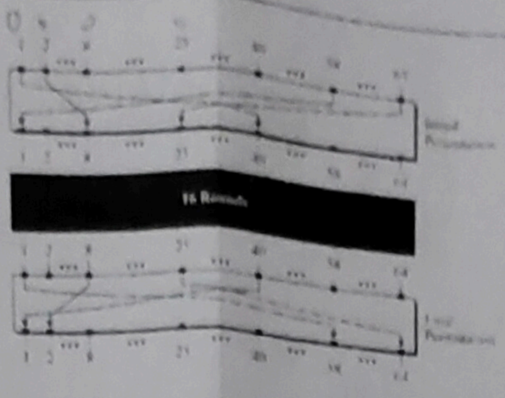
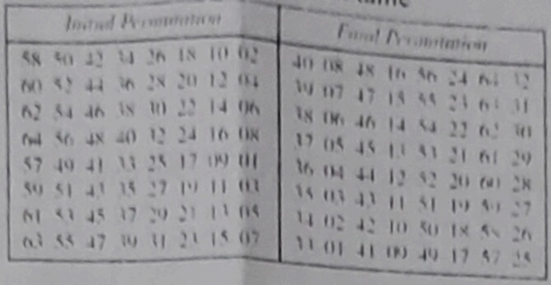
SOMAIYA
VIDYAVIHAR UNIVERSITY

| | | | |
|---|---|---|---|
| Maximum Marks: 30 | Semester: January 2025-April 2025<br>Examination: In-Semester Examination | | Duration:1 Hr. 15 Mins |
| Programme code: 01<br>Programme: Computer Engineering | | Class:<br>TY B.Tech | Semester:<br>VI (SVU2020) |
| Institute/School/ Department:<br>K. J. Somaiya College of Engineering | | Name of the department: COMP | |
| Course Code: 116U01C602 | Name of the Course: Information Security | | |

<table>
<tr><th>Question No.</th><th></th><th>Max.<br>Marks</th></tr>
<tr><td>Q1 A)</td><td>Describe various methods of defense required in security?</td><td>05</td></tr>
<tr><td>Q1 B)</td><td>A small private club has only 100 members. Answer the following<br>1. How many secret keys are needed if all members of club need to send secret messages to each other?<br>2. How many secret keys are needed if everyone trusts the President of the club? If member needs to send a message to another member, she first sends it to President; the President sends message to the other member.<br>3. How many secret keys are needed if the President decides that the two members who need to communicate should contact him first? The President then creates a temporary key to be used between the two. The temporary key is encrypted and sent to both members.</td><td>05</td></tr>
<tr><td>Q2 A)</td><td>In a Polybius cipher, each letter is enciphered as two integers. The key is a 5 × 5 matrix of characters as in a Playfair cipher. The plaintext is the character in the matrix, the ciphertext is the two integers (each between 1 and 5) representing row and column numbers.<br><br>Encipher the message "<i>An exercise</i>" using the Polybius cipher with the following key:
<table>
<tr><th></th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th></tr>
<tr><td>1</td><td>z</td><td>q</td><td>p</td><td>f</td><td>e</td></tr>
<tr><td>2</td><td>y</td><td>r</td><td>o</td><td>g</td><td>d</td></tr>
<tr><td>3</td><td>x</td><td>s</td><td>n</td><td>h</td><td>c</td></tr>
<tr><td>4</td><td>w</td><td>t</td><td>m</td><td>i/j</td><td>b</td></tr>
<tr><td>5</td><td>v</td><td>u</td><td>l</td><td>k</td><td>a</td></tr>
</table>
<br><b>OR</b><br><br>Consider the following initiatl permutation and final permutation in DES algorithm</td><td>05</td></tr>
</table>



Initial permutation tanle



| Initial Permutation | Final Permutation |
|---|---|
| 58 50 42 34 26 18 10 02 | 40 08 48 16 56 24 64 32 |
| 60 52 44 36 28 20 12 04 | 39 07 47 15 55 23 63 31 |
| 62 54 46 38 30 22 14 06 | 38 06 46 14 54 22 62 30 |
| 64 56 48 40 32 24 16 08 | 37 05 45 13 53 21 61 29 |
| 57 49 41 33 25 17 09 01 | 36 04 44 12 52 20 60 28 |
| 59 51 43 35 27 19 11 03 | 35 03 43 11 51 19 59 27 |
| 61 53 45 37 29 21 13 05 | 34 02 42 10 50 18 58 26 |
| 63 55 47 39 31 23 15 07 | 33 01 41 09 49 17 57 25 |

Using above table, Find the output of the initial permutation box when the input is given in hexadecimal as:

0x0000 0080 00010002

Q2 B) What are the design principles of security? Explain any one in detail. 05

OR

Explain in what circumstances penetrate and patch is useful program maintenance strategy.

Q3 A) Explain why genetic diversity is good principle for secure development. Cite an example of lack of diversity that has had a negative impact on security. 10

OR

What are unintentional program errors? Explain any two in detail.