International Students' Olympiad in Cryptography - 2016 First round NSUCRYPTO Section A


## Problem 1. «Cipher from the pieces»

Recover the original message, splitting the figure into equal pieces such that each color occurs once in every piece.


## Problem 2.《Get an access»

To get an access to the safe one should put 20 non-negative integers in the following cells. The safe will be opened if and only if the sum of any two numbers is even number $k$, such that $4 \leqslant k \leqslant 8$, and each possible sum occurs at least once. Find the sum of all these numbers.


International Students' Olympiad in Cryptography - 2016

## Problem 3. «Find the key»

The key of a cipher is the set of positive integers $a, b, c, d, e, f, g$, such that the following relation holds:

$$
a^{3}+b^{3}+c^{3}+d^{3}+e^{3}+f^{3}+g^{3}=2016^{2017}
$$

Find the key!

International Students' Olympiad in Cryptography - 2016 First round NSUCRYPTO

## Problem 4. «Labyrinth»

Read the message hidden in the labyrinth!


## Problem 5. «System of equations»

Analyzing a cipher Caroline gets the following system of equations in binary variables $x_{1}, x_{2}, \ldots, x_{16} \in\{0,1\}$ that represent the unknown bits of the secrete key:

$$
\left\{\begin{array}{l}
x_{1} x_{3} \oplus x_{2} x_{4}=x_{5}-x_{6}, \\
x_{14} \oplus x_{11}=x_{12} \oplus x_{13} \oplus x_{14} \oplus x_{15} \oplus x_{16}, \\
\left(x_{8}+x_{9}+x_{7}\right)^{2}=2\left(x_{6}+x_{11}+x_{10}\right), \\
x_{13} x_{11} \oplus x_{12} x_{14}=-\left(x_{16}-x_{15}\right), \\
x_{5} x_{1} x_{6}=x_{4} x_{2} x_{3}, \\
x_{11} \oplus x_{8} \oplus x_{7}=x_{10} \oplus x_{6}, \\
x_{6} x_{11} x_{10} \oplus x_{7} x_{9} x_{8}=0, \\
\left(\frac{x_{12}+x_{14}+x_{13}}{\sqrt{2}}\right)^{2}-x_{15}=x_{16}+x_{11}, \\
x_{1} \oplus x_{6}=x_{5} \oplus x_{3} \oplus x_{2}, \\
x_{6} x_{8} \oplus x_{9} x_{7}=x_{10}-x_{11}, \\
2\left(x_{5}+x_{1}+x_{6}\right)=\left(x_{4}+x_{3}+x_{2}\right)^{2}, \\
x_{11} x_{13} x_{12}=x_{15} x_{14} x_{16} .
\end{array}\right.
$$

Help Caroline to find the all possible keys!
Remark. If you do it in analytic way (without computer calculations) you get twice more scores.

## 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 $40-60 \%$.

$$
c=0110000111000001
$$ b = 1110011000010001



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 $b_{\text {template }}$ of his iris;
2) extend 5 -bit key $k$ to 16 -bit string $s$ using Hadamard encoding, i. e. if $k=$ $\left(k_{1}, \ldots, k_{5}\right)$, where $k_{i} \in\{0,1\}$, then $s$ is the vector of values of the Boolean function $f\left(x_{1}, \ldots, x_{4}\right)=k_{1} x_{1} \oplus \ldots \oplus k_{4} x_{4} \oplus k_{5}$, where $\oplus$ is summing modulo 2 ;
3) save the vector $c=b_{\text {template }} \oplus s$ 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 $s^{\prime}$ as $s^{\prime}=b \oplus c$;
3) decode $s^{\prime}$ to the 5 -bit vector $k^{\prime}$ using Hadamard decoding procedure.

Then the bank system checks: if $k^{\prime}=k$ then the client is authenticated and the key is correct; hence bank provides an access to the account of this client. Otherwise, if $k^{\prime} \neq k$ 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
$\left(f\left(x^{0}\right), f\left(x^{1}\right), \ldots, f\left(x^{15}\right)\right)$ of length 16 , where $x^{0}=(0,0,0,0), x^{1}=(0,0,0,1), \ldots, x^{15}=(1,1,1,1)$, ordered by lexicographical order; for, example, vector of values of the function $f\left(x_{1}, x_{2}, x_{3}, x_{4}\right)=$ $x_{3} \oplus x_{4} \oplus 1$ is equal to (1010101010101010).

