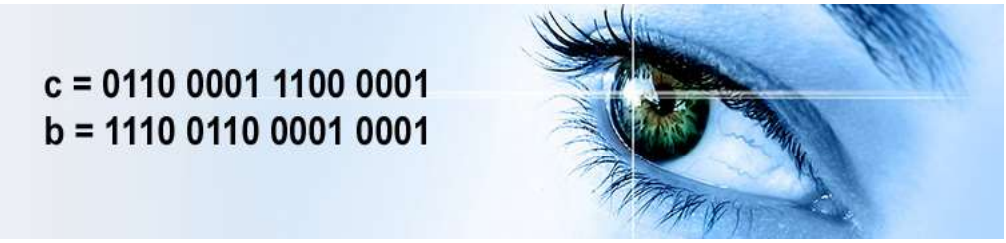
Problem 6. «Biometric pin-code»

Iris is one of the most reliable biometric characteristics of a human. While measuring let us take 16-bit vector from the biometric image of an iris. As in reality, we suppose that two 16-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 5-bit vector. We suppose that the key is a pin-code that should be used in order to get an 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 16-bit biometric image $b_{template}$ of his iris;

2) extend 5-bit key k to 16-bit string s using Hadamard encoding, i. e. if $k = (k_1, \ldots, k_5)$, where $k_i \in \{0, 1\}$, then s is the vector of values of the Boolean function $f(x_1, \ldots, x_4) = k_1x_1 \oplus \ldots \oplus k_4x_4 \oplus k_5$, 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 16-bit biometric image b of his iris;

2) using information from the smart-card count 16-bit vector s' as $s' = b \oplus c$;

3) decode s' to the 5-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. Find the 5-bit k of Alice if you know her smart-card data c and a new biometric image b (both are given on the picture).

Remark. Vector of values of a Boolean function f in 4 variables is a binary vector $(f(x^0), f(x^1), \ldots, f(x^{15}))$ of length 16, where $x^0 = (0, 0, 0, 0)$, $x^1 = (0, 0, 0, 1)$, …, $x^{15} = (1, 1, 1, 1)$, ordered by lexicographical order; for, example, vector of values of the function $f(x_1, x_2, x_3, x_4) = x_3 \oplus x_4 \oplus 1$ is equal to (1010101010101010).