# Problem 4. «TwinPeaks2»

Bob realized that his last year cipher `TwinPeaks` (NSUCRYPTO-2017) is not secure enough and modified it. He considerably increased the number of rounds and made rounds more complicated. New Bob's cipher works as follows.

A message $X$ is represented as a binary word of length 128. It is divided into four 32-bit words $a, b, c, d$ and then the following round transformation is applied 48 times:

$$(a, b, c, d) \leftarrow (b, c, d, a \oplus S_3(S_1(b) \oplus S_2(b \wedge \neg c \oplus c \vee d) \oplus S_1(d))),$$

Here $S_1, S_2, S_3$ are secret permutations over 32-bit words; $\neg$, $\wedge$, $\vee$, $\oplus$ are binary bitwise "NOT', "OR", "AND", "XOR" respectively (the operations are listed in descending order of priority). The concatenation of the final $a, b, c, d$ is the resulting ciphertext $Y$ for the message $X$.

Agent Cooper again wants to read Bob's messages! He caught the ciphertext

$$Y = \texttt{DEB239852F1B47B005FB390120314478}$$

and captured also Bob's smartphone with the `TwinPeaks2` implementation! Here it is. Now Cooper (and you too) can encrypt any messages with `TwinPeaks2` but still can not decrypt any one.

Help Cooper to decrypt $Y$.

**Remark.** The ciphertext is given in hexadecimal notation, the first byte is `DE`.