

MCA DEGREE THIRD SEMESTER EXAMINATION, JANUARY 2022

20-382-0327 INTRODUCTION TO CRYPTOGRAPHY

(Regular)

Time : 3 Hours

Maximum Marks:50

(Answer **ANY FIVE** questions)

Each question carries EQUAL Marks.

No		QUESTIONS	MARKS	CO	BL	PI																																																																																																																																																																																																																																																																																																														
1.	(a)	<table border="1"><tr><td>6</td><td>24</td><td>1</td></tr><tr><td>13</td><td>16</td><td>10</td></tr><tr><td>20</td><td>17</td><td>15</td></tr></table> <p>Prove that the above key is invertible for Hill Cipher Decryption.</p>	6	24	1	13	16	10	20	17	15	5	CO1	L3	1.7.1																																																																																																																																																																																																																																																																																																					
	6	24	1																																																																																																																																																																																																																																																																																																																	
	13	16	10																																																																																																																																																																																																																																																																																																																	
20	17	15																																																																																																																																																																																																																																																																																																																		
(b)	Use the VIGENERE CIPHER With Keyword HEALTH To encipher the message LIFE IS FULL OF SURPRISES.	3																																																																																																																																																																																																																																																																																																																		
(c)	Evaluate $(-7503) \bmod 81$.	2																																																																																																																																																																																																																																																																																																																		
2.	(a)	Compare Feistel and non feistel ciphers.	4	CO2	L2	2.6.2																																																																																																																																																																																																																																																																																																														
	(b)	Rijindael AES supports the use of 16X16 S-Boxes for byte substitution operation. Consider the given S-Box and below given state table . <table border="1"><tr><td colspan="2" rowspan="2"></td><td colspan="16">y</td></tr><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>a</td><td>b</td><td>c</td><td>d</td><td>e</td><td>f</td></tr><tr><td rowspan="16">x</td><td>0</td><td>63</td><td>7c</td><td>77</td><td>7b</td><td>f2</td><td>6b</td><td>6f</td><td>c5</td><td>30</td><td>01</td><td>67</td><td>2b</td><td>fe</td><td>d7</td><td>ab</td><td>76</td></tr><tr><td>1</td><td>ca</td><td>82</td><td>c9</td><td>7d</td><td>fa</td><td>59</td><td>47</td><td>f0</td><td>ad</td><td>d4</td><td>a2</td><td>af</td><td>9c</td><td>a4</td><td>72</td><td>c0</td></tr><tr><td>2</td><td>b7</td><td>fd</td><td>93</td><td>26</td><td>36</td><td>3f</td><td>f7</td><td>cc</td><td>34</td><td>a5</td><td>e5</td><td>f1</td><td>71</td><td>d8</td><td>31</td><td>15</td></tr><tr><td>3</td><td>04</td><td>c7</td><td>23</td><td>c3</td><td>18</td><td>96</td><td>05</td><td>9a</td><td>07</td><td>12</td><td>80</td><td>e2</td><td>eb</td><td>27</td><td>b2</td><td>75</td></tr><tr><td>4</td><td>09</td><td>83</td><td>2c</td><td>1a</td><td>1b</td><td>6e</td><td>5a</td><td>a0</td><td>52</td><td>3b</td><td>d6</td><td>b3</td><td>29</td><td>e3</td><td>2f</td><td>84</td></tr><tr><td>5</td><td>53</td><td>d1</td><td>00</td><td>ed</td><td>20</td><td>fc</td><td>b1</td><td>5b</td><td>6a</td><td>cb</td><td>be</td><td>39</td><td>4a</td><td>4c</td><td>58</td><td>cf</td></tr><tr><td>6</td><td>d0</td><td>ef</td><td>aa</td><td>fb</td><td>43</td><td>4d</td><td>33</td><td>85</td><td>45</td><td>f9</td><td>02</td><td>7f</td><td>50</td><td>3c</td><td>9f</td><td>a8</td></tr><tr><td>7</td><td>51</td><td>a3</td><td>40</td><td>8f</td><td>92</td><td>9d</td><td>38</td><td>f5</td><td>bc</td><td>b6</td><td>da</td><td>21</td><td>10</td><td>ff</td><td>f3</td><td>d2</td></tr><tr><td>8</td><td>cd</td><td>0c</td><td>13</td><td>ec</td><td>5f</td><td>97</td><td>44</td><td>17</td><td>c4</td><td>a7</td><td>7e</td><td>3d</td><td>64</td><td>5d</td><td>19</td><td>73</td></tr><tr><td>9</td><td>60</td><td>81</td><td>4f</td><td>dc</td><td>22</td><td>2a</td><td>90</td><td>88</td><td>46</td><td>ee</td><td>b8</td><td>14</td><td>de</td><td>5e</td><td>0b</td><td>db</td></tr><tr><td>a</td><td>e0</td><td>32</td><td>3a</td><td>0a</td><td>49</td><td>06</td><td>24</td><td>5c</td><td>c2</td><td>d3</td><td>ac</td><td>62</td><td>91</td><td>95</td><td>e4</td><td>79</td></tr><tr><td>b</td><td>e7</td><td>c8</td><td>37</td><td>6d</td><td>8d</td><td>d5</td><td>4e</td><td>a9</td><td>6c</td><td>56</td><td>f4</td><td>ea</td><td>65</td><td>7a</td><td>ae</td><td>08</td></tr><tr><td>c</td><td>ba</td><td>78</td><td>25</td><td>2e</td><td>1c</td><td>a6</td><td>b4</td><td>c6</td><td>e8</td><td>dd</td><td>74</td><td>1f</td><td>4b</td><td>bd</td><td>8b</td><td>8a</td></tr><tr><td>d</td><td>70</td><td>3e</td><td>b5</td><td>66</td><td>48</td><td>03</td><td>f6</td><td>0e</td><td>61</td><td>35</td><td>57</td><td>b9</td><td>86</td><td>c1</td><td>1d</td><td>9e</td></tr><tr><td>e</td><td>e1</td><td>f8</td><td>98</td><td>11</td><td>69</td><td>d9</td><td>8e</td><td>94</td><td>9b</td><td>1e</td><td>87</td><td>e9</td><td>ce</td><td>55</td><td>28</td><td>df</td></tr><tr><td>f</td><td>8c</td><td>a1</td><td>89</td><td>0d</td><td>bf</td><td>e6</td><td>42</td><td>68</td><td>41</td><td>99</td><td>2d</td><td>0f</td><td>b0</td><td>54</td><td>bb</td><td>16</td></tr></table>					y																0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0
		y																																																																																																																																																																																																																																																																																																																		
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f																																																																																																																																																																																																																																																																																																			
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76																																																																																																																																																																																																																																																																																																			
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0																																																																																																																																																																																																																																																																																																			
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15																																																																																																																																																																																																																																																																																																			
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75																																																																																																																																																																																																																																																																																																			
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84																																																																																																																																																																																																																																																																																																			
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf																																																																																																																																																																																																																																																																																																			
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8																																																																																																																																																																																																																																																																																																			
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2																																																																																																																																																																																																																																																																																																			
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73																																																																																																																																																																																																																																																																																																			
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db																																																																																																																																																																																																																																																																																																			
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79																																																																																																																																																																																																																																																																																																			
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08																																																																																																																																																																																																																																																																																																			
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a																																																																																																																																																																																																																																																																																																			
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e																																																																																																																																																																																																																																																																																																			
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df																																																																																																																																																																																																																																																																																																			
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16																																																																																																																																																																																																																																																																																																			

		<table border="1"><tr><td>19</td><td>a0</td><td>9a</td><td>e9</td></tr><tr><td>3d</td><td>f4</td><td>c6</td><td>f8</td></tr><tr><td>e3</td><td>e2</td><td>8d</td><td>48</td></tr><tr><td>be</td><td>2b</td><td>2a</td><td>08</td></tr></table> <p>i) What is the value of the matrix after Substitute byte operation?</p> <p>ii) Write the output of shiftrow operation from the result of i.</p>	19	a0	9a	e9	3d	f4	c6	f8	e3	e2	8d	48	be	2b	2a	08	3			
19	a0	9a	e9																			
3d	f4	c6	f8																			
e3	e2	8d	48																			
be	2b	2a	08																			
			3	CO2	L3	2.5.3																
3.	(a)	Consider an Elgamal Scheme with a common prime $p = 29$, having a prime root $a = 10$. Write the method to prove that a is a primitive root modulo p .	2	CO6	L3	2.5.3																
		i) If Bala, the receiver has a private key = 3, then what is the public key shared with the sender?	2																			
		ii) For communication, Ashok (sender) chooses the random integer $r=2$, what is the cipher text (C1, C2) corresponding to the plaintext message $M=20$?	2																			
	(b)	Euler's Totient Function is denoted as $\Phi(n)$. Solve a) $\Phi(19)$ b) $\Phi(361)$ c) $\Phi(323)$ d) $\Phi(342)$ Using properties of $\Phi(n)$	4	CO6	L3	1.7.1																
4.	(a)	If we have a message M of size 128 bits, whose MD5 hash $H1$ is exactly 128 bits = '844f85c2723bbd39381c7379a6041608'. What will be the size of the hash for the message created by appending M with another copy of the same message if the hashing algorithm remains the same?	2	CO5	L4	1.6.1																

	(b)	Let m be a message consisting of 50 blocks. Alice transmits m to Bob using block mode of encryption. Due to a network error, the 24th block gets corrupted, but all other ciphertext blocks are transmitted correctly. Once Bob decrypts the cipher text, how many plaintext blocks will be affected, in? If using a) CFB mode of operation? b) OFB mode of operation?	4	CO3	L2	1.6.1
	(c)	Consider the message with 2400 bits given as input to SHA512 algorithm, how many bits need to be added to it excluding the length. If the size of the message is 900 in bits, How many bits need to be padded if SHA1 algorithm used for digest preparation.	4	CO5	L3	1.7.1
5.		Answer the questions below regarding key generation with Diffie-Hellman and RSA. (a) Suppose the Diffie-Hellman public values p and a are 7 and 4, respectively. If one user's secret is 3. Find public key and a session key? Also by selecting a valid secret for the next user, prove that both session keys are same (b) Suppose that you are computing an RSA key pair. What are p and q and $\phi(n)$ for an $n = 51$? Find a legal RSA public key pair for this p and q . How many possible values for e are there?	5+5	CO6	L3	2.5.3
6.		Consider the curve $Y^2 = X^3 + 2X + 2$ over the prime field Z_{17} . Find all the points on the curve. If point $P = (5, 1)$ is a point on the curve find what is $2P$ and $3P$	6+4	CO6	L3	2.5.3
7.	(a)	Explain the role of X.509 certificate for security.	5+5	CO7	L2	1.2.2
	(b)	With a block diagram explain Digital Certificate Issue process.				
