>04</td></tr>
<tr><td>3</td><td>03</td><td>15</td><td>00</td><td>06</td><td>10</td><td>01</td><td>13</td><td>08</td><td>09</td><td>04</td><td>05</td><td>11</td><td>12</td><td>07</td><td>02</td><td>14</td></tr>
</table></td><td>CO2</td><td>PO2</td><td><b>06</b></td></tr>
<tr><td></td><td></td><td>c)</td><td>Analyze how double DES is vulnerable to Meet-in-the-middle attack. Also prove that double DES improves this vulnerability slightly (to 2^{57} tests), but not tremendously (to 2^{112}). Include appropriate figures.</td><td>CO2</td><td>PO2</td><td><b>08</b></td></tr>
<tr><td></td><td></td><td></td><td><b>UNIT - III</b></td><td></td><td></td><td></td></tr>
<tr><td></td><td>4</td><td>a)</td><td>Using quadratic residues, solve the following congruences:
i) $x^2 \equiv 4 \bmod 7$
ii) $x^2 \equiv 5 \bmod 11$</td><td>CO1</td><td>PO1</td><td><b>06</b></td></tr>
<tr><td></td><td></td><td>b)</td><td>Apply Miller-Rabin test & check it 891 is prime or not.</td><td>CO1</td><td>PO1</td><td><b>06</b></td></tr>
<tr><td></td><td></td><td>c)</td><td>Find the value of x for the following set of congruence using CRT:
(a) $x \equiv 2 \bmod 7$ and $x \equiv 3 \bmod 9$
(b) $x \equiv 4 \bmod 5$ and $x \equiv 10 \bmod 11$</td><td>CO1</td><td>PO1</td><td><b>08</b></td></tr>
<tr><td></td><td></td><td></td><td><b>UNIT - IV</b></td><td></td><td></td><td></td></tr>
<tr><td></td><td>5</td><td>a)</td><td>Explain the compression function in SHA-512.</td><td>CO1</td><td>PO1</td><td><b>06</b></td></tr>
<tr><td></td><td></td><td>b)</td><td>Briefly analyse the idea behind the Elgamal cryptosystem.
i) What is the one-way function in this system?
b) What is the trapdoor in this system?
c) Define the public and private keys in this system.
d) Describe the security of this system.</td><td>CO1</td><td>PO1</td><td><b>06</b></td></tr>
<tr><td></td><td></td><td>c)</td><td>Alice uses Bob’s RSA public key (e = 7, n = 143) to send the plaintext P = 8 encrypted as ciphertext C = 57. Show how Eve can</td><td>CO2</td><td>PO2</td><td><b>08</b></td></tr>
</table>

			use the chosen-ciphertext attack if she has access to Bob’s computer to find the plaintext			
			OR			
	6	a)	Write briefly about Elliptic Curve Cryptosystem. Draw a figure that has one real root and two imaginary ones.	CO1	PO1	**06**
		b)	Analyze how the three schemes Davies-Meyer Scheme, Matyas-Meyer-Oseas Scheme and Miyaguchi-Preneel Scheme are related and the explain their functionalities	CO2	PO2	**06**
		c)	In ElGamal cryptosystem, given the prime p = 31 a. Choose appropriate values for e1 and d, then calculate e2. b. Encrypt the message “HELLO”. Use 00 to 25 for encoding. Use different blocks to make P < p. c. Decrypt the ciphertext to obtain the plaintext. Clearly show all the steps involved in encryption and decryption.	CO2	PO2	**08**
			UNIT - V			
	7	a)	Explain the attacks on Digital Signature.	CO1	PO1	**06**
		b)	Using the RSA Digital Signature scheme, let p = 809, q = 751 and d = 23. Calculate the public key e. Then do the following: i. Sign and verify a message with M1 = 100 Calculate the signature S1. ii. Sign and verify a message with M2 = 50. Calculate the signature S2.	CO2	PO2	**06**
		c)	In the Diffie-Hellman protocol, g = 7, p = 23, x = 3, and y = 5. i. What is the value of the symmetric key? ii. What is the value of R1 and R2? iii. Consider the above values for Alice and Bob. Demonstrate Man in the middle attack with your own value for Eve.	CO2	PO2	**08**

******