Date : 20-05-2

K J Somaiya Institute of Engineering and Information Technology
An Autonomous Institute Affiliated to University of Mumbai

K. J. Somaiya Institute of Engineering and Information Technology, Sion, Mumbai-22
(Autonomous College Affiliated to University of Mumbai)
End Semester Exam
May –June 2022
B.Tech-Program (Computer Engineering)
Examination: TY Semester VI
Course Code: 1UCEC602 and Course Name: Cryptography and System Security
Duration:03Hours **Max.Marks:60**

Instructions:
(1) All questions are compulsory.
(2) Draw neat diagrams wherever applicable
(3) Assume suitable data, if necessary.

Q.No.	Question	Max.Marks	CO	BTLevel
Q 1	**Solve any six questions out of eight:**	**12**		
i)	Compute GCD of (2222,1234).	**2**	CO1	Ap
ii)	Which parameters the design of Feistal cipher depends on?	**2**	CO2	U
iii)	Which of the malicious programs do not replicate themselves?	**2**	CO6	U
iv)	MD5 and SHA are --- --- a. Asymmetric block cipher, b. stream ciphers c. Message signing algorithms d. symmetric block ciphers.	**2**	CO3	U
v)	Compare AES and triple DES in terms of type of algorithm, key length, rounds, and resource consumption.	**2**	CO2	U
vi)	Difference between authorization and authentication.	**2**	CO4	U
vii)	What is the responsibility of Change cipher Spec Protocol?	**2**	CO5	U
viii)	Explain the security model with block diagram.	**2**	CO1	U
Q.2	**Solve any four questions out of six.**	**16**		
i)	What are the four basic operations in the AES round function? Which are responsible for confusion, and which are responsible for diffusion.	4	CO2	An
ii)	Apply cryptanalysis on the following ciphertext which was encrypted using single columnar transposition: EOCXMTUEALEXECTXTAAXMTNXEBBN	4	C01	Ap
iii)	Explain SHA-1 in detail	4	CO3	U
iv)	What are the different attacks in digital signatures	4	CO4	U
v)	What is packet sniffing? Explain with example.	4	CO5	U

<table>
<tr><td>vi)</td><td>Write short note on SQL injection attack. How it can be prevented?</td><td>4</td><td>CO6</td><td>U</td></tr>
<tr><td>Q.3</td><td>Solve any two questions out of three</td><td>16</td><td></td><td></td></tr>
<tr><td>i)</td><td>What are different methods of authentication. Explain each in detail.</td><td>8</td><td>CO4</td><td>U</td></tr>
<tr><td>ii)</td><td>What are the requirements of cryptographic hash functions? How it can be applied in real world scenario.</td><td>8</td><td>CO3</td><td>An</td></tr>
<tr><td>iii)</td><td>Explain DES algorithm in detail</td><td>8</td><td>CO2</td><td>U</td></tr>
<tr><td>Q. 4</td><td>Solve any two out of three</td><td>16</td><td></td><td></td></tr>
<tr><td>i)</td><td>Apply Hill cipher to encrypt the message “ESSENTIAL”. The key for encryption is “ANOTHERBZ”. And decrypt the encrypted message</td><td>8</td><td>CO1</td><td>Ap</td></tr>
<tr><td>ii)</td><td>Let message is M= compitdt and K= COEPPUNE. M and K both are in Hexadecimal. Generate first two subkeys for DES Encrption.

Initial Permutation Table:
(64 bit):
<table><tr><td>58</td><td>50</td><td>42</td><td>34</td><td>26</td><td>18</td><td>10</td><td>2</td></tr><tr><td>60</td><td>52</td><td>44</td><td>36</td><td>28</td><td>20</td><td>12</td><td>4</td></tr><tr><td>62</td><td>54</td><td>46</td><td>38</td><td>30</td><td>22</td><td>14</td><td>6</td></tr><tr><td>64</td><td>56</td><td>48</td><td>40</td><td>32</td><td>24</td><td>16</td><td>8</td></tr><tr><td>57</td><td>49</td><td>41</td><td>33</td><td>25</td><td>17</td><td>9</td><td>1</td></tr><tr><td>59</td><td>51</td><td>43</td><td>35</td><td>27</td><td>19</td><td>11</td><td>3</td></tr><tr><td>61</td><td>53</td><td>45</td><td>37</td><td>29</td><td>21</td><td>13</td><td>5</td></tr><tr><td>63</td><td>55</td><td>47</td><td>39</td><td>31</td><td>23</td><td>15</td><td>7</td></tr></table>
Compression Table (48 bit):</td><td>8</td><td>CO2</td><td>Ap</td></tr>
</table>

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

Expansion Permutation Table: (56 bit)

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

iii)	What is the need of IPSec? Explain IPSec in detail	**8**	CO5	U