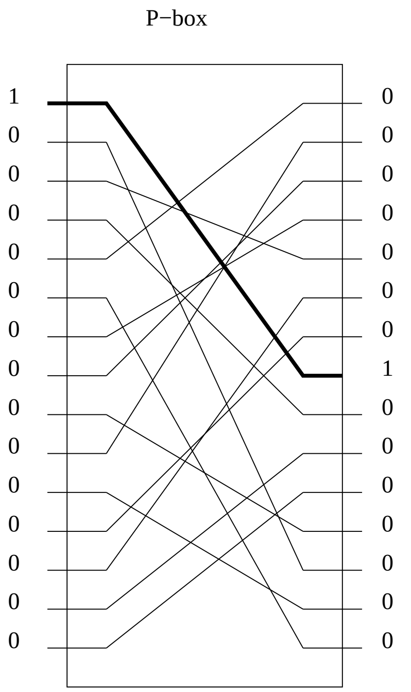
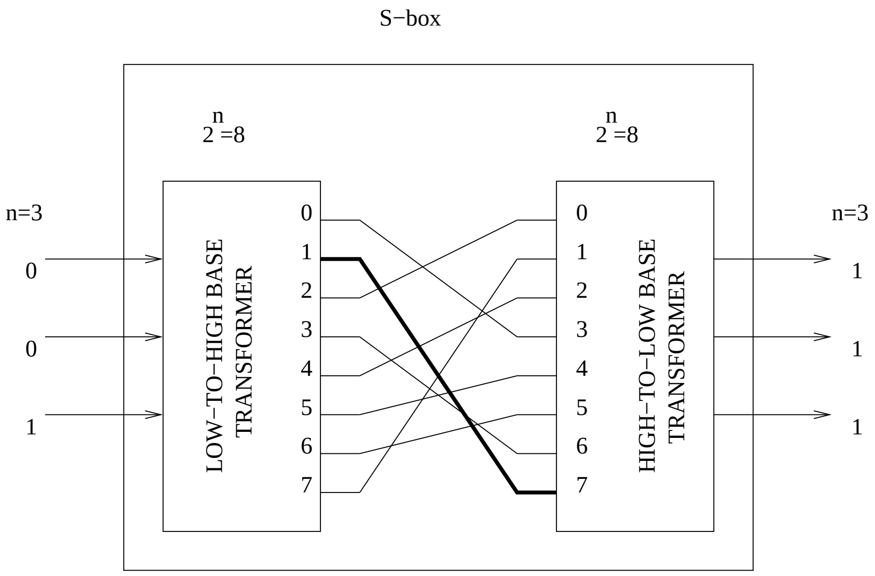
IBM's Lucifer Cipher

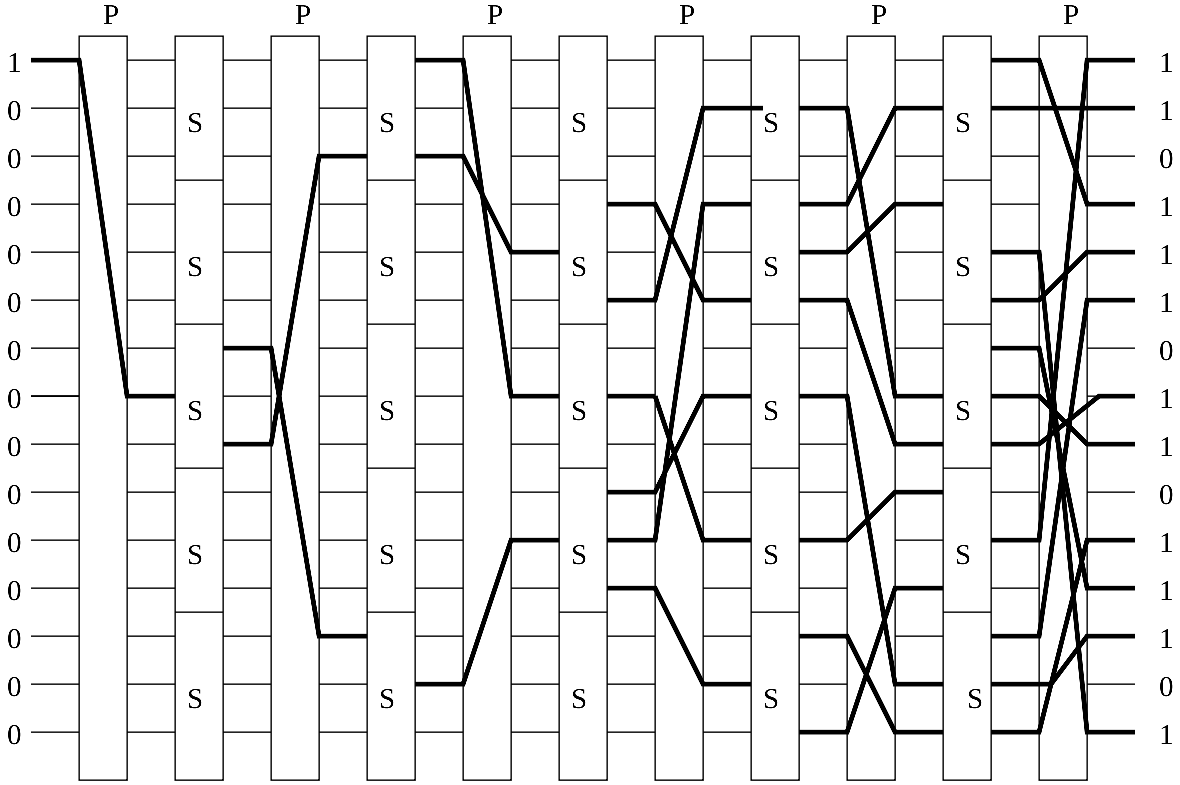
IBM's Lucifer system. This system uses permutations (transpositions) on large blocks for the mixing transformation, and substitution on small blocks for confusion.

Since this system was set up in hardware, they called the chips which did the permutation "P-boxes" and those that did the substitution "S-boxes."





The Lucifer system simply consisted of a number of P and S boxes in alternation.


P
P
P
P
P
P
S
S
S
S
S
1
0
0
0
0
0
0
0
0
0
0
0
0
0
0
1
1
0
1
1
1
0
1
1
0
1
1
1
0
1