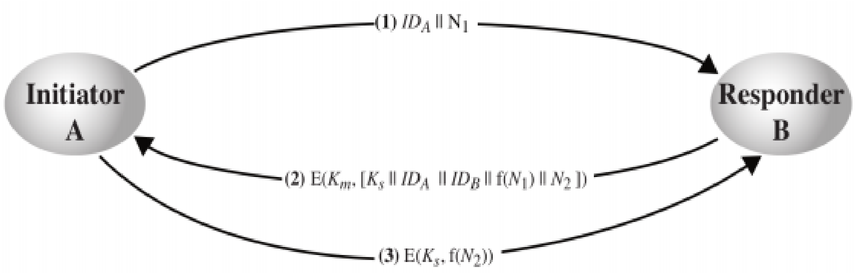
## DHARMSINH DESAI UNIVERSITY, NADIAD
## FACULTY OF TECHNOLOGY
## B.TECH. SEMESTER V [INFORMATION TECHNOLOGY]
## SUBJECT: E- COMMERCE & E-SECURITY [IT-710]

| | | | |
|---|---|---|---|
| **Examination:** | **First Sessional** | | |
| **Date:** | **2/8/2021** | **Time:** | **1:15 to 2:30 (45 mins for descriptive exam)** |

**INSTRUCTIONS:**
1 Figures to the right indicate maximum marks for that question.
2. The symbols used carry their usual meanings.
3. Assume suitable data, if required & mention them clearly.
4. Draw neat sketches wherever necessary.

| | | |
|---|---|---|
| Q:2 | Attempt ***Any Two*** from the following questions. | [8] |
| (a) | Generate at least 4 3-bit number using Blum Blum Shub generator where the seed value is 11 and the two prime numbers are 13 and 17. | [4] |
| (b) | Encrypt the plain text “dd university” using playfair cipher given the keyword: nadiad | [4] |
| (c) | Explain the following key distribution scenario.<br><br> (1) $ID_A \parallel N_1$<br>Initiator A<br>Responder B<br>(2) $E(K_m, [K_s \parallel ID_A \parallel ID_B \parallel f(N_1) \parallel N_2])$<br>(3) $E(K_s, f(N_2))$ | [4] |

<table>
<tr><td>Q:3<br>(a)</td><td>Find the cipher text of the plain text 1010 0000 using S-DES with counter mode algorithm.<br>Key: 11000 10001 ;<br>Counter: 1110 0111<br>P10: 3,5,2,7,4,10,1,9,8,6 ;<br>P8: 6,3,7,4,8,5,10,9 ;<br>IP: 2,6,3,1,4,8,5,7 ;<br>E/P: 4,3,2,1,1,2,3,4 ;<br>P4: 4, 3, 2, 1:<br>$S0 = \begin{array}{cc} & \begin{array}{cccc}0&1&2&3\end{array} \\ \begin{array}{c}0\\1\\2\\3\end{array} & \begin{bmatrix}1&0&3&2\\3&2&1&0\\0&2&1&3\\3&1&3&2\end{bmatrix}\end{array}$ $S1 = \begin{array}{cc} & \begin{array}{cccc}0&1&2&3\end{array} \\ \begin{array}{c}0\\1\\2\\3\end{array} & \begin{bmatrix}0&1&2&3\\2&0&1&3\\3&0&1&0\\2&1&0&3\end{bmatrix}\end{array}$</td><td>[8]</td></tr>
<tr><td colspan="3">OR</td></tr>
<tr><td>Q:3<br>(a)</td><td>Consider following algorithm for hybrid Encryption:<br>1) Transform each of the letters in the plaintext alphabet to the corresponding integer in the range 0 to m-1. Consider this integer as “x”.<br>2)With this done, the encryption process for each letter is given by:<br>E(x) = (ax+b) mod 26. Where a=2 and b=1.<br>(Note: where a and b are the key for the cipher and m is Number of alphabets.)<br>3) Then transform the result obtained from step to into cipher text using HILL cipher with key :<br>| 1 2 3 |<br>| 0 1 4 |<br>| 5 6 0 |<br><br>Using the above algorithm transform the plain text “lockdown” into cipher text.</td><td>[8]</td></tr>
</table>