Problem 2. «POLY»

A/1 feladat

During a job interview, Bob was proposed to think up a small cryptosystem that operates with integers. Bob invented and implemented a complex algorithm POLY that can be represented mathematically as a polynomial. Namely, if x is a plaintext, then ciphertext y is equal to $p(x)$, where p is a polynomial with integer coefficients.

Bob's employer decided to test it. At first, he encrypted the number 20 and obtained the number 7. Secondly, he encrypted the number 15 and obtained the number 5. After that he said to Bob that there was a mistake in the implementation of the algorithm and did not hire him. What was wrong?

Problem 3. «Autumn leaves»

A/2 feladat

Read a hidden message!..

Problem 1. «A 1024-bit key»

A/3 (*) feladat

Alice has a 1024-bit key for a symmetric cipher (the key consists of 0s and 1s). Alice is afraid of malefactors, so she changes her key everyday in the following way:

1. Alice chooses a subsequence of key bits such that the first bit and the last bit are equal to 0. She also can choose a subsequence of length 1 that contains only 0.
2. Alice inverts all the bits in this subsequence (0 turns into 1 and vice versa); bits outside of this subsequence remain as they are.

Prove that the process will stop. Find the key that will be obtained by Alice in the end of the process.

Example of an operation. 11001 01101110 011... turns to 11001 10010001 011...

B/1 feladat

Problem 1. «A digital signature»

Alice uses a new digital signature algorithm that turns a text message M into a pair (M, s), where s is an integer and generated in the following way:

1. The special function h transforms M into a big positive integer $r = h(M)$.

2. The number $t = r^2$ is calculated, where $t = \overline{t_1 t_2 \dots t_n}$.

3. The signature s is calculated as $s = t_1 + t_2 + \dots + t_n$.

Bob obtained the signed message

(`Congratulations on the fifth year anniversary of NSUCRYPTO!`, 2018)

from Alice and immediately recognized that something was wrong with the signature! How did he discover it?

A remark. By $t = \overline{t_1 t_2 \dots t_n}$ we mean that $t_1, t_2, \dots, t_n$ are decimal digits and all digits over the bar form decimal number t.

Problem 4. «Timing attack»

B/2 feladat

Anton invented a ciphermachine that can automatically encrypt messages consisting of English letters. Each letter corresponds to the number from 1 to 26 by alphabetical order (1 is for `A`, 2 is for `B`, ..., 26 is for `Z`). The machine encrypts messages letter by letter. It encrypts one letter as follows.

Step 1. If the letter belongs to the special secret set of letters, the machine does not encrypt it, adds the original letter to the ciphertext, and does not go to Step 2; otherwise it goes to Step 2.

Step 2. According to the secret rule, it replaces the current letter with number k by a letter with number ℓ, where ℓ has the same remainder of division by 7, and adds this new letter to the ciphertext.

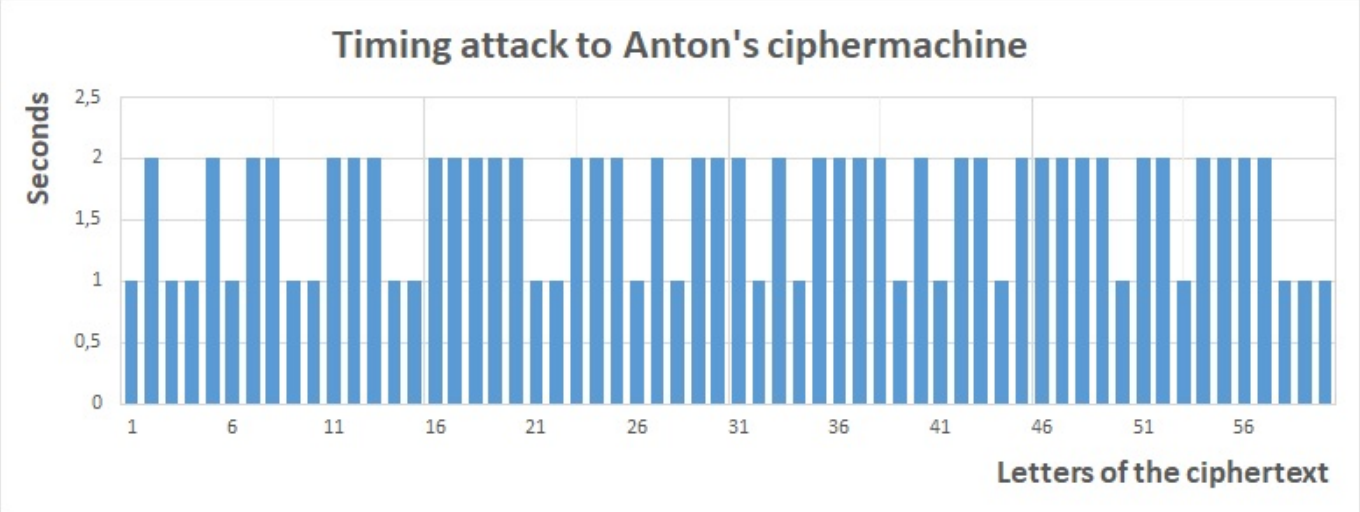
Anton's classmate Evgeny is interested in different kinds of cryptanalysis that use some physical information about the encryption process. He measured the amount of time that is required for each letter encryption by Anton's ciphermachine and found out that a timing attack can be applied to it!

He captured the ciphertext that Anton sent to his friend and were able to read the message using the information of his measurements!

Could you also decrypt the ciphertext:

```
Tois kevy is fhye tvvu xust hgvtoed iyife ngfbey!
Wvat ka rvn knvw owvnt it?
```

if you know how much time encryption of each message letter took?



B/3 (*) feladat

Problem 1. «PIN code»

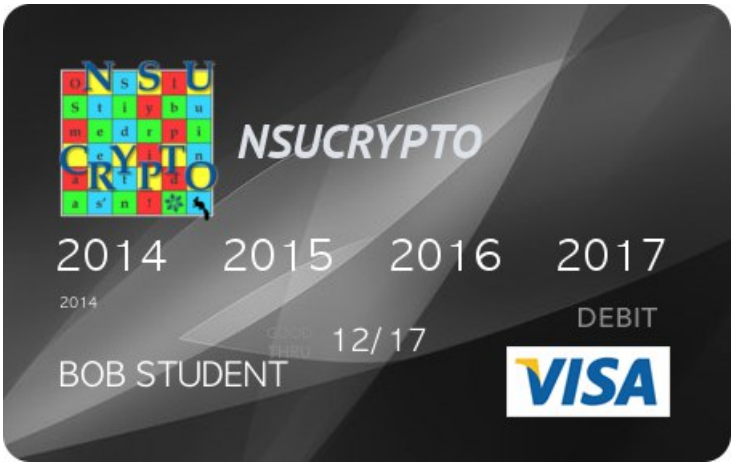
A PIN code $P = \overline{p_1 p_2 \ldots}$ is an arbitrary number consisting of a few pairwise different digits in ascending order ($p_1 < p_2 < \ldots$). Bob got his personal PIN code in the bank, but he decided that the code is not secure enough and changed it in the following way:

1. Bob multiplied his PIN code P by 999 and obtained the number $A = \overline{a_1 a_2 \ldots}$;

2. Then he found the sum of all digits of A: $a_1 + a_2 + \ldots = S = \overline{s_1 s_2 \ldots}$;

3. Finally, he took all digits (starting from 0) that are smaller than s_1, sorted them in ascending order and inserted between digits s_1 and s_2 in the number S. Resulting number P' is Bob's new PIN code. For example, if S was 345, then, after such insertion we obtain $P' = 301245$.

Find the new code P'!

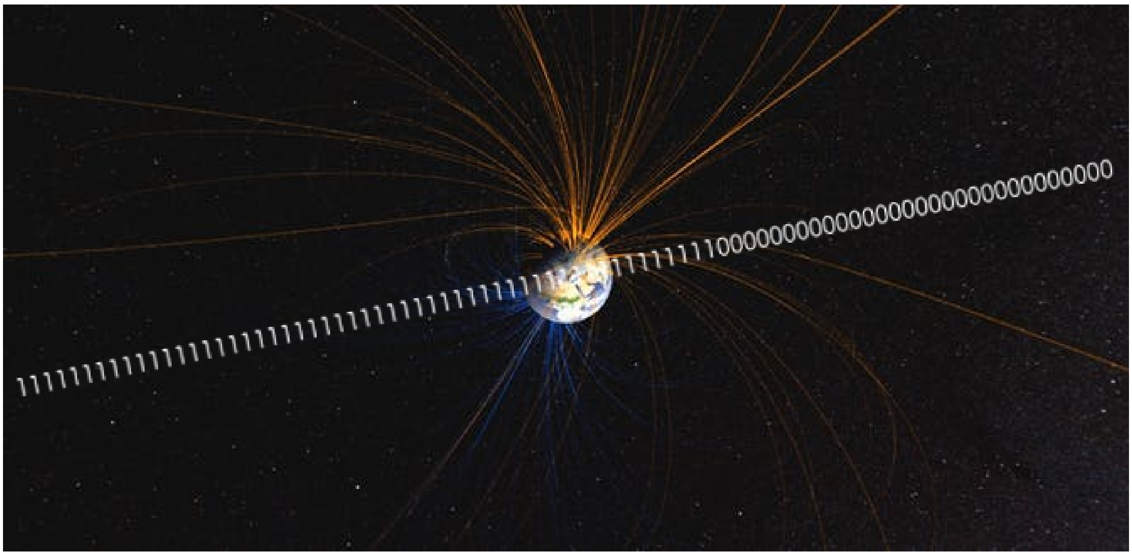


Problem 2. «The magnetic storm»

C/1 feladat

A hardware random number generator is a device that generates random sequences consisting of 0s and 1s. Unfortunately, a disturbance caused by a magnetic storm affected this random number generator. As a result, the device had generated a sequence of 0s of length k (where k is a positive integer), and then started to generate an infinite sequence of 1s.

Prove that at some point the generator will produce a number $1\ldots10\ldots0$ that is divisible by 2019.

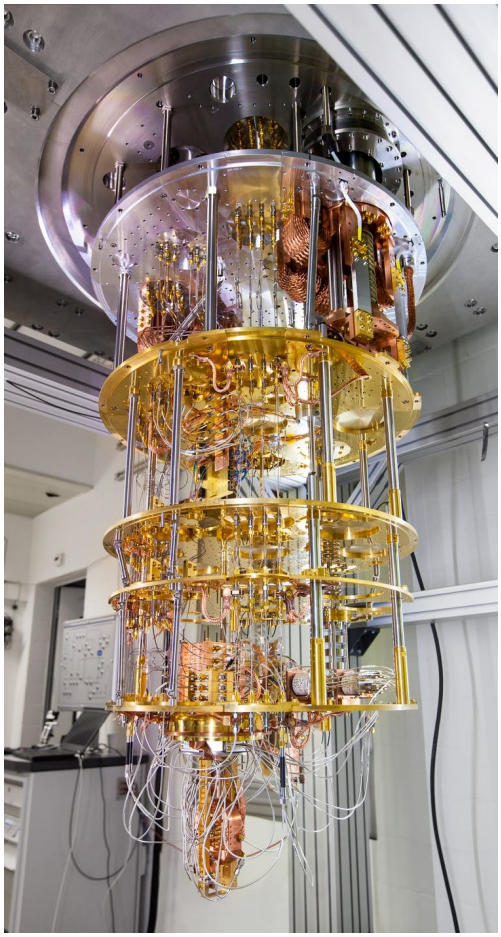


Problem 6. «A promise»

C/2 feladat

Young cryptographers, Alice, Bob and Carol, are interested in quantum computings and really want to buy a quantum computer. A millionaire gave them a certain amount of money (say, X_A for Alice, X_B for Bob, and X_C for Carol). He also made them promise that they would not tell anyone, including each other, how much money everyone of them had received.

- Could you help the cryptographers to invent an algorithm how to find out (without breaking the promise) whether the total amount of money they have, $X_A + X_B + X_C$, is enough to buy a quantum computer?
- What weaknesses does your algorithm have (if someone breaks the promise)? Does it always protect the secret of the honest participants from the dishonest ones?



IBM's 50 qubit quantum computing system

Problem 4. «Labyrinth»

C/3 (*) feladat

Read the message hidden in the labyrinth!

C/4 (*) feladat

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:

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

Help Caroline to find the all possible keys!

Remark. If you do it in analytic way (without computer calculations) you get twice more scores.