PRACTICAL: 6

AIM:

Simplified DES (S-DES) is a symmetric-key block cipher. The S-DES encryption algorithm takes an 8-bit block of plaintext and a 10-bit key as input and produces an 8-bit block of ciphertext as output. It follows two rounds. Implement S-DES symmetric encryption Algorithm.

THEORY:

A Simplified DES algorithm is used for the encryption and decryption of the data. It has many features of DES(Data Encryption System) but it is simpler than DES. The SDES encryption algorithm produces an 8-bit block of plaintext and a 10-bit key as input and makes an 8-bit block of ciphertext as output.

It is a symmetric key algorithm, which means that the same key is used for encrypting and decrypting data. it has been highly influential in the advancement of cryptography. Encryption and decryption is done using 12 bit block size.

CODE:

```
def apply_table(inp, table):
    """
    >>> apply_table("0123456789", list(range(10)))
    '9012345678'
    >>> apply_table("0123456789", list(range(9, -1, -1)))
    '8765432109'
    """
    res = ""
    for i in table:
        res += inp[i - 1]
    return res


def left_shift(data):
    """
    >>> left_shift("0123456789")
    '1234567890'
    """
    return data[1:] + data[0]


def XOR(a, b):
    """
    >>> XOR("01010101", "00001111")
    '01011010'
    """
    res = ""
    for i in range(len(a)):
```

```
        if a[i] == b[i]:
            res += "0"
        else:
            res += "1"
    return res


def apply_sbox(s, data):
    row = int("0b" + data[0] + data[-1], 2)
    col = int("0b" + data[1:3], 2)
    return bin(s[row][col])[2:]


def function(expansion, s0, s1, key, message):
    left = message[:4]
    right = message[4:]
    temp = apply_table(right, expansion)
    temp = XOR(temp, key)
    l = apply_sbox(s0, temp[:4])  # noqa: E741
    r = apply_sbox(s1, temp[4:])
    l = "0" * (2 - len(l)) + l  # noqa: E741
    r = "0" * (2 - len(r)) + r
    temp = apply_table(l + r, p4_table)
    temp = XOR(left, temp)
    return temp + right


if __name__ == "__main__":

    key = input("Enter 10 bit key: ")
    message = input("Enter 8 bit message: ")

    p8_table = [6, 3, 7, 4, 8, 5, 10, 9]
    p10_table = [3, 5, 2, 7, 4, 10, 1, 9, 8, 6]
    p4_table = [2, 4, 3, 1]
    IP = [2, 6, 3, 1, 4, 8, 5, 7]
    IP_inv = [4, 1, 3, 5, 7, 2, 8, 6]
    expansion = [4, 1, 2, 3, 2, 3, 4, 1]
    s0 = [[1, 0, 3, 2], [3, 2, 1, 0], [0, 2, 1, 3], [3, 1, 3, 2]]
    s1 = [[0, 1, 2, 3], [2, 0, 1, 3], [3, 0, 1, 0], [2, 1, 0, 3]]

    # key generation
    temp = apply_table(key, p10_table)
    left = temp[:5]
    right = temp[5:]
    left = left_shift(left)
    right = left_shift(right)
    key1 = apply_table(left + right, p8_table)
    left = left_shift(left)
    right = left_shift(right)
    left = left_shift(left)
```

```
    right = left_shift(right)
    key2 = apply_table(left + right, p8_table)

    # encryption
    temp = apply_table(message, IP)
    temp = function(expansion, s0, s1, key1, temp)
    temp = temp[4:] + temp[:4]
    temp = function(expansion, s0, s1, key2, temp)
    CT = apply_table(temp, IP_inv)
    print("Cipher text is:", CT)

    # decryption
    temp = apply_table(CT, IP)
    temp = function(expansion, s0, s1, key2, temp)
    temp = temp[4:] + temp[:4]
    temp = function(expansion, s0, s1, key1, temp)
    PT = apply_table(temp, IP_inv)
    print("Plain text after decypting is:", PT)
```

OUTPUT:

```
C:\Users\Administrator\Downloads>python sdes.py
Enter 10 bit key: 1010000010
Enter 8 bit message: 01110111
Cipher text is: 10100110
Plain text after decypting is: 01110111

C:\Users\Administrator\Downloads>19IT016 Manav Butani
```

LATEST APPLICATIONS:

It was developed for educational purpose so that understanding DES can become easy. It is a block cipher algorithm and uses a symmetric key for its algorithm i.e. they use the same key for both encryption and decryption. It has 2 rounds for encryption which use two different keys.

LEARNING OUTCOME:

For encryption purpose Simplified DES use the two key which is generated by the 10 bit key which provided by the user. So, SDES use the two key for the encryption of data. The size of the data is 8 bit.

REFERENCES:

1. https://www.c-sharpcorner.com/article/s-des-or-simplified-data-encryption-standard/
2. https://www.geeksforgeeks.org/simplified-data-encryption-standard-key-generation/