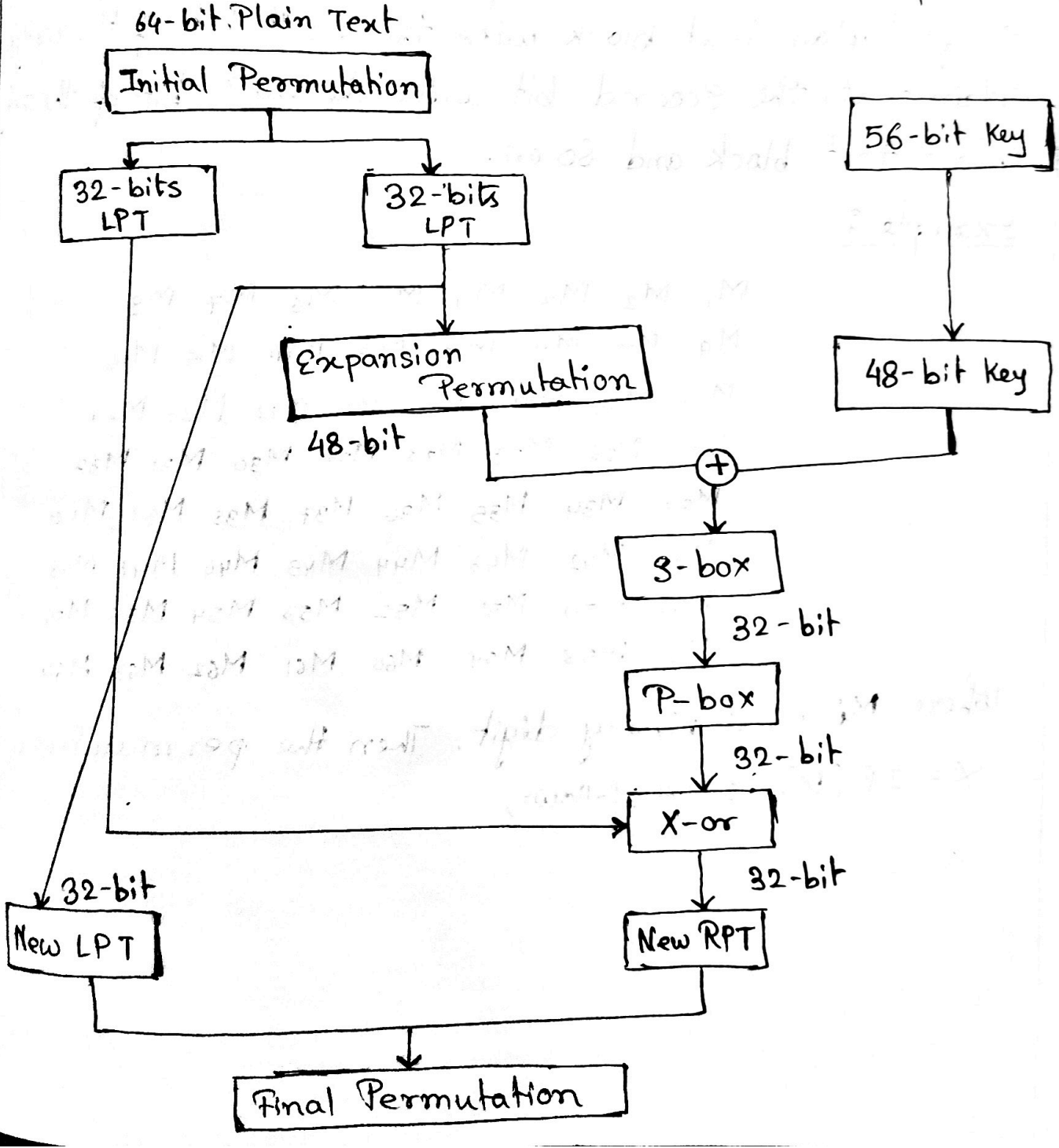
DES: (Data Encryption Standards)

The DES is a symmetric key block cipher published by the National Institute of Standards and Technology. It is based on the Feistal structure in which the plain text is seperated into two halves. It takes input as 64-bits plaintext and a 56 bit key to produce 64 bit ciphertext. Before processing the entire plaintext is separated into two pices of 32 bits each. Each piece goes through 16 rounds of operation before the final permutation is used to obtain the 64 bits ciphertext.



Initial Permutation:

The initial permutation happens only once and it happens before the first round. The initial permutation and its inverse are defined by tables. The input to a table consists of 64 bits numbered from 1 to 64. Each entry in the permutation table indicates the position of the numbered input bit in the output. This is nothing but jugglery of bit positions of the original plain text. For example the initial permutation replace the first bit of the original plain text block with the 58th bit of the original plain text, the second bit with the 50th bit of the original plain text block and so on.

Example:

M_1 M_2 M_3 M_4 M_5 M_6 M_7 M_8
M_9 M_{10} M_{11} M_{12} M_{13} M_{14} M_{15} M_{16}
M_{17} M_{18} M_{19} M_{20} M_{21} M_{22} M_{23} M_{24}
M_{25} M_{26} M_{27} M_{28} M_{29} M_{30} M_{31} M_{32}
M_{33} M_{34} M_{35} M_{36} M_{37} M_{38} M_{39} M_{40}
M_{41} M_{42} M_{43} M_{44} M_{45} M_{46} M_{47} M_{48}
M_{49} M_{50} M_{51} M_{52} M_{53} M_{54} M_{55} M_{56}
M_{57} M_{58} M_{59} M_{60} M_{61} M_{62} M_{63} M_{64}

Where M_i is a binary digit. Then the permutation $X = IP(M)$, is as follows,

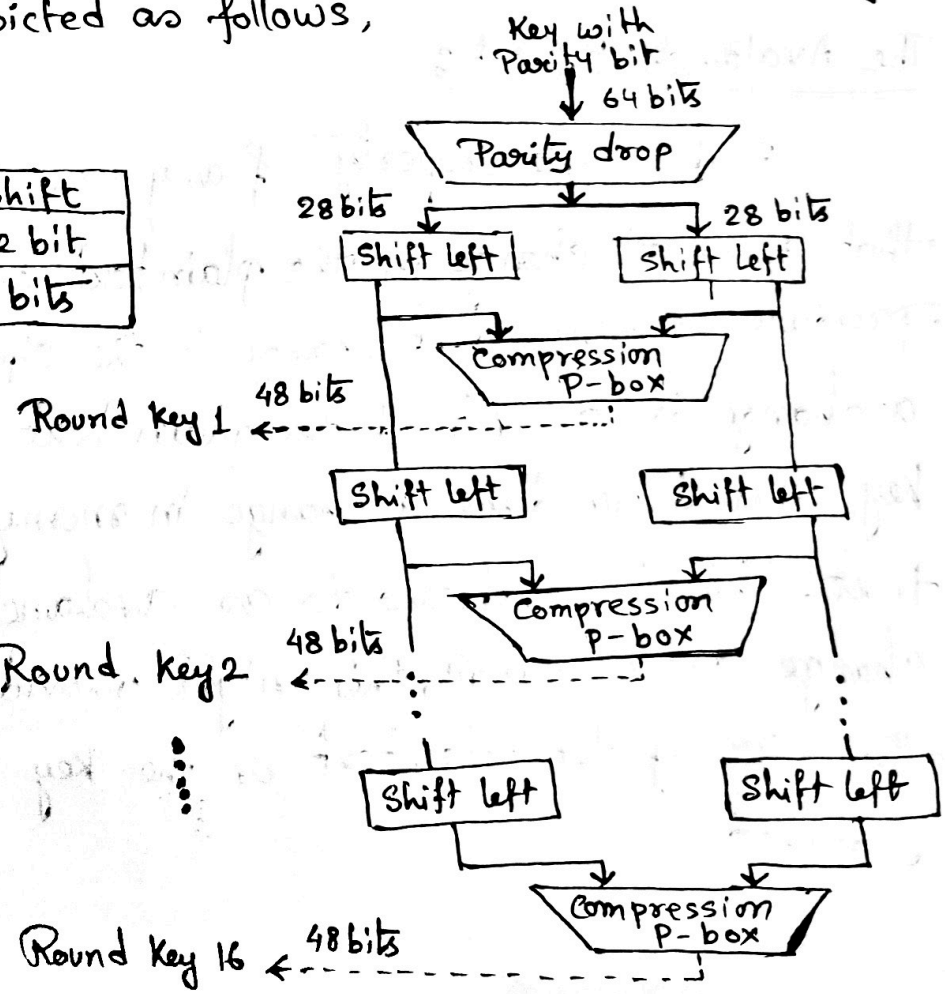
M_{58}	M_{50}	M_{42}	M_{34}	M_{26}	M_{18}	M_{10}	M_2
M_{60}	M_{52}	M_{44}	M_{36}	M_{28}	M_{20}	M_{12}	M_4
M_{62}	M_{54}	M_{46}	M_{38}	M_{30}	M_{22}	M_{14}	M_6
M_{64}	M_{56}	M_{48}	M_{40}	M_{32}	M_{24}	M_{16}	M_8
M_{57}	M_{49}	M_{41}	M_{33}	M_{25}	M_{17}	M_9	M_1
M_{59}	M_{51}	M_{43}	M_{35}	M_{27}	M_{19}	M_{11}	M_3
M_{61}	M_{53}	M_{45}	M_{37}	M_{29}	M_{21}	M_{13}	M_5
M_{63}	M_{55}	M_{47}	M_{39}	M_{31}	M_{23}	M_{15}	M_7

If we take the inverse permutation $Y = IP^{-1}(X) = IP^{-1}(IP(M))$, it can be seen that the original ordering of the bits is restored.

Key Generation: The round-key generation creates sixteen 48 bit keys out of 56 bit cipher key. The process of key generation is depicted as follows,

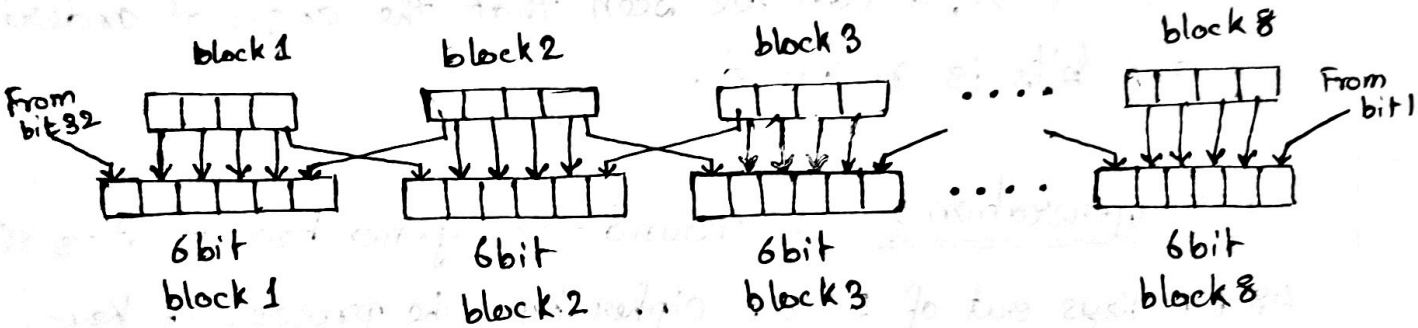
Shifting rule

Rounds	Shift
1, 2, 9, 16	One bit
Other	2 bits



Expansion Permutation:

After the initial permutation, we have two 32-bit plain text called left plain text (LPT) and right plain text (RPT). During the expansion permutation, the RPT is expanded from 32 bits to 48 bits. This happens as the 32-bits RPT is divided into 8 blocks with each block ~~Containing~~ consisting of 4 bits. Then each 4 bits block is expanded to a corresponding 6-bit block. i.e ior per 4 bit block, 2 more bits are added.



The Avalanch Effect:

A desirable property of any encryption algorithm is that a small change in the plaintext or the key should produce a significant change in the ciphertext. In particular a change in one bit of the plain text or one bit of the key should produce a change in many bits of the cipher text. This is reffered to as avalanch effect. If the change were small, this might provide a way to reduce the size of the plaintext or the key space to be searched.

The Strength of DES:

With a key length of 56 bits, there are 2^{56} possible keys, which is approximately 7.2×10^{16} keys. Thus on the face of it, a brute-force attack appears impractical. Assuming that on average half the keyspace has to be searched, a single machine performing DES encryption per micro second would take more than a thousand years to break the cipher.

DES finally and definitirely proved insecure in 1998 when the Electronic Frontier foundation announced that it had broken DES encryption using a special purpose "DES cracker" machine. The attack took less than three days.