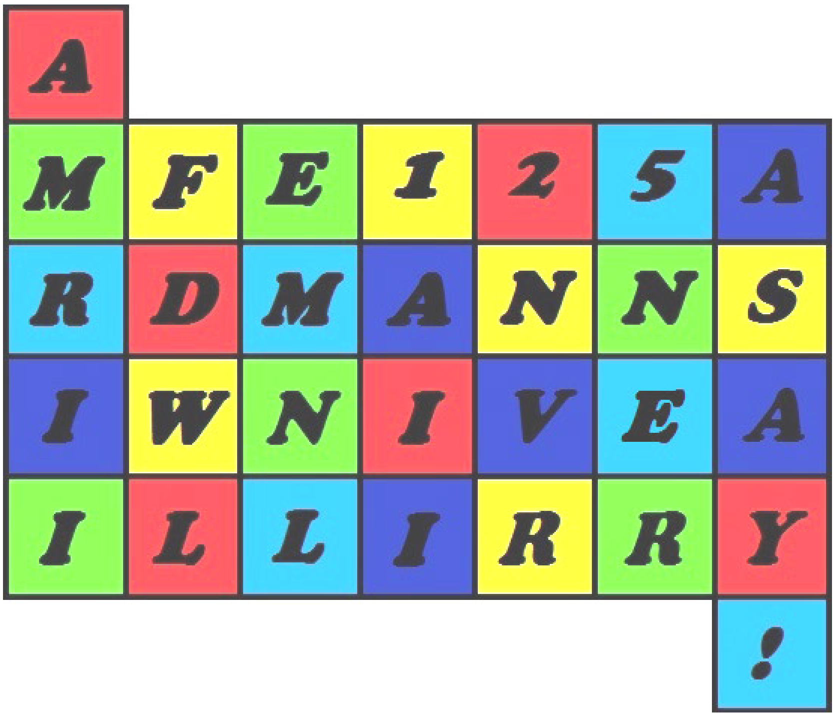
Problem 1. «Cipher from the pieces»

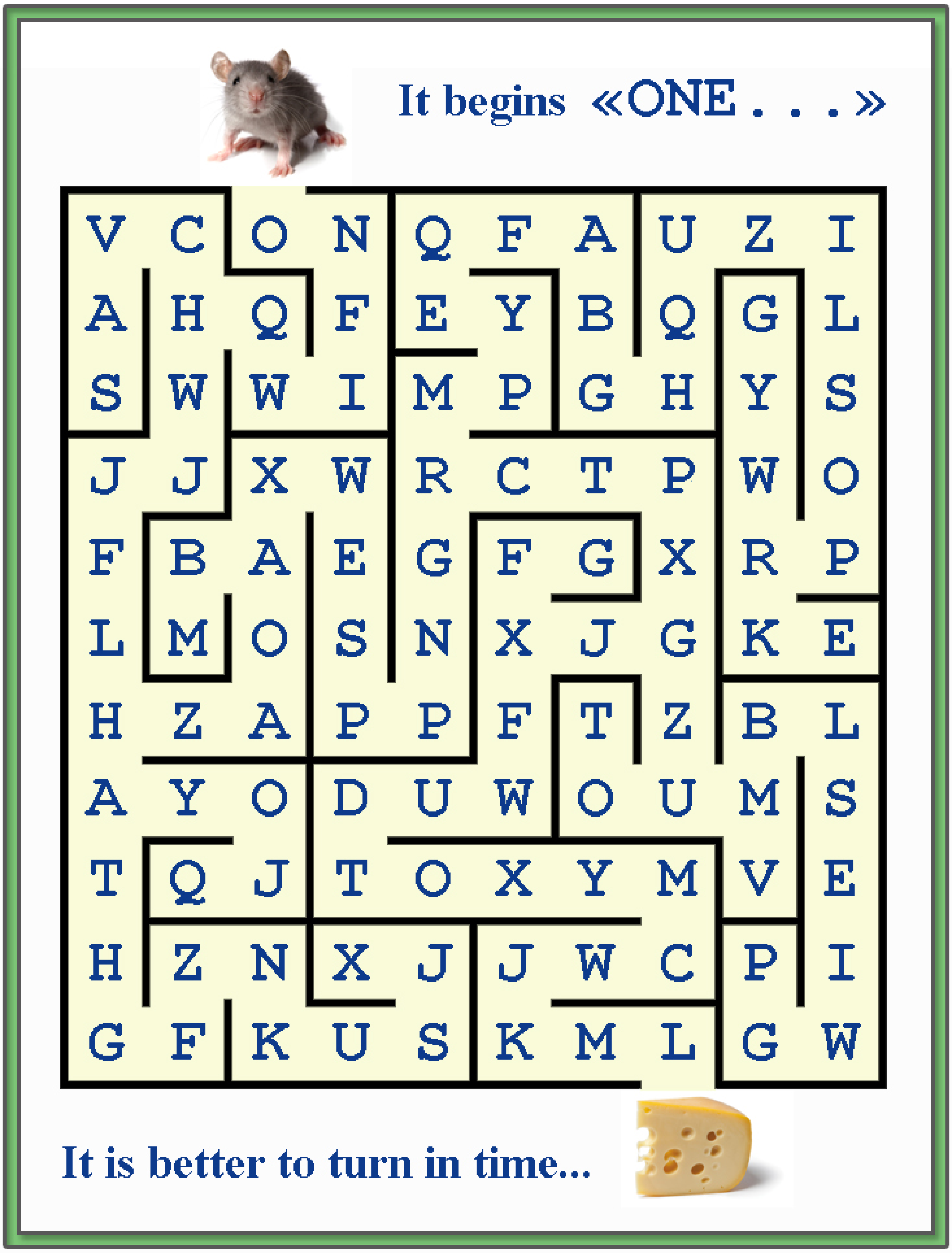
Recover the original message, splitting the figure into equal pieces such that each color occurs once in every piece.



A						
M	F	E	1	2	5	A
R	D	M	A	N	N	S
I	W	N	I	V	E	A
I	L	L	I	R	R	Y
						!

Problem 2. «Labyrinth»

Read the message hidden in the labyrinth!



It begins «ONE . . . »

V	C	O	N	Q	F	A	U	Z	I
A	H	Q	F	E	Y	B	Q	G	L
S	W	W	I	M	P	G	H	Y	S
J	J	X	W	R	C	T	P	W	O
F	B	A	E	G	F	G	X	R	P
L	M	O	S	N	X	J	G	K	E
H	Z	A	P	P	F	T	Z	B	L
A	Y	O	D	U	W	O	U	M	S
T	Q	J	T	O	X	Y	M	V	E
H	Z	N	X	J	J	W	C	P	I
G	F	K	U	S	K	M	L	G	W

It is better to turn in time...

Problem 3. «Quadratic functions»

Alice and Bob are going to use the following pseudorandom binary sequence $u = \{u_i\}$, $u_i \in \mathbb{F}_2$:

- $u_1, \ldots, u_n$ are initial values;
- $u_{i+n} = f(u_i, u_{i+1}, \ldots, u_{i+n-1})$, where

$$f \in Q_n = \{a_0 \oplus \bigoplus_{i=1}^{n} a_i x_i \oplus \bigoplus_{1\leq i<j\leq n} a_{ij} x_i x_j \mid a_0, a_i, a_{ij} \in \mathbb{F}_2\}.$$

Suppose that you have intercepted the elements $u_t, u_{t+1}, \ldots, u_{t+k-1}$ of a sequence for some t. Is it possible to uniquely reconstruct the elements

$$u_{t+k}, u_{t+k+1}, u_{t+k+2}, \ldots$$

provided $k \leqslant cn$, where c is a constant independent on n?

Problem 4. «System of equations»

Analyzing a cipher Caroline gets the following system of equations in binary variables $x_1, x_2, \ldots, x_{16}$ that represent the unknown bits of the secrete key:

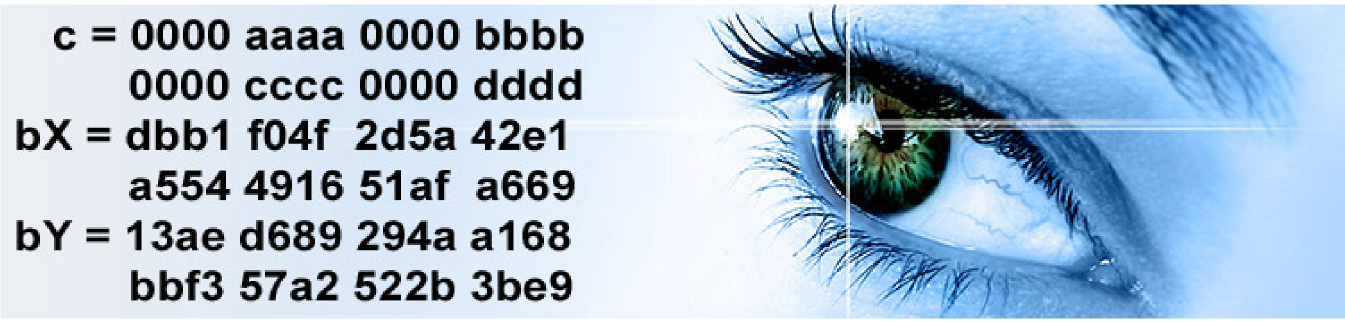
$$\begin{cases} x_1x_3 \oplus x_2x_4 = x_5 - x_6, \\ x_{14} \oplus x_{11} = x_{12} \oplus x_{13} \oplus x_{14} \oplus x_{15} \oplus x_{16}, \\ (x_8 + x_9 + x_7)^2 = 2(x_6 + x_{11} + x_{10}), \\ x_{13}x_{11} \oplus x_{12}x_{14} = -(x_{16} - x_{15}), \\ x_5x_1x_6 = x_4x_2x_3, \\ x_{11} \oplus x_8 \oplus x_7 = x_{10} \oplus x_6, \\ x_6x_{11}x_{10} \oplus x_7x_9x_8 = 0, \\ \left(\frac{x_{12}+x_{14}+x_{13}}{\sqrt{2}}\right)^2 - x_{15} = x_{16} + x_{11}, \\ x_1 \oplus x_6 = x_5 \oplus x_3 \oplus x_2, \\ x_6x_8 \oplus x_9x_7 = x_{10} - x_{11}, \\ 2(x_5 + x_1 + x_6) = (x_4 + x_3 + x_2)^2, \\ x_{11}x_{13}x_{12} = x_{15}x_{14}x_{16}. \end{cases}$$

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 5. «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%.



```
 c = 0000 aaaa 0000 bbbb
     0000 cccc 0000 dddd
bX = dbb1 f04f  2d5a 42e1
     a554 4916 51af  a669
bY = 13ae d689 294a a168
     bbf3 57a2 522b 3be9
```

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 $x^0 = (0, \ldots, 0, 0)$, $x^1 = (0, \ldots, 0, 1)$, …, $x^{2^n-1} = (1, \ldots, 1, 1)$, 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 $(1001) = \texttt{9}$. The vector of values of the function $f(x_1, \ldots, x_8) = x_1 \oplus x_2 \oplus 1$ is `ffff ffff 0000 0000 0000 0000 ffff ffff`.

Problem 6. «Secret sharing»

Alena, Boris and Sergey developed the following secret sharing scheme to share a password $P \in \mathbb{F}_2^{32}$ into three parts to collectively manage money through online banking.

- Vectors $v_i^a, v_i^b, v_i^s \in \mathbb{F}_2^{32}$ and values $c_i^a, c_i^b, c_i^s \in \mathbb{F}_2$ are randomly generated for all $i = 1, \ldots, 32$.
- Vectors v_i^a, v_i^b, v_i^s are known to all participants of the scheme.
- Values $c_i^a, c_i^b, c_i^s \in \mathbb{F}_2$ are known only to Alena, Boris and Sergey respectively.
- Then the secret password P is calculated by the rule

$$P = \bigoplus_{i=1}^{32} c_i^a v_i^a \oplus \bigoplus_{i=1}^{32} c_i^b v_i^b \oplus \bigoplus_{i=1}^{32} c_i^s v_i^s.$$

What is the probability that Alena and Boris together can not get any information about the password P? What is the probability that they are able without Sergey to get a guaranteed access to online banking using not more than 23 attempts?

Problem 7. «Protocol»

Alena and Boris developed a new protocol for establishing session keys. It consists of the following three steps:

1. The system has a common prime modulus p and a generator g. Alena and Boris have their own private keys $\alpha_a \in \mathbb{Z}_{p-1}$, $\alpha_b \in \mathbb{Z}_{p-1}$ and corresponding public keys $P_a = g^{\alpha_a} \mod p$, $P_b = g^{\alpha_b} \mod p$.

2. To establish a session key Alena generates a random number $R_a \in \mathbb{Z}_{p-1}$, computes $X_a = (\alpha_a + R_a) \mod (p-1)$ and sends it to Boris. Then Boris generates his random number R_b, computes X_b in the same way as Alena and sends it back to her.

3. Alena computes the session key in the following way:

$$K_{a,b} = (g^{X_b} P_b^{-1})^{R_a} \mod p.$$

Bob computes the session key in the following way:

$$K_{b,a} = (g^{X_a} P_a^{-1})^{R_b} \mod p.$$

How can an attacker Evgeniy compute any future session key between Alena and Boris, if he steals the only one session key $K_{a,b}$?