Name:

Enrolment No:

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2021

Course: Information Security	**Semester:** I
Program: B. Sc. (Hons.) Geology	**Time** : 03 hrs.
Course Code: MATH2022G	**Max. Marks: 100**

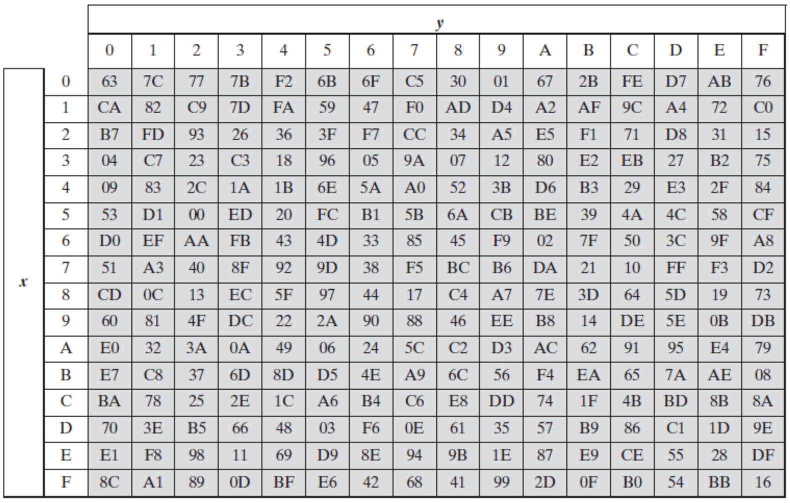
Instructions: 1. Be specific while answering the questions.
2. Justify your answers with the help of examples and diagrams.
3. Internal choices are provided in Question 9 and 11

SECTION A

S. No.		Marks	CO
Q 1	Fill in the blanks: a) 1 KB = ____ B b) 1 ___= 1024 KB c) 2 TB= ____ GB d) 1 PB= ____ GB	**4**	**CO3**
Q 2	Discuss the three main components of security with the help of examples.	**4**	**CO1**
Q 3	Consider the given scenarios and write which factor is maintained (Privacy/ security/ both/ None). a) The bank uses your information to open your account and provide you with products and services. They go on to protect that data. b) The bank sells some of your information to a marketer. Note: You may have agreed to this in the bank's privacy disclosure. The result? Your personal information is in more hands than you may have wanted.	**4**	**CO1**
Q 4	Calculate the value of W, X, Y, and Z: a) $(180)_{10} = (W)_2$ b) $(1F9D)_{16}= (X)_8$ c) $(180)_{10} = (Y)_8$ d) $(01110110)_2 = (Z)_{10}$	**4**	**CO2**
Q 5	Write the type of attack (Active/ Passive) a) Impersonation b) Interception c) Loss of integrity d) Denial of Service	**4**	**CO2**

SECTION B

S. No.		Marks	CO
Q 6	Differentiate monoalphabetic and polyalphabetic cipher. Discuss the encryption and decryption of both the techniques using an example.	**10**	**CO3**
Q 7	Define the terms with example: a) Risk b) Threat	**10**	**CO2**

<table>
<tr><td></td><td>c) Vulnerability
d) Exploit</td><td></td><td></td></tr>
<tr><td>Q 8</td><td>Differentiate authentication and authorization. Discuss different types of authentication techniques. Elaborate the process of password-based authentication process.</td><td><b>10</b></td><td><b>CO1</b></td></tr>
<tr><td>Q 9</td><td>Discuss the classification of intrusion detection system and intrusion prevention system.
<b>OR</b>
Compare and contrast intrusion detection system and intrusion prevention system.</td><td><b>10</b></td><td><b>CO6</b></td></tr>
<tr><td colspan="4"><b>SECTION-C</b></td></tr>
<tr><td>Q 10</td><td>a) Write the algorithm for digital signature using DSS approach.
b) Alice is sending a message to Bob. The message is digitally signed using DSS approach and the hash value of the message is 3. The value of p is 7, h is 2, k is 2 and the private key of sender is 2. Apply signature and verification algorithms to calculate v and r.</td><td><b>20</b></td><td><b>CO5</b></td></tr>
<tr><td>Q 11</td><td>a) Discuss about AES algorithm and draw the complete architecture.
b) The S-Box and 128-bit key value in hexadecimal format are given below. Calculate Key for the first round of AES algorithm.
Key: 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75

<table>
<tr><td></td><td></td><td colspan="16"><i>y</i></td></tr>
<tr><td></td><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>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td></tr>
<tr><td rowspan="16"><i>x</i></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>
(a) S-box
<b>OR</b>
a) Discuss about DES algorithm and draw the complete architecture.
b) The PC-1, PC-2 tables, and 64-bit key value in hexadecimal format are given below. Calculate key for the first round of DES algorithm.
K = 133457799BBCDFF1</td><td><b>20</b></td><td><b>CO4</b></td></tr>
</table>

PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Table 1

PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Table 2