Anjali
MT20082

Aditi Sharma
MT20100

We have used following functions for implementing DES:

1. Binary to hex: It takes an input as string, checks the 4 characters at a time and assigns the corresponding hex code.

2. Binary to decimal: It takes a binary number and gives the corresponding decimal number.

3. Decimal to Binary: It takes a decimal number and gives the corresponding binary representation.

4. left_circularshift: It takes a string and do a circular left shift of n bits from the string

5. xor: This function returns the xor of two input strings

6. permute: This function permutes the string in accordance with the given table

7. sbox_subs: This function performs the sbox operation of converting a 48 bit string to 32 bit using tables of sboxes

8. keygen: This function generates 16 subkeys for each round using parity drop permutation and key compression permutation

9. encrypt: It encrypts the plain text to cipher text as follows:

- Plain text in hex is converted to binary
- Initial permutation is applied on plain text using IP table
- Plain text is divided into left and right part
- Then 16 rounds are applied as follows:
    - The right part of plain text is permuted according to the expansion table
    - Then xor is obtained on right part and key of the round
    - The result is then sent to 8 sboxes to get 32 bit string
    - D box permutation is applied to result string
    - Then xor is obtained on left part and result string to give final part
    - The final part and right part are swapped
- Final part and right part are concatenated to form cipher text

10. decrypt: It calls encrypt on cipher text and the reverse of keys used in encrypt

11. DES: This is the main function which takes plain text and key and call encrypt and decrypt

12: Optional: Pad: This function pads the block in case size of block < 64 bits

Anjali
MT20082

Aditi Sharma
MT20100

Output:

```
pt1 = "123456ABCD132536"
key1 = "AABB09182736CCDD"
```

```
Encryption
Round  Left Part    Right Part    Key
1    18CA18AD      5A78E394      194CD072DE8C
2    5A78E394      4A1210F6      4568581ABCCE
3    4A1210F6      B8089591      06EDA4ACF5B5
4    B8089591      236779C2      DA2D032B6EE3
5    236779C2      A15A4B87      69A629FEC913
6    A15A4B87      2E8F9C65      C1948E87475E
7    2E8F9C65      A9FC20A3      708AD2DDB3C0
8    A9FC20A3      308BEE97      34F822F0C66D
9    308BEE97      10AF9D37      84BB4473DCCC
10    10AF9D37      6CA6CB20      02765708B5BF
11    6CA6CB20      FF3C485F      6D5560AF7CA5
12    FF3C485F      22A5963B      C2C1E96A4BF3
13    22A5963B      387CCDAA      99C31397C91F
14    387CCDAA      BD2DD2AB      251B8BC717D0
15    BD2DD2AB      CF26B472      3330C5D9A36D
16    19BA9212      CF26B472      181C5D75C66D
Cipher Text :  C0B7A8D05F3A829C

 Decryption
 Round  Left Part    Right Part    Key
 1    CF26B472      BD2DD2AB      181C5D75C66D
 2    BD2DD2AB      387CCDAA      3330C5D9A36D
 3    387CCDAA      22A5963B      251B8BC717D0
 4    22A5963B      FF3C485F      99C31397C91F
 5    FF3C485F      6CA6CB20      C2C1E96A4BF3
 6    6CA6CB20      10AF9D37      6D5560AF7CA5
 7    10AF9D37      308BEE97      02765708B5BF
 8    308BEE97      A9FC20A3      84BB4473DCCC
 9    A9FC20A3      2E8F9C65      34F822F0C66D
 10    2E8F9C65      A15A4B87      708AD2DDB3C0
 11    A15A4B87      236779C2      C1948E87475E
 12    236779C2      B8089591      69A629FEC913
 13    B8089591      4A1210F6      DA2D032B6EE3
 14    4A1210F6      5A78E394      06EDA4ACF5B5
 15    5A78E394      18CA18AD      4568581ABCCE
 16    14A7D678      18CA18AD      194CD072DE8C
 Plain Text :  123456ABCD132536
 Encryption round 1 and decryption round 15 results are identical
 DES Successful, output plaintest and input plaintext match
```

```
pt2 = "0000000000000000"
key2 = "22234512987ABB23"
```

```
 Encryption
 Round  Left Part    Right Part    Key
 1    00000000      B1F96E5D      4A18AACA41A3
 2    B1F96E5D      A0413507      51A2A125E9A2
 3    A0413507      C8ED692A      919C96240C53
 4    C8ED692A      9FC2A920      7422C6CF8056
 5    9FC2A920      302F2CBA      32D42405C7C8
 6    302F2CBA      9650B447      C80176189445
 7    9650B447      080DB8B9      A4C23DCAC4A4
 8    080DB8B9      94F94E3B      871322086F89
 9    94F94E3B      5E98EFDA      72834B243C31
 10    5E98EFDA      A59B5B3A      29D013AB0876
 11    A59B5B3A      6F87B4B8      2509DE05CB92
 12    6F87B4B8      086DCDD3      366091150455
 13    086DCDD3      C331993D      1F0D30CB80C4
 14    C331993D      7158B362      CE209D00E78D
 15    7158B362      E6D41639      1F860C3A1485
 16    9D845DCF      E6D41639      F10D892A3076
 Cipher Text :  4789FD476E82A5F1

 Decryption
 Round  Left Part    Right Part    Key
 1    E6D41639      7158B362      F10D892A3076
 2    7158B362      C331993D      1F860C3A1485
 3    C331993D      086DCDD3      CE209D00E78D
 4    086DCDD3      6F87B4B8      1F0D30CB80C4
 5    6F87B4B8      A59B5B3A      366091150455
 6    A59B5B3A      5E98EFDA      2509DE05CB92
 7    5E98EFDA      94F94E3B      29D013AB0876
 8    94F94E3B      080DB8B9      72834B243C31
 9    080DB8B9      9650B447      871322086F89
 10    9650B447      302F2CBA      A4C23DCAC4A4
 11    302F2CBA      9FC2A920      C80176189445
 12    9FC2A920      C8ED692A      32D42405C7C8
 13    C8ED692A      A0413507      7422C6CF8056
 14    A0413507      B1F96E5D      919C96240C53
 15    B1F96E5D      00000000      51A2A125E9A2
 16    00000000      00000000      4A18AACA41A3
 Plain Text :  0000000000000000
 Encryption round 1 and decryption round 15 results are identical
 DES Successful, output plaintest and input plaintext match
```