Problem 8. «Biometric key»

Iris is one of the most reliable biometric characteristics of a human. While measuring let us take 128-bit biometric image of an iris. As in reality, we suppose that two 128-bit biometric images of *the same human* can differ not more than by 10–20%, while biometric images of *different people* have differences at least 40–60%.

Let a key k be an arbitrary 8-bit vector. It can be represented in hexadecimal notation. For example, `e2` = 11100010. We suppose that the key is a pin-code that should be used in order to get access to the bank account of a client.

To avoid situation when malefactor can steal the key of a some client and then be able to get an access to his account, the bank decided to combine usage of the key with biometric authentication of a client by iris-code. The following scheme of covering the key with biometric data was proposed:

1) on registration of a client take 128-bit biometric image $b_{template}$ of his iris;

2) extend 8-bit key k to 128-bit string s using Hadamard encoding, i. e. if $k = (k_1, \ldots, k_8)$, where $k_i \in \mathbb{F}_2$, then s is the vector of values of the Boolean function $f(x_1, \ldots, x_7) = k_1x_1 \oplus \ldots \oplus k_7x_7 \oplus k_8$, where $\oplus$ is summing modulo 2;

3) save the vector $c = b_{template} \oplus s$ on the smart-card and give it to the client. A vector c is called *biometrically encrypted key*.

To get an access to his account a client should

1) take a new 128-bit biometric image b of his iris;

2) using information from the smart-card count 128-bit vector s' as $s' = b \oplus c$;

3) decode s' to 8-bit vector k' using Hadamard decoding procedure.

Then the bank system checks: if $k' = k$ then the client is authenticated and the key is correct; hence bank provides an access to the account of this client. Otherwise, if $k' \neq k$ then bank signals about an attempt to get illegal access to the bank account.

The problem. One day a person, say X, came to the bank and tried to get an access to the bank account of Alice using the smart-card. This may be noticed that

person X was in hurry and may be a little bit nervous. Suddenly, another person, say Y, appeared in the bank and declared loudly: "Please stop any operation! I am Alice! My smart-card was stolen."

Bank clerk, say Claude, stopped all operations. In order to solve the situation he took new biometric images b^X and b^Y of persons X and Y respectively, and with smart-card containing vector c leaved his post for consultations with bank specialists.

When Claude came back, he already knew who was Alice. He wanted to stop the other person and call to police but that person has already disappeared. So, can you solve this problem too? Who was real Alice? Determine her 8-bit key k. You can use the data b^X, b^Y and c presented on the picture. It is known also that the key of Alice contains odd number of ones.

Remark. The vector of values of a Boolean function f in n variables is a binary vector $(f(x^0), f(x^1), \ldots, f(x^{2^n-1}))$ of length 2^n, where $x^0 = (0, \ldots, 0, 0)$, $x^1 = (0, \ldots, 0, 1)$, $\ldots$, $x^{2^n-1} = (1, \ldots, 1, 1)$, ordered by lexicographical order; for example, the vector of values of the function $f(x_1, x_2) = x_1 \oplus x_2 \oplus 1$ is equal to $(1001) =$ `9`. The vector of values of the function $f(x_1, \ldots, x_7) = x_1 \oplus x_2 \oplus 1$ is `ffff ffff 0000 0000 0000 0000 ffff ffff`.