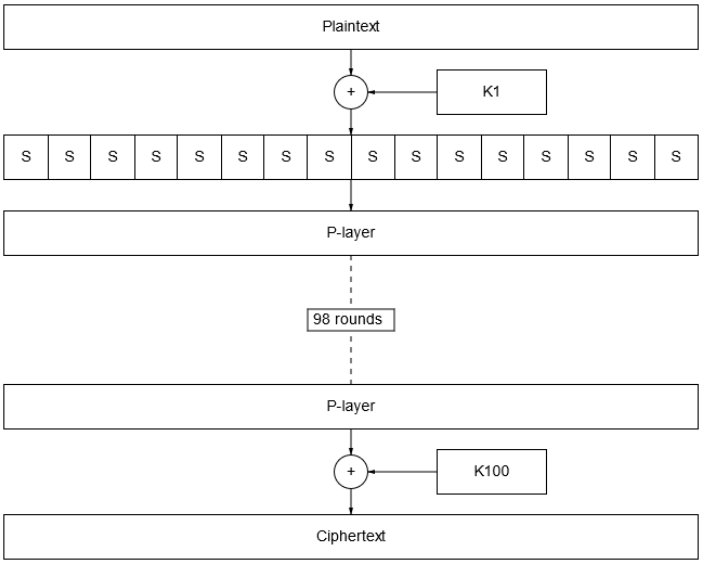
Problem 5. «Unsecure SP-network»

Bob heard about the SP-network, and decided to make his own cipher on this base, so that Carol would not be able to read his correspondence with Alice. The block size was chosen 32 bits. He made S-boxes of size 2×2 and P-layer used the part of secret key. Recall that P is an arbitrary linear transformation $P : \mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$, i. e. $P(x \oplus y) = P(x) \oplus P(y)$ for any $x, y \in \mathbb{F}_2^{32}$.

In addition to this, there is secret key $K \in \mathbb{F}_2^{128}$. Using it Bob determined

$$K^i = (K_{32(i \mod 4)+1}, \ldots, K_{32(i \mod 4)+32})$$

of length 32 for all $i \in \{1, \ldots, 100\}$. Here is the scheme of the cipher:



The i-th round of the cipher is as follows:

$$r_i(x) = P(S(x_1 \oplus K_1^i, x_2 \oplus K_2^i), S(x_3 \oplus K_3^i, x_4 \oplus K_4^i), \ldots, S(x_{31} \oplus K_{31}^i, x_{32} \oplus K_{32}^i)), x \in \mathbb{F}_2^{32}$$

The encrypted message (ciphertext) is

$$c = K^{100} \oplus r_{99}(r_{98}(\ldots r_1(m))),$$

where m is the initial message (plaintext), $m = (m_1, \ldots, m_{32})$, where $m_i \in \mathbb{F}_2$.

However, he soon discovered that Carol could read his correspondence with Alice without any problems if she had known some 100 random pairs of plaintext and ciphertext. How is this possible?