# Problem 4. «TwinPeaks3»

As Bob's previous cipher `TwinPeaks2` (NSUCRYPTO-2018) was broken again, he finally decided to read some books on cryptography. His new cipher is now inspired by practical ciphers, while the number of rounds was reduced a bit for better performance.

Not only the best techniques were adopted by Bob, but also he decided to enhance his cipher by security through obscurity, so the round functions are now unknown. The only thing known about these functions is that they are the same for odd and even rounds.

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 32 times:

$$(a, b, c, d) \leftarrow (b, c, d, a \oplus (F_i(b, c, d)))$$
$$F_i = F_1 \text{ for odd rounds and } F_i = F_2 \text{ for the rest.}$$

Here $F_1$ and $F_2$ are secret functions accepting three 32-bit words and returning one word; and $\oplus$ is the binary bitwise XOR. 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

$$Y = \texttt{e473f19a247429ab33b66268d57dd241}$$

(the ciphertext is given in hexadecimal notation, the first byte is `e4`).

He was also able to gain access to Bob's testing server with encryption and decryption routines, using the secret key. Here it is. Unfortunately, the version of software available on this server is not final. So, the decryption routine is incomplete and only uses keys in the reverse order, which is not sufficient for decryption:

$$(a, b, c, d) \leftarrow (b, c, d, a \oplus (F_i(b, c, d)))$$
$$F_i = F_2 \text{ for odd rounds and } F_i = F_1 \text{ for the rest.}$$

The server can also process multiple blocks of text at a time: they will be processed one-by-one and then concatenated, as in the regular ECB cipher mode of operation. Ciphertexts and plaintexts are given and processed by the server in hexadecimal notation.

Help Cooper to decrypt $Y$.