Problem 1. «Key sharing»

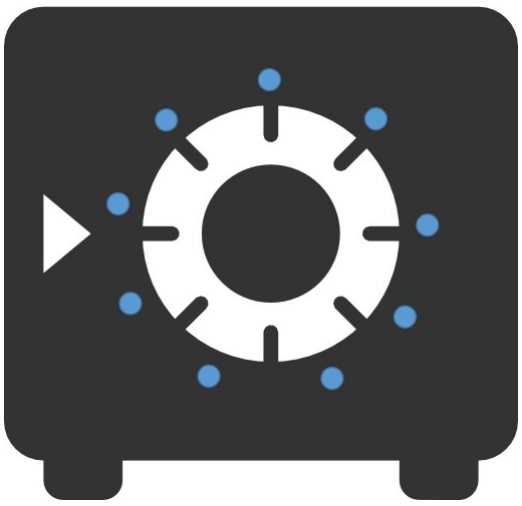
A bank safe can be opened with 9 keys inserted in its keyholes in a right order. The keyholes are arranged in a circle. The order of keys is *right* if sum of keys (each key is associated with a natural number) in every three consequent keyholes is divisible by 3.

The safe has two special features: if you insert a key in a keyhole, you can not get it back until all 9 keys are inserted; if the order of inserted 9 keys is wrong, the safe sends «SOS signal» and blocks itself.

Keys were divided between 3 persons: Alice, Bob and Caroline. Together they have a permission to open the bank safe. Their keys are the following:

- Alice: {4,14,24};
- Bob: {34,44,54};
- Caroline: {64,74,84}.

Today Alice, Bob and Caroline are going to open the safe. But one of them forgot the rule of right order for keys and has already inserted two his keys into consequent keyholes when was stopped by his friends. Prove that Alice, Bob and Caroline still are able to open the safe in this situation.



Problem 2. «RSA numbers»

RSA is one of the most popular cryptosystems with a public key. We know that it operates with two big prime numbers p and q that should be kept in secret by each user.

Eve is a malefactor that likes to steal secret RSA parameters of users and then offers to buy them via the Internet. Today she offers to buy the new pair of primes p and q satisfying the following relation:

$$p^{4x} + 4 \cdot 2015 = q^{4y} \text{ for some natural numbers } x \text{ and } y.$$

Should the clients of Eve buy these numbers?

Problem 3. «Bigrams»

Users of a some communication system send messages to each other. Every message is written in English. Eve is a malefactor who intercepts messages in this channel and replaces them with new ones. In detail she does the following: intercepts a message, removes all spaces and punctuation marks from it, splits the message into bigrams starting from the beginning. Then she makes several iterations of destruction of the message. The number of iterations is random.

All bigrams are divided into 3 types:

I. Bigram contains only vowels (i. e. `AA, EI, IO, UO, YU, ...`).
II. Bigram contains only consonants (i. e. `BN, TR, LL, PW, SD, ...`).
III. Bigram contains one vowel and one consonant (i. e. `QA, EC, HI, KO, ...`).

On each iteration Eve takes two random bigrams B_1 and B_2 of the different types and removes them from the message, at the same time she adds a new random bigram B_3 of the third type at the beginning of the message. So, if she chooses bigrams of I and II types (II and III; I and III) she will add an arbitrary bigram of III (I; II) type.

For example, the message `CRYPTO TEXT` can be transformed by Eve like this:

`CRYPTO TEXT` → `(CR)(YP)(TO)(TE)(XT)` → `(OE)(CR)(TO)(TE)` → `(FE)(TO)(TE)`

The question is the following. You know that Alice has send to Bob the message

`THE MEETING WILL TAKE PLACE AT THREE IN ‘‘EEYORE-EAGLE-BEE CREEK INN’’`

that was intercepted by Eve. She had repeated iterations of destruction until the only one bigram left. Could it be a bigram consisting of one vowel and one consonant?

Problem 4. «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 5. «Crypto street»

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

Problem 6. «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!