A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

* Laboratory Practice II (Information Security) - Experiment Number - 3.

Name:- Kaustubh Shrikant Kabra.
Class:- Third Year Engineering.
Div:- A
ERP Number:- 38
Department:- Computer Department
College:- AISSMS's IOIT.

Title:-

DES Algorithm

Aim:-

Write a Java/C/C++/Python program to implement DES algorithm.

Objective:-

1. To understand and learn DES algorithm.
2. To implement DES algorithm.

Theory:-

Data Encryption Standard:-

The Data Encryption Standard (DES) system developed for the U.S. government, was intended for use by the general public. It has been officially accepted as a cryptographic standard both in the US and abroad.

The DES algorithm is a careful and complex combination of two fundamental building blocks of encryption: substitution and

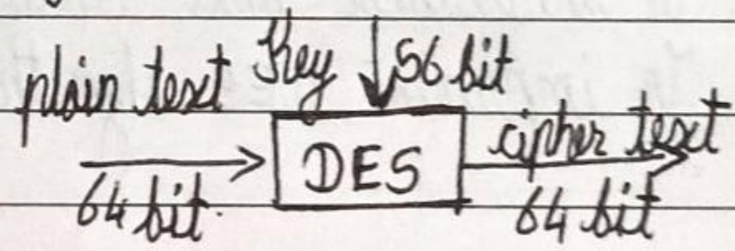
A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

transposition. The algorithm derives its strength from repeated application of these two techniques, one on top of the other for a total of 16 cycles. The sheer complexity of tracing a single bit through 16 iterations of substitutions and transpositions has so far stopped researchers in the public from identifying more than a handful general properties of the algorithm.

The algorithm begins by encrypting the plaintext as blocks of 64 bits. The key is 64 bits long but in fact it can be any 56-bit number.

Features :-

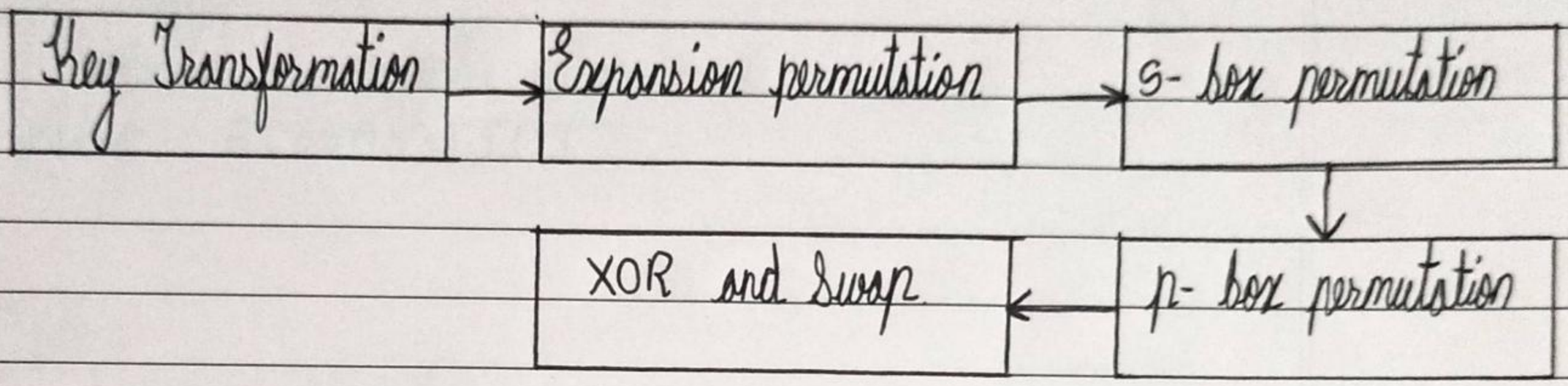
Block size = 64 bits
- Key size = 56 bits (in reality 64 bits, but 8 are used as parity / check bits for error control)
- number of rounds = 16
- 16 intermediary keys, each 48 bits.



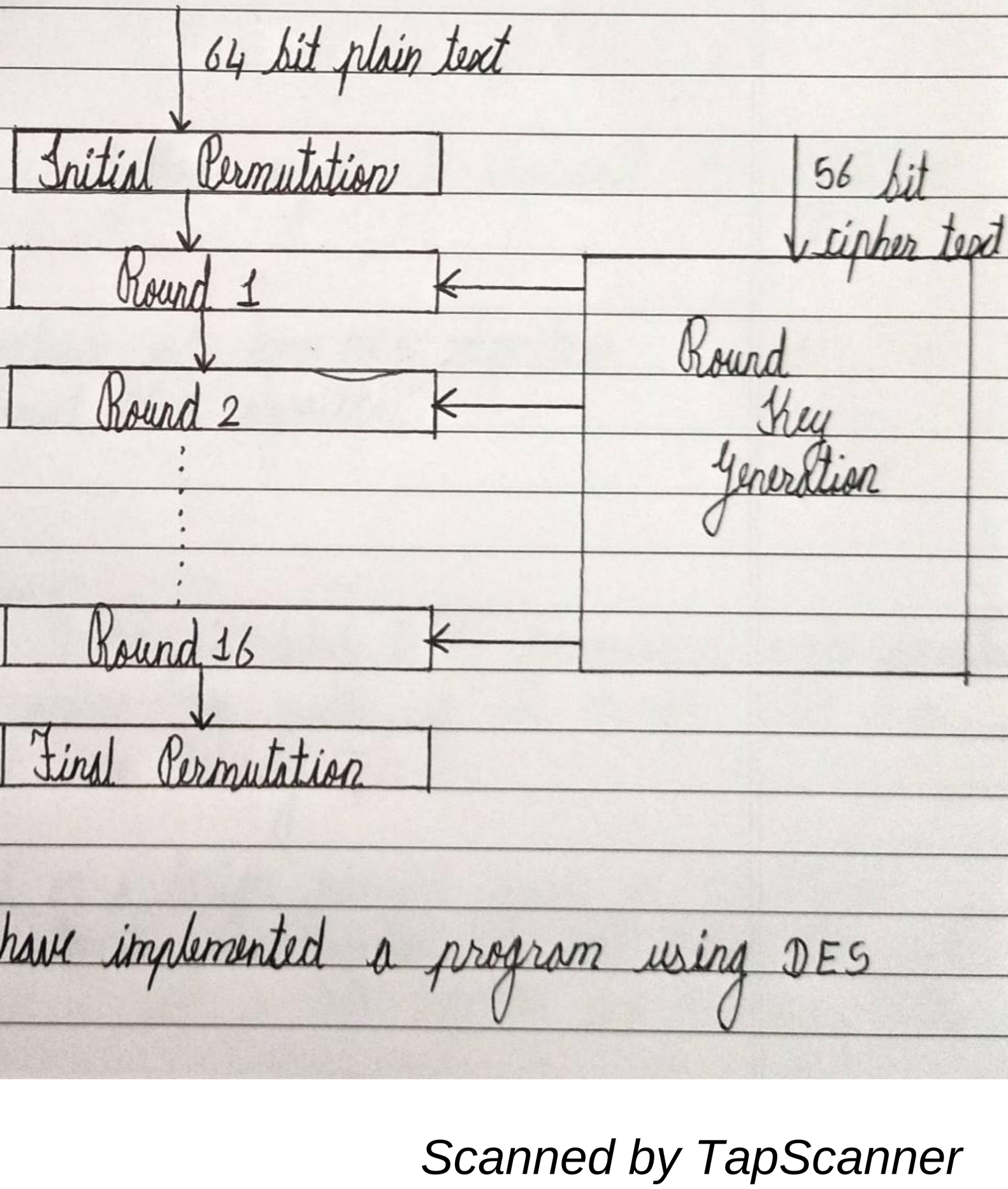
Explanation :-

1. In the first step, the 64-bit plain text block is handed over to an initial permutation (IP) function.
2. The initial permutation is performed on plain text.
3. Next, the initial permutation produces two halves of the permuted block, says Left Plain Text (LPT) and Right Plain Text (RPT).

4. Now each LPT and RPT go throught 16 rounds of the encryption process.
5. In the end, LPT and RPT are rejoined and a final permutation (FP) is performed on the combined block.
6. The result of this process produces 64-bit cipher text.



Working Principle :-



Conclusion:-

Thus we have implemented a program using DES algorithm.