REG.NO.:

VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2024-2025

SLOT: C1+TC1

Programme Name & Branch	: M.Tech (Integrated) Computer Science and Engineering
Course Code and Course Name	: CSI3022 & Cyber Security and Application Security
Faculty Name(s)	: Prof. K. Parthiban & Prof. S. Siva Sankari
Class Number(s)	: VL2024250101961 & VL2024250101962
Date of Examination	: 15.10.2024
Exam Duration	: 90 minutes

Maximum Marks: 50

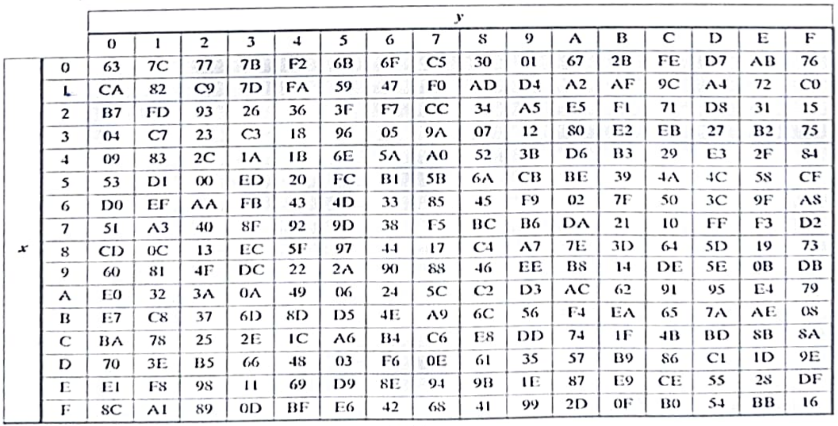
Answer All Questions

M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)

CO3: Understand and implement the cryptographic techniques and know the real time applications of various cryptographic techniques.

CO4: Know fundamentals of cybercrimes and the cyber offenses.

CO5: Understand the cyber threats, attacks, vulnerabilities and its defensive mechanisms

<table>
<tr><th>Q. No</th><th>Question</th><th>M</th><th>CO</th><th>BL</th></tr>
<tr><td>1.</td><td>
A. Given the plaintext [1100 1122 0002 0003 0004 0121 1213 AB1C] and the key [0111 1101 0222 1203 0006 3030 4004 5114]. Apply AES algorithm to perform the following
i) Show the original contents of state, displayed as a 4x4 matrix. (1Mark)
ii) Show the value of state after initial AddRoundKey. (3 Marks)
iii) Show the value of State after SubBytes. (2 Marks)
iv) Show the value of State after ShiftRows. (1 Marks)

<table>
<tr><th></th><th></th><th colspan="16">y</th></tr>
<tr><th></th><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>A</th><th>B</th><th>C</th><th>D</th><th>E</th><th>F</th></tr>
<tr><td>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></td><td>L</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></td><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></td><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></td><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></td><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></td><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></td><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></td><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></td><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></td><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></td><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></td><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></td><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></td><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></td><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>
(a) S-box
B. In an elliptic curve group defined by $E_{13}(10,6)$, What is 2P, if the point P is (5,5). (3Marks)
</td><td>10</td><td>CO3</td><td>BL3</td></tr>
<tr><td>2.</td><td>In a digital world where secure communication is paramount, Robert wishes to send a confidential message to Russel, ensuring that only he can read it. To achieve this, they decide to use RSA algorithm, a widely used method for</td><td>10</td><td>CO3</td><td>BL4</td></tr>
</table>

REG.NO.:

VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CONTINUOUS ASSESSMENT TEST - II

FALL SEMESTER 2024-2025

SLOT: C1+TC1

	secure data transmission. Russel selects two prime numbers as 7 and and 17. These numbers will be the foundation of his encryption and decryption process. Russel selects a public exponent which is relatively prime to $\phi(n)$ as 13. Robert wants to send the message 25 to Russel. Apply RSA algorithm to generate a key pair and then perform the encryption and decryption of messages between them. Show all the steps.			
3.	Assume there are two parties A and B wish to share some information secretly. They planned to use Elliptic Curve Cryptosystem for their communication. Perform Elliptic curve encryption using the elliptic curve $y^2 \equiv x^3+x+1$ mod 23 with generator point G=(3,10) and B's private key n=2. i Find B's public key P_U. (4 Marks) ii A wishes to share the message M=(9,7) to B. Let the random integer k=2. Find the cipher text and show all the steps A follows for encrypting the plaintext to cipher text. (6 Marks)	10	CO3	BL5
4.	Assuming Mr. Rahul is running a ROZOinFO cyber cafe in Vellore, providing computer-related services to the public, let's discuss the possible vulnerabilities in his cafe. Could you discuss the safety and security policies that should be followed in a cyber cafe? Additionally, what instructions should Mr. Rahul provide to customers who are using the computer services in his cafe to help them protect themselves from cyber-attacks?	10	CO4	BL2
5.	A. Suppose you are running XYZ Company, a tech firm focused on software development. You have a team of developers and support staff who use company-provided laptops to perform their jobs. You want to ensure that employees are not misusing company resources by engaging in other activities. To achieve this, you plan to identify the software that can be installed on all company laptops to record the keystroke. Discuss the different categories of that software available in market. (5 Marks) B. You are using your laptop when you notice that the webcam light unexpectedly turns on for a few seconds, even though you haven't opened any applications that would use the camera. Alongside this, your device has been running slower than usual, and you experience frequent browser redirects to unknown websites. Based on these observations, what type of attack or threat might your device be experiencing? Provide a list of preventive measures you can take to protect your device from such attacks in the future. (5 Marks)	10	CO5	BL3

****