Assignment No. 3 B

DES Algorithm

Problem Statement :

Implement a client and a server on different computers using python. Perform the encryption of message of sender between these two entities by using DES Algorithm and use Diffie Hellman method for exchange of keys.

Theory:

Data Encryption Standard (DES)

It is a block cipher algorithm that takes plain text in blocks of 64 bits and converts them to ciphertext using keys of 48 bits. It is a symmetric key algorithm, which means that the same key is used for encrypting and decrypting data.

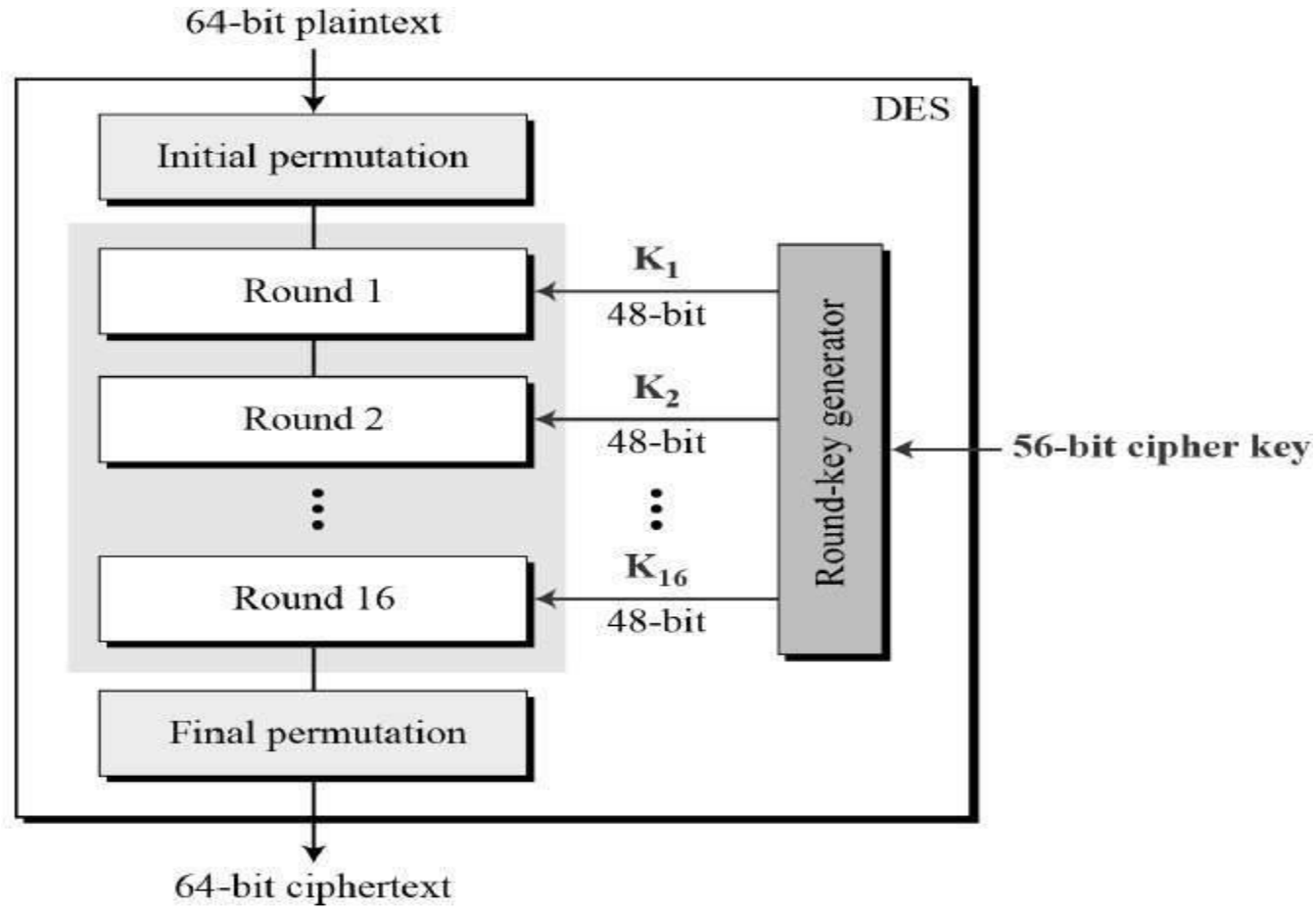

Figure : General structure of DES

Since DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows –

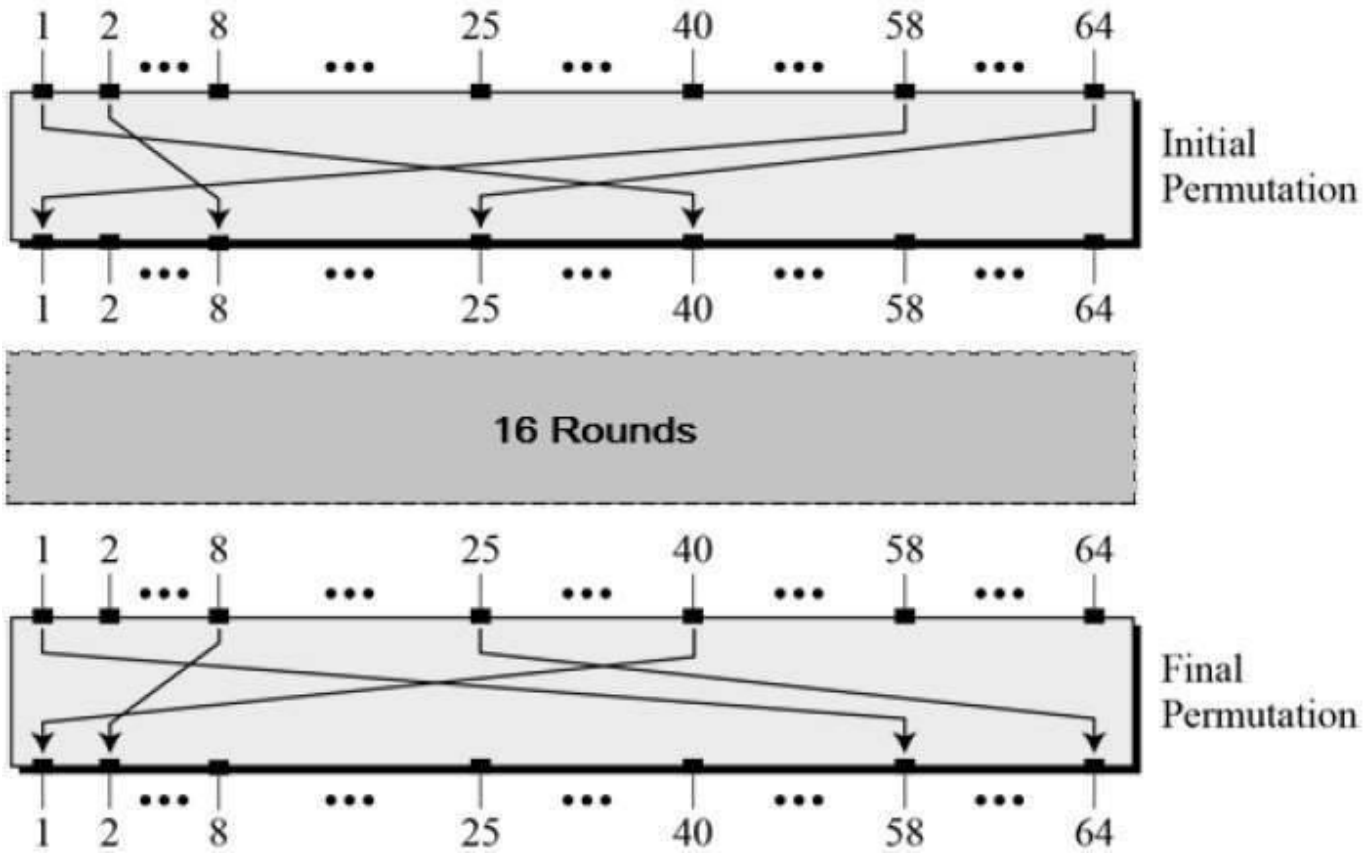

Figure: Initial and final Permutation

The DES algorithm steps are given below:

1. The process begins by giving 64-bit plain text as an input to an initial permutation function (IP).
2. The initial permutation (IP) is then carried out on the plain text.
3. The initial permutation (IP) generates two halves of the permuted block, known as RPT (Right Plain Text) and LPT (Left Plain Text).
4. Each Left Plain Text (LPT) and Right Plain Text (RPT) is encrypted through 16 rounds. This encryption process consists of five stages:

    [1] Key transformation
    [2] Expansion permutation
    [3] S-box permutation
    [4] P-box permutation
    [5] XOR & Swap

5. Finally Left Plain Text (LPT) is combined with Right Plain Text (RPT). After that, on the newly combined block generated, a final permutation is performed.
6. The output of this process will produce a 64-bit ciphertext.

The total number of 16 rounds in DES makes the algorithm complex. DES was mainly designed for hardware so it runs relatively slow on software compared to hardware.

The 56-bit key length used in DES makes it possible to decrypt the encrypted code with modern technologies. Moreover, it can be broken using brute-force attacks and linear cryptanalysis. Hence, **AES (Advanced Encryption Standard) has replaced the DES (Data Encryption Standard)**.

Conclusion – DES (Data Encryption Standard) forms the foundation for encryption algorithms. This makes it easy for one to understand the implementation or working of currently used encryption algorithms or methods, which are much faster than the DES algorithm.