Back to TOC

3.3.4 The P-Box Permutation in the Feistel Function

The last step in the Feistel function shown in Figure 4 is labeled "Permutation with P-Box". The permutation sequence is shown below. [It looks like a table, but it is not — as explained below]

P-Box Permutation							
15	6	19	20	28	11	27	16
0	14	22	25	4	17	30	9
1	7	23	13	31	26	2	8
18	12	29	5	21	10	3	24

- This permutation 'table' says that the 0^{th} output bit will be the 15^{th} bit of the input, the 1^{st} output bit the 6^{th} bit of the input, and so on, for all of the 32 bits of the output that are obtained from the 32 bits of the input.

- Do NOT associate any meaning with the row-organization of the table — except for the following: Each row of the table tells us how to select the input bits for the output byte corresponding to the row. For example, for the second output byte, the first entry in the second row means that the 0^{th} bit of the second output byte — meaning the 8^{th} bit of the output — will be the 0^{th} bit of the 32-bit input. *Note that bit indexing is 0-based — as it would be in your Perl or Python script*