Problem 1. «An encryption table»

Mary read a book about history of cryptography and found an interesting cipher. It encrypts messages consisting of letters from English alphabet (26 letters from «A» to «Z»). For encryption one needs to choose a codeword of length n in English alphabet and construct an encryption table T of the size $n \times n$ in the following way. The first column is filled by the letters of the chosen codeword. Then each row is filled by letters in alphabetical order starting with the letter in the first cell.

A message is encrypted letter by letter. The ciphertext for a message of length t consists of t ordered pairs of integers (i, j), where i is the row number and j is the column number in the table T of a current letter.

	1	2	3	4
1	M	N	O	P
2	A	B	C	D
3	R	S	T	U
4	Y	Z	A	B

An example. Let the codeword be MARY. Then the ciphertext for the message CRYPTO is (2,3) (3,1) (4,1) (1,4) (3,3) (1,3).
But for the message RSA the ciphertext could be (3,1) (3,2) (2,1) or (3,1) (3,2) (4,3).

Mary has encrypted a sentence using this cipher. As a result she got the following ciphertext, where all spaces in the text are saved:

(8,1) (7,8) (1,1) (2,6) (5,5) (7,5) (11,7) (7,8) (5,7) (8,11) (9,1) (3,1)
(6,1) (7,5) (7,6) (7,5) (1,10) (2,5) (7,5) (7,4) (2,7) (11,2) (3,9) (1,11)
(6,3) (7,8) (7,5) (11,6) (7,9) (1,5) (9,8) (1,4) (7,5)
(3,1) (5,9) (6,4) (8,8) (5,10) (7,5) (3,11) (9,1) (1,8) (7,8) (7,5) (9,10)

Try to read it if you know that the codeword was of length 11, the encryption table contained all English letters and a fragment of it was:

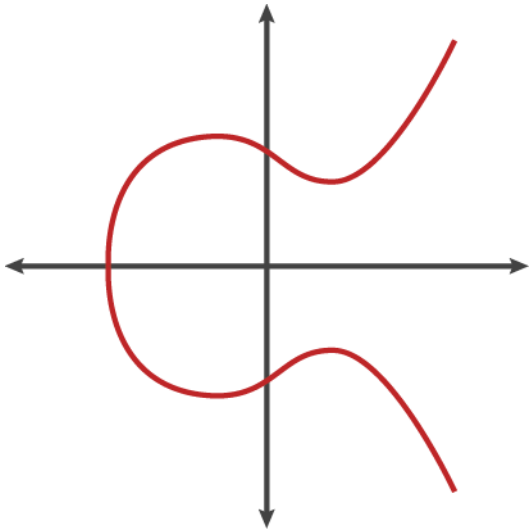
M	N	O
S	T	U
R	S	T

Problem 2. «Crypto street»

You are walking near Novosibirsk State University and its new hostels with a secret message in hands. Could you read it?

Problem 3. «An elliptic curve»

Bob develops a new cryptosystem based on elliptic curves. An elliptic curve is the set of points (x, y) satisfying the equation $y^2 = x^3 + ax + b$ for some fixed real numbers a, b. For the system Bob chooses the curve $y^2 = x^3 + 56x + 6$ and needs to find all integer points of this curve, i. e. points (x, y), where x and y are both integer numbers. Help Bob to do this!



Problem 4. «Give an answer»

Two young friends Roman and Stephan use some method to communicate with each other without exchanging common secrete keys. Their messages consist of letters from the following extended English alphabet: «A», «B», ..., «Z», «0», «1», ..., «9», « », «?», «.».

Here there is a fragment of their recent dialog:

Stephan to Roman: `Q2A?4FV4GOCX4IASOXF?K4AJSKN?CXK4NOSK6T`
Roman to Stephan: `AXOLNJ42?K4QOXUJ4IN4804JA7S.`

They had supposed that nobody could understand their dialog but surprisingly Stephan recieved the message

`2?K4AJVKN2LXKS4OF42OM4SAQ7KX`

from their classmate Anton. And Stephan easily understood it!

Try to read the chat!
And what would be your answer?

Problem 5. «A binary tape»

A cipher machine works with a binary infinite tape that starts with an input word of length n and all its other elements are zero. The machine encrypts an input word and writes the result instead of it.

The cipher machine can do two operations:

1) copy any symbol of the tape to other position;

2) apply some fixed one-to-one function $S : \mathbb{F}_2^m \to \mathbb{F}_2^m$ to the first m symbols, where $\mathbb{F}_2 = \{0, 1\}$.

Find the conditions for S such that the machine can perform any bijective mapping of words of length n.

Examples of operations.

1) For instance, the machine can copy the third symbol to the fifth place:

1	1	**1**	0	**0**	0	1	1	1	...

the result will be

1	1	1	0	**1**	0	1	1	1	...

2) Let m be 3 and $S(x, y, z) = (x, y, x \oplus z)$; applying S to the first three symbols:

1	**1**	**1**	0	0	0	1	1	1	...

the result will be

1	**1**	**0**	0	0	0	1	1	1	...

Problem 6. «Covering radius»

In order to protect a new block cipher against some attack based on S-box approximations Alice needs to solve the following problem.

Let $\mathbb{F}_2^n$ be a n-dimensional vector space over the field $\mathbb{F}_2 = \{0, 1\}$. Let $n = 2k$, where k is a positive integer. Evaluate the covering radius and describe the metrical complement of the linear subspace spanned by rows of the following $k \times n$ matrix:

$$M = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & \ldots & 0 & 1 \\ 0 & 1 & \ldots & 0 & 0 & \ldots & 1 & 0 \\ \ldots & \ddots & & & & \iddots & & \ldots \\ 0 & \ldots & 1 & 0 & 0 & 1 & \ldots & 0 \\ 0 & \ldots & 0 & 1 & 1 & 0 & \ldots & 0 \end{pmatrix}$$

Remark I. Recall several definitions and notions. A set $L \subseteq \mathbb{F}_2^n$ is called a *linear subspace* if for every $x, y \in L$ the sum $x \oplus y$ is also in L. The *Hamming distance* $d(x, y)$ between vectors $x, y \in \mathbb{F}_2^n$ is defined as the number of positions where they differ, i. e. $d(x, y) = |\{i \mid x_i \neq y_i\}|$. The Hamming distance from a vector y to a subset $X \subseteq \mathbb{F}_2^n$ is defined as $d(y, X) = \min_{x \in X} d(y, x)$. Since the distance between any two vectors is bounded by n, for an arbitrary subset X there exists the number $d(X)$ such that:

- for every $y \in \mathbb{F}_2^n$ it holds $d(y, X) \leqslant d(X)$;
- there exists a vector $z \in \mathbb{F}_2^n$ with $d(z, X) = d(X)$.

This number is called the *covering radius* of X. Set $\widehat{X} = \{z \in \mathbb{F}_2^n \mid d(z, X) = d(X)\}$ is called the *metrical complement* of X.

Remark II. Let us consider several examples:

- Let X consist of a single vector $x \in \mathbb{F}_2^n$. It is easy to see that $d(X) = n$ and $\widehat{X} = \{x \oplus \mathbf{1}\}$, where $\mathbf{1}$ is the all-ones vector;
- Let Y be a ball of radius r centered at x: $Y = \{y \in \mathbb{F}_2^n \mid d(x, y) \leqslant r\}$. One can verify that $d(Y) = n - r$ and $\widehat{Y} = \{x \oplus \mathbf{1}\}$.

Problem 7. «The machine DH-d»

Let G be a cyclic group of a large prime order q and g be a generator of G. Tom designed the machine DH-d that on input (g, g^x) outputs g^{x^d}. Here g^x is an arbitrary element of G and d is a small fixed positive integer.

Use the machine DH-d to solve the Diffie – Hellman problem, that is, find g^{xy} from (g, g^x, g^y). Suggest a solution with the minimal requests to the machine.