0198CS171017

DES

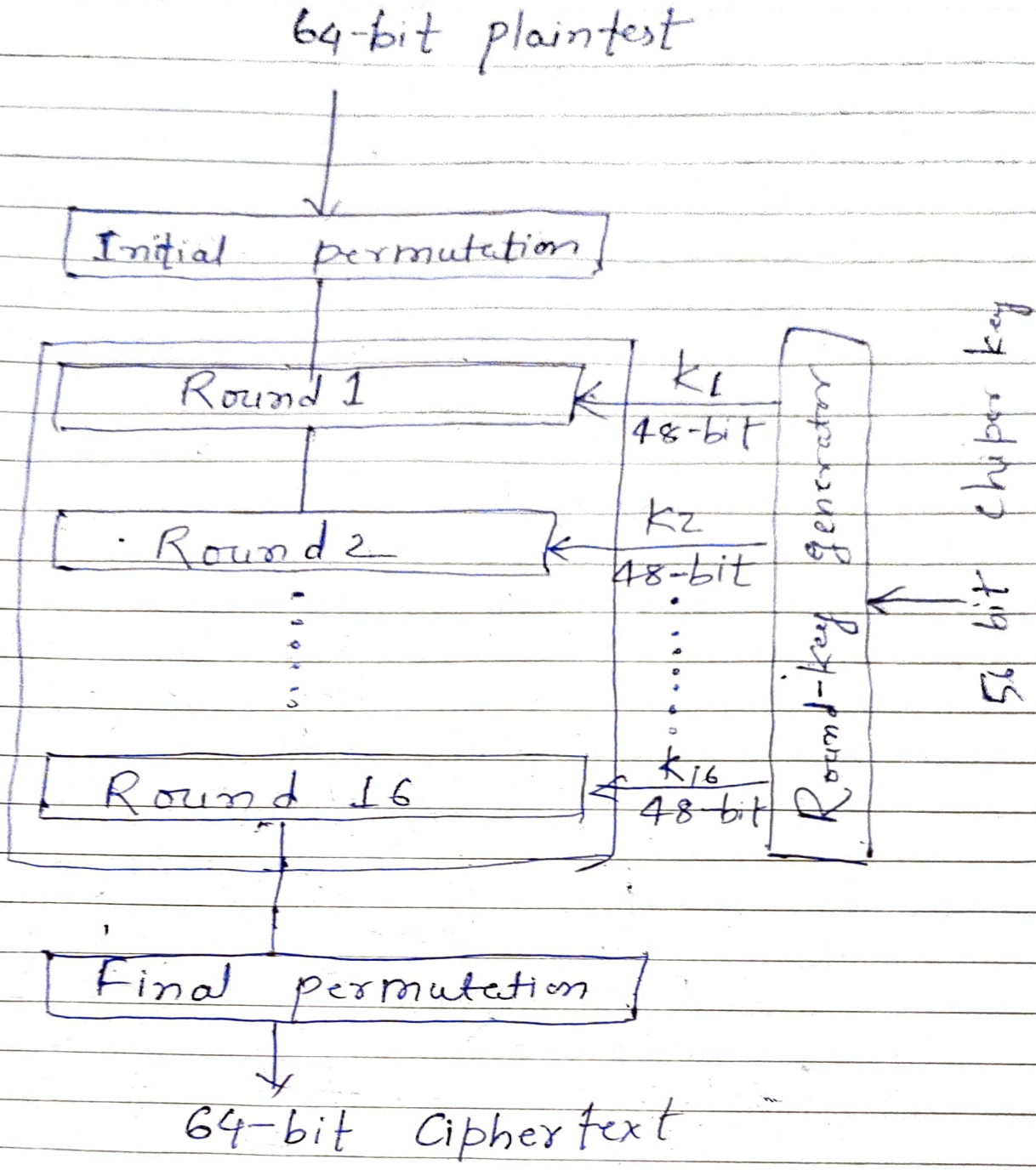
The Data Encryption standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel cipher. It uses 16 round Feist structe.

The block size is 64-bit. Though the 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. (function as check bits only)

General structure of DES is depicted in following illustration in next page.

0198C5171017



Since DES is based on the Fiestel Cipher, all that is required to specify DES is —

(1) Round function
(2) Key schedule
(3) Any additional processing - Initial & final