



## Problem 2. «TwinPeaks»

On Bob's smartphone there is a program that encrypts messages with the algorithm **TwinPeaks**. It works as follows:

1. It takes an input message  $P$  that is a hexadecimal string of length 32 and represents it as a binary word  $X$  of length 128.
2. Then  $X$  is divided into four 32-bits words  $a, b, c, d$ .
3. Then 6 iterations of the following transformation are applied:

$$(a, b, c, d) \leftarrow (a + c + S(c + d), a + b + d + S(c + d), a + c + d, b + d + S(c + d)),$$

where  $S$  is a secret permutation from  $\mathbb{F}_2^{32}$  to itself and  $+$  denotes the coordinate-wise sum modulo 2.

4. The word  $Y$  is obtained as a concatenation of  $a, b, c, d$ .
5. Finally,  $Y$  is converted to the hexadecimal string  $C$  of length 32. The algorithm gives  $C$  as the ciphertext for  $P$ .

Agent Cooper caught the ciphertext  $C = 59A0D027D032B394A0A47A9ED19C98A8$  send from Bob to Alice and decided to decrypt it.

In order to solve this problem agent Cooper captured also Bob's smartphone with **TwinPeaks** realization! [Here](#) it is. Now Cooper (and you too) can encrypt any messages with **TwinPeaks** but still can not decrypt any one.

Help Cooper to decrypt  $C$ .