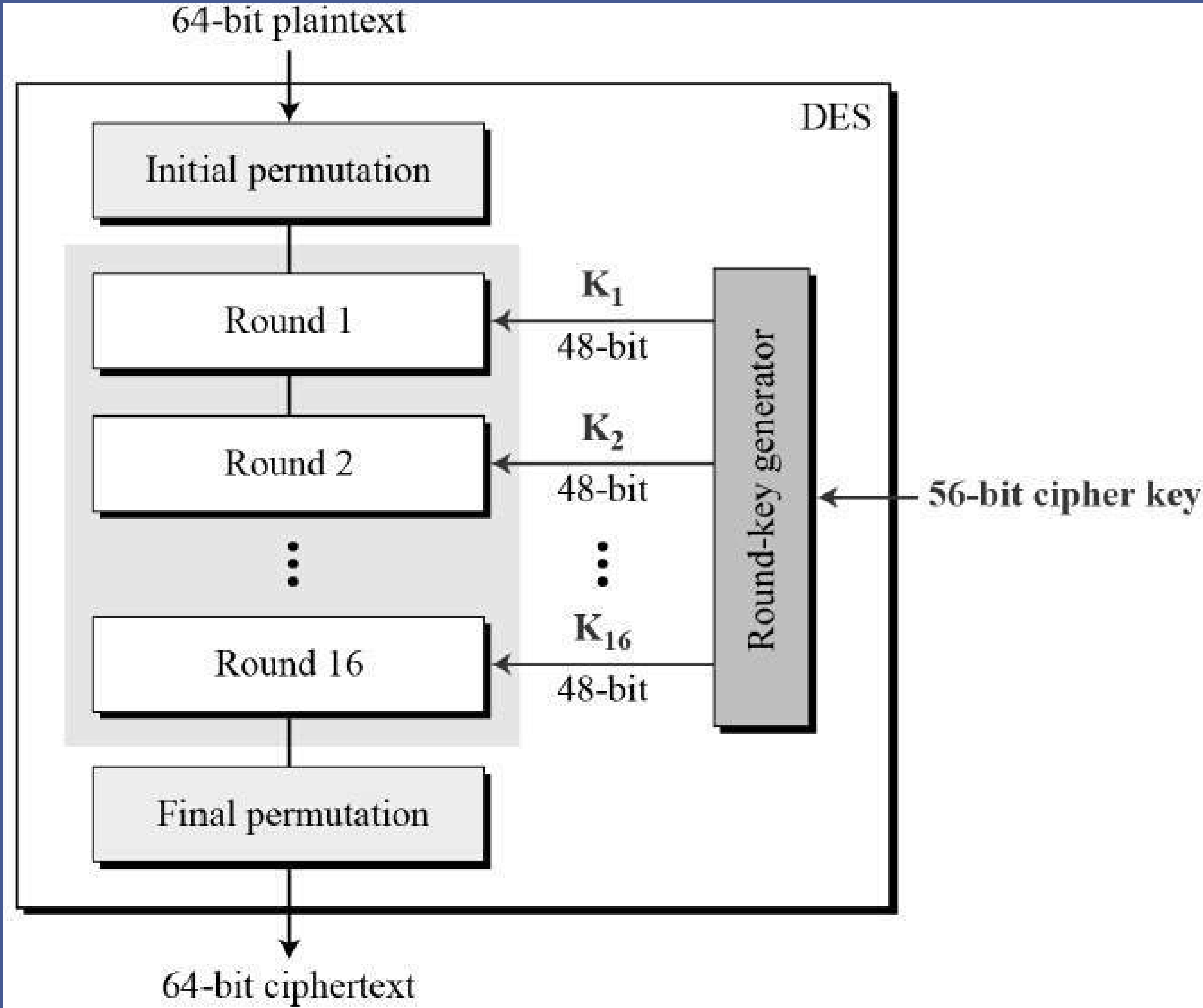
Data Encryption Standard (DES) Algorithm

Presented By: Manav Raj

What is DES?

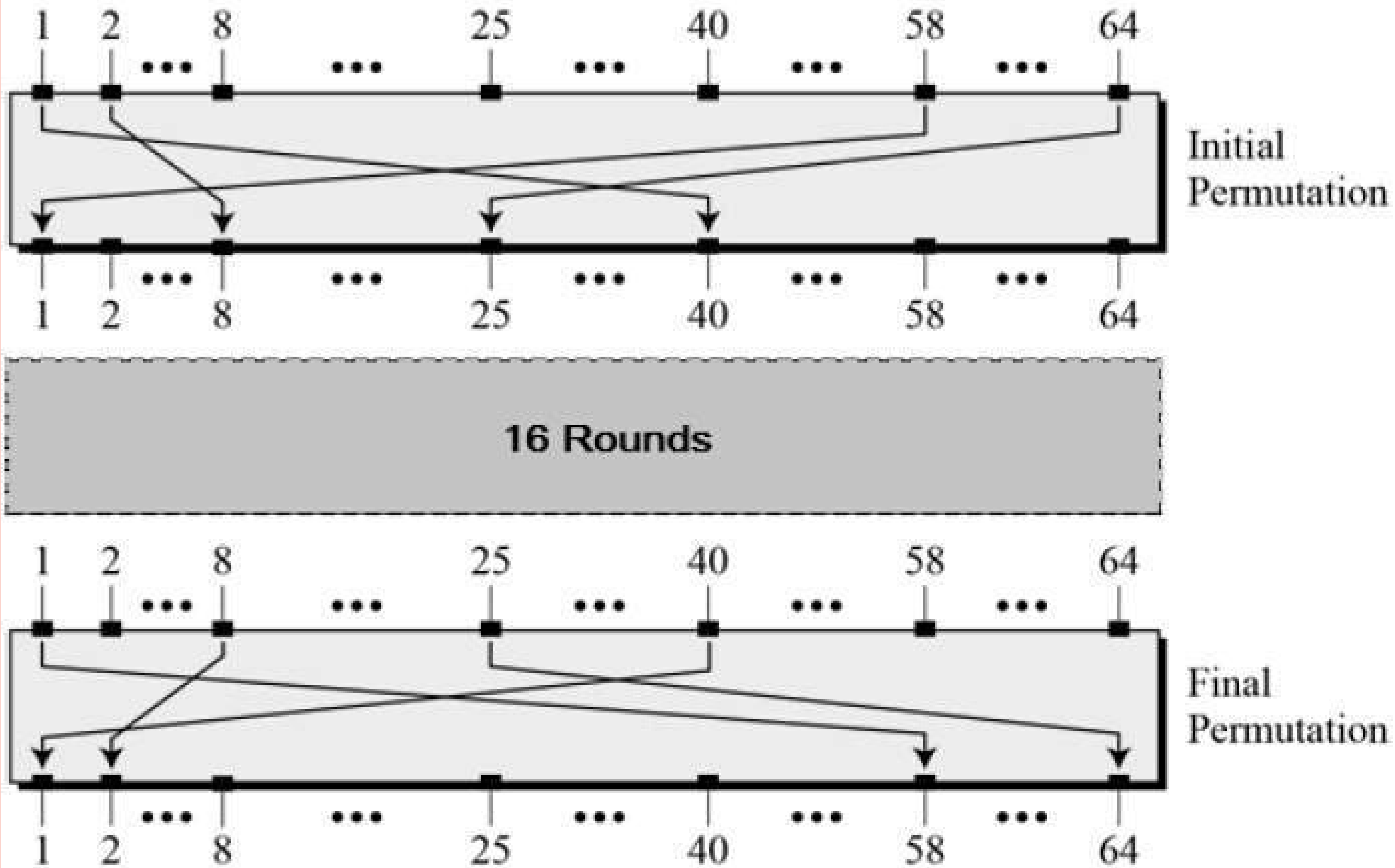
The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm

FLOW DIAGRAM:



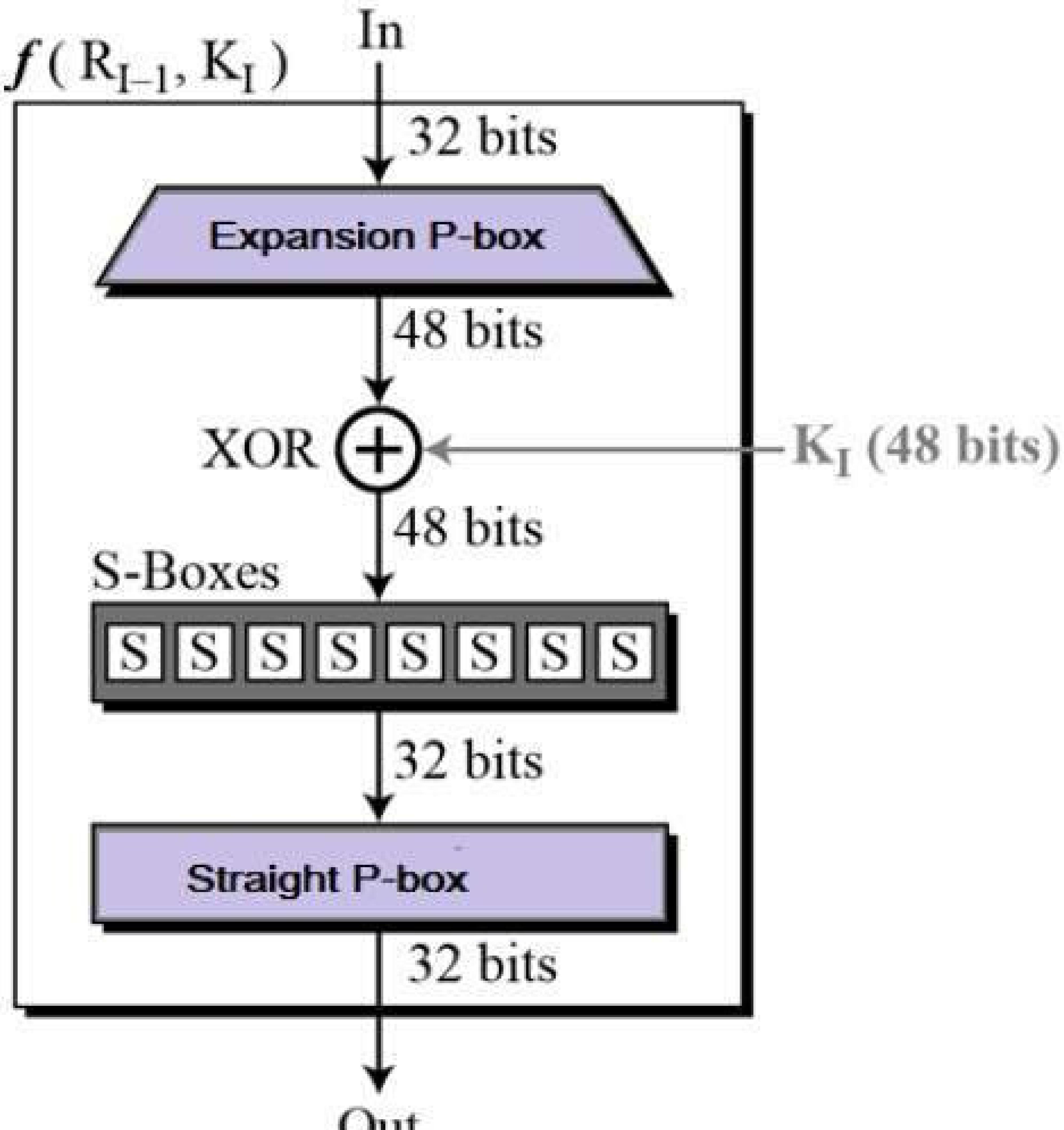
what is Initial and Final Permutation:

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 -



Round Function:

The heart of this cipher is the DES function, f. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



DES Analysis:

THE DES SATISFIES BOTH THE DESIRED PROPERTIES OF BLOCK CIPHER. THESE TWO PROPERTIES MAKE CIPHER VERY STRONG.

Avalanche effect - A small change in plaintext results in the very great change in the
. ciphertext.

Completeness - Each bit of ciphertext depends on many bits of plaintext.

During the last few years, cryptanalysis have found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.