1). Considersimplified DES algorithm that takes 8-bit plaintext M and 6-bit key K as inputs. Its components are defined as follows. Round key generation technique defined as K0 = K, Ki = CiDi where Ci and Di are both of 3-bit length and computed by Ci = Ci−1 ‹‹‹ 2, Di=Di−1 ‹‹‹ 1. Initial Permutation IP = [1 2 4 7 8 3 5 6]. Inverse Initial Permutation IP-1 = [1 2 6 3 7 8 4 5]. Expansion Permutation E has the schema [4 1 2 4 3 2] and another Permutation box has the schema [2 4 1 3]. Only one S-Box is used. Encrypt the message M = 01010011 for one iteration by considering key K=110001.**4M**

**S-**Box Table

|  |
| --- |
| 13 2 8 4 6 15 11 1 10 9 3 14 5 0 12 7 |
| 1 15 13 8 10 3 7 4 12 5 6 11 0 14 9 2 |
| 7 11 4 1 9 12 14 2 0 6 10 13 15 3 5 8 |
| 2 1 14 7 4 10 8 13 15 12 9 0 3 5 6 11 |