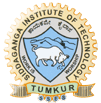
**Siddaganga Institute of Technology, Tumkur-572103**

**Department of Computer Science and Engineering**

**CRYPTOGRAPHY AND NETWORK SECURITY LAB (7CSL02)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Student Name: | | | USN: | Batch No: | | Date: | |
| **Evaluation:** | | | | | | | |
| **Write Up (10 marks)** | **Clarity in concepts (10 marks)** | **Implementation and execution of the algorithms (10 marks)** | | | **Viva (05 marks)** | | **Total (35 marks)** |
|  |  |  | | |  | |  |
|  | | | | | | | |
| Sl.No | Name of the Faculty In-Charge | | | | | | Signature |
| 1. |  | | | | | |  |
| 2. |  | | | | | |  |
| **Question No: 3**  Write a program to perform the following using Hill cipher:   1. Encrypt a message M with a given key matrix of size 2X2 and 3X3 2. Decrypt the cipher text obtained in (i) by computing inverse of the respective key matrix | | | | | | | |
| **Hill Cipher:**  This encryption algorithm takes m successive plaintext letters and substitutes for them m ciphertext letters. The substitution is determined by m linear equations in which each character is assigned a numerical value (a = 0, b = 1, , z = 25) . For m = 3, the system can be described as  c1 = (k11p1 + k12p2 + k13p3)mod 26  c2 = (k21p1 + k22p2 + k23p3)mod 26  c3 = (k31p1 + k32p2 + k33p3)mod 26  C = PK mod 26 where C and P are row vectors of length 3 representing the plaintext and ciphertext, and K is a 3 X 3 matrix representing the encryption key. Operations are performed mod 26.  Decryption requires using the inverse of the matrix K.  C = E(K, P) = PK mod 26  P = D(K, C) = CK-1 mod 26 = PKK-1 = P  For the 2X2 matrix determinant is k11k22 - k12k21. For a 3X3 matrix, the value of the determinant is k11k22k33 + k21k32k13 + k31k12k23 - k31k22k13 - k21k12k33 - k11k32k23  If a square matrix A has a nonzero determinant, then the inverse of the matrix is computed as [A-1]ij = (det A)-1(-1)i+j(Dji) , where (Dji ) is the sub determinant formed by deleting the ‘j’th row and the’ i’th column of A, det(A) is the determinant of A, and (detA)-1 is the multiplicative inverse of (det A) mod 26. | | | | | | | |