EX-NO-7-Implement-DES-Encryption-and-Decryption

Aim:

To use the Data Encryption Standard (DES) algorithm for a practical application, such as securing sensitive data transmission in financial transactions.

ALGORITHM:

1. DES is based on a symmetric key encryption technique that encrypts data in 64-bit blocks.
2. DES uses a Feistel network structure with 16 rounds of processing for encryption.
3. DES has a 64-bit key, but only 56 bits are used for encryption (the remaining 8 bits are for parity).
4. DES applies initial and final permutations along with 16 rounds of substitution and permutation transformations to produce ciphertext.

Program:

```
Developed By: Muhammad Afshan A
Reg No.: 212223100035
```

```
#include <stdio.h>
#include <string.h>


void encrypt(char *message, char *key, char *encryptedMessage, int messageLe
    int keyLength = strlen(key);
    for (int i = 0; i < messageLength; i++) {

        encryptedMessage[i] = message[i] ^ key[i % keyLength];
    }
    encryptedMessage[messageLength] = '\0'; // Null-terminate the encrypted
}


void decrypt(char *encryptedMessage, char *key, char *decryptedMessage, int
```

```
    int keyLength = strlen(key);
    for (int i = 0; i < messageLength; i++) {

        decryptedMessage[i] = encryptedMessage[i] ^ key[i % keyLength];
    }
    decryptedMessage[messageLength] = '\0'; // Null-terminate the decrypted
}

int main() {
    char message[100];
    char key[100];

    printf("\n *****Simulation of DES encryption and decryption*****\n\n");


    printf("Enter the message to encrypt: ");
    fgets(message, sizeof(message), stdin);
    message[strcspn(message, "\n")] = '\0';

    printf("Enter the encryption key: ");
    fgets(key, sizeof(key), stdin);
    key[strcspn(key, "\n")] = '\0';
    int messageLength = strlen(message);


    char encryptedMessage[100];
    char decryptedMessage[100];


    encrypt(message, key, encryptedMessage, messageLength);

    printf("Original Message: %s\n", message);


    printf("Encrypted Message: ");
    for (int i = 0; i < messageLength; i++) {
        printf("%02X ", (unsigned char)encryptedMessage[i]);
    }
    printf("\n");

    // Decrypt the message
    decrypt(encryptedMessage, key, decryptedMessage, messageLength);
    printf("Decrypted Message: %s\n", decryptedMessage);
```

```
    return 0;
}
```

Output:

```
*****Simulation of DES encryption and decryption*****

Enter the message to encrypt: Muhammad Afshan
Enter the encryption key: Saveetha
Original Message: Muhammad Afshan
Encrypted Message: 1E 14 1E 04 08 19 09 05 73 20 10 16 0D 15 06
Decrypted Message: Muhammad Afshan
```

Result:

The program is executed successfully