Class Test-I

Subject: Cryptography and Network Security **Semester: VII**
Subject Code: MC407
Class: B.Tech. MC1 and MC2 **Academic Year: 2020-21**

Q.N.	Type and marks	Question	Answer
1.	Short 1	What would be the size of the key domain of a multiplicative cipher if space, comma and full stop are allowed in the plaintext. **Answer:** There would be 29 (26+3) symbols. Therefore, number of elements whose multiplicative inverse modulo 29 exist would be 28 as 29 is a prime number.	28
2.	Short Answer 2	Let $K = [12, 5; 7, 17]$ be the key used in a Hill cipher encryption algorithm. Find the key which would be used in the decryption algorithm. **Answer:** Does Not Exist, because $\|K\| = 13\ and\ K^{-1} = \|K\|^{-1} adj(K)$ but $\|K\|^{-1}$ does not exist as gcd(13, 26)$\neq$ 1.	Not exist
3.	Short Answer 1	How many unique substitution boxes in DES after the 48-bit XOR operation are required? **Answer: 8**	8
4.	Short Answer 1	How much time it will take (in seconds) to break DES by a brute force attack if a computer can search 2^{30} keys per second. **Answer:** DES uses 56-bits key. Therefore, required time is $\frac{2^{56}}{2^{30}} = 2^{26} =$ 67108864	67108864
5.	Short Answer 2	Encrypt the message "attacknewyork" using Playfair cipher. Use the keyword "wonder is the beginning of wisdom" to make the secret key. **Answer:** Key is given by W O N D E R I/J S T H B G F M A C K L P Q U V X Y Z **Ciphertext:** MH HM KL DW DU WI LV	MH HM KL DW DU WI LV
6.	Short Answer 1	Briefly explain single letter frequency attack. **Answer:** Frequency of letters in a language is not uniform. Some letters occur more frequently than others. For example, in English, the letter "e" occurs most frequently. This property of a language can be utilised to analyse a ciphertext if the ciphertext obtained is a monoalphabetic cipher. Attacking a ciphertext using the frequency of single letters is called single letter frequency attack.	

<table>
<tr><td>7.</td><td>Short Answer

1</td><td>Let $C = E(p) = (12p + 17)\ mod\ 26$ be the encryption in a cryptographic scheme. What would be the formula for decryption?

Answer: Not exist, because $12^{-1} mod\ 26$ does not exist.</td><td>Not exist</td></tr>
<tr><td>8.</td><td>Grid

1</td><td><table><tr><td></td><td>Monoalphabetic</td><td>Polyalphabetic</td></tr><tr><td>Ceaser Cipher</td><td>1</td><td>0</td></tr><tr><td>Hill cipher</td><td>0</td><td>1</td></tr><tr><td>Affine cipher</td><td>1</td><td>0</td></tr><tr><td>Playfair cipher</td><td>0</td><td>1</td></tr><tr><td>Autokey cipher</td><td>0</td><td>1</td></tr><tr><td>Vigenere</td><td>0</td><td>1</td></tr><tr><td></td><td></td><td></td></tr></table></td><td></td></tr>
<tr><td>9.</td><td>Checkbox

1</td><td>Which of the following is/are not correct?

(a) DES is a Feistel cipher.
(b) IDEA uses 64- bit key.
(c) 2DES is more secure than 3DES.
(d) There are no non-invertible elements in DES.</td><td>(b), (c), (d)</td></tr>
<tr><td>10.</td><td>Multiple choice

1</td><td>Consider the following D-Box.
<table><tr><td>8</td><td>10</td><td>11</td><td>5</td></tr><tr><td>4</td><td>6</td><td>4</td><td>8</td></tr><tr><td>12</td><td>1</td><td>2</td><td>7</td></tr><tr><td>3</td><td>9</td><td>12</td><td>2</td></tr></table>What type of D-Box is this?

(a) Compression D-Box.
(b) Expansion D-Box.
(c) Straight D-Box
(d) None of the above</td><td>(b)</td></tr>
<tr><td>11.</td><td>Short Answer

1</td><td>Consider the following S-Box.
<table><tr><td></td><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>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td></tr><tr><td>0</td><td>14</td><td>04</td><td>13</td><td>01</td><td>02</td><td>15</td><td>11</td><td>08</td><td>03</td><td>10</td><td>06</td><td>12</td><td>05</td><td>09</td><td>00</td><td>07</td></tr><tr><td>1</td><td>00</td><td>15</td><td>07</td><td>04</td><td>14</td><td>02</td><td>13</td><td>10</td><td>03</td><td>06</td><td>12</td><td>11</td><td>09</td><td>05</td><td>03</td><td>08</td></tr><tr><td>2</td><td>04</td><td>01</td><td>14</td><td>08</td><td>13</td><td>06</td><td>02</td><td>11</td><td>15</td><td>12</td><td>09</td><td>07</td><td>03</td><td>10</td><td>05</td><td>00</td></tr><tr><td>3</td><td>15</td><td>12</td><td>08</td><td>02</td><td>04</td><td>09</td><td>01</td><td>07</td><td>05</td><td>11</td><td>03</td><td>14</td><td>10</td><td>00</td><td>06</td><td>13</td></tr></table>What would be the output if the input to this S-box is 110101?

Answer: First and last bits define the row and middle 4 bits define the column.</td><td>03_{10}

or

0011_2</td></tr>
<tr><td>12.</td><td>1</td><td>Which of the following is/are correct?
(a) Two specially chosen inputs to an S-box array can create the same output.
(b) IDEA uses 126- bit key.
(c) There are no S-boxes in IDEA.
(d) IDEA uses addition modulo 2^{16} and multiplication modulo 2^{16} operations.</td><td>(a),

(c)</td></tr>
</table>

13.	Short 1	What is the minimum number of plaintext-ciphertext pairs required to successfully break 2DES with probability almost equal to 1?	2
14.	Short 2	Encrypt the message “handover the briefcase to John” using a transposition cipher which uses the key $[3\ 5\ 1\ 6\ 2\ 4]$. **Answer:** NOHVAD TEEBRH ECRAIF TJSOEO WYHZHX	
15.	Short 2	What would be the size of the key (2×2) domain of a Hill cipher if the punctuation marks (periods, question marks and spaces) are allowed in the plaintext. **Answer:** Number of possible keys are $29^4 = 707{,}281$. Note: Some of them might not be invertible. Number of invertible keys would be given by $(29^2 - 1)(29^2 - 29) = 682080$.	
16.	Short 1	Does double encryption in an additive cipher increase the security of the cipher? Justify your answer. Ans: No, because double encryption with two keys (say *n* and *m*) is same as the single encryption (with the key $(n + m)$ mod 26).	No

End