**Cryptography and Network Security**

**Lab**

**Assignment No. 5**

**Name : Sourabh Shankar Patil**

**PRN : 21510045**

**Batch : B2**

**Data Encryption Standard (DES)**

The **Data Encryption Standard (DES)** is a symmetric-key block cipher that was adopted as a federal standard in the United States in 1977. It encrypts data in fixed-size blocks of 64 bits using a 56-bit key.

**Key Features:**

* **Symmetric Encryption**: The same key is used for both encryption and decryption.
* **Block Cipher**: Operates on fixed-size blocks of data (64 bits).
* **Feistel Structure**: DES uses a Feistel network, dividing the block into two halves and applying multiple rounds of transformation.
* **Rounds**: It consists of 16 rounds of processing, including substitution and permutation steps, to increase security.

**Security:**

* DES was considered secure for many years; however, advances in computing power have made it vulnerable to brute-force attacks.
* It was officially withdrawn as a standard by the National Institute of Standards and Technology (NIST) in 2005 in favor of more secure algorithms like **AES (Advanced Encryption Standard)**.

#include <iostream>

#include <bitset>

#include <vector>

using namespace std;

// Initial Permutation table for DES

int IP[] = {58, 50, 42, 34, 26, 18, 10, 2,

            60, 52, 44, 36, 28, 20, 12, 4,

            62, 54, 46, 38, 30, 22, 14, 6,

            64, 56, 48, 40, 32, 24, 16, 8,

            57, 49, 41, 33, 25, 17, 9, 1,

            59, 51, 43, 35, 27, 19, 11, 3,

            61, 53, 45, 37, 29, 21, 13, 5,

            63, 55, 47, 39, 31, 23, 15, 7};

// Final Permutation table for DES

int FP[] = {40, 8, 48, 16, 56, 24, 64, 32,

            39, 7, 47, 15, 55, 23, 63, 31,

            38, 6, 46, 14, 54, 22, 62, 30,

            37, 5, 45, 13, 53, 21, 61, 29,

            36, 4, 44, 12, 52, 20, 60, 28,

            35, 3, 43, 11, 51, 19, 59, 27,

            34, 2, 42, 10, 50, 18, 58, 26,

            33, 1, 41, 9, 49, 17, 57, 25};

bitset<64> DES\_encrypt(bitset<64> plaintext)

{

    bitset<64> permutedText;

    for (int i = 0; i < 64; i++)

    {

        permutedText[i] = plaintext[IP[i] - 1];

    }

    bitset<64> cipherText;

    for (int i = 0; i < 64; i++)

    {

        cipherText[i] = permutedText[FP[i] - 1];

    }

    return cipherText;

}

int main()

{

    bitset<64> plaintext("1100101010110101011101001010101010101010101010101010101010101010");

    bitset<64> cipherText = DES\_encrypt(plaintext);

    // Display the result

    cout << "Encrypted text: " << cipherText << endl;

    return 0;

}

Output:

