# 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: 7**  Given 48-bit input to S-box and permutation table P, find the 32-bit output Ri of ith round of DES algorithm. | | | | | | | |
| Algorithm: To Generate 32-bits S-box output, we need to DES S-boxes for each of 6 bit Input.  The outer two bits of each group select one of four possible substitutions (one row of an S-box). Then a 4-bit output value is substituted for the particular 4-bit input (the middle four input bits). The 32-bit output from the eight S-boxes is then permuted, so that on the next round, the output from each S-box immediately affects as many others as possible.   |  | | --- | | 48-bit input to S-box    Figure: The 32-bit output Ri of ith round, given 48-bit input | | Table: Permutation Function (P) | |  | | Tables: DES S-Boxes | | | | | | | | |