Problem 1. «PIN code»

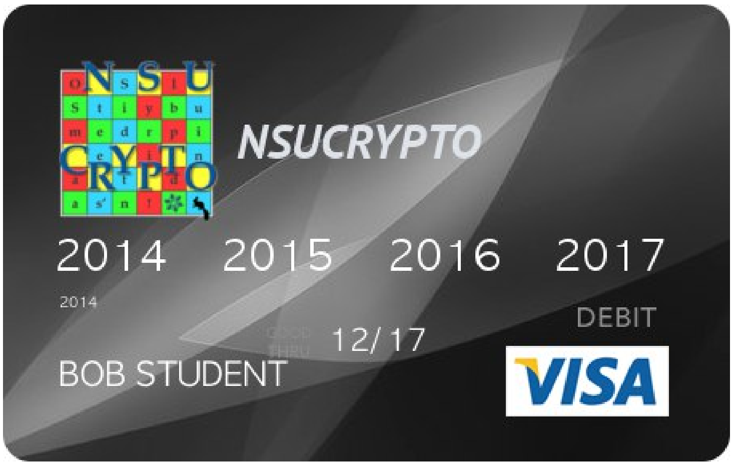
A PIN code $P = \overline{p_1 p_2 \ldots}$ is an arbitrary number consisting of a few pairwise different digits in ascending order ($p_1 < p_2 < \ldots$). Bob got his personal PIN code in the bank, but he decided that the code is not secure enough and changed it in the following way:

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. «Chests with treasure»

We have three closed chests. Some of them contain the treasures (diamonds, gold coins, bitcoins as well) but we do not know which ones. A parrot knows which chests contain the treasures and which do not; he agrees to answer to questions by «yes» or «no». He may possibly lie in his answers but not more than once. List six questions such that it is possible to deduce from the answers of the parrot which chests contain the treasures and which do not.

Problem 3. «A numerical rebus»

Buratino keeps his Golden Key in the safe that is locked with a numerical password. For secure storage of the password he replaced some digits in the password by letters (in a way that different letters substitute different digits). After replacement Buratino got the password **NSUCRYPTO17**.

Alice the Fox found out that:

- the number **NSUCRYPTO** is divisible by all integers n, where $n < 17$, and
- the difference **NSU** − **CRY** is divisible by 7.

Could she find the password?

Remark. Here we denote $\overline{ABC\dots}$ by **ABC. . . .**

Problem 4. «Timing attack»

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.

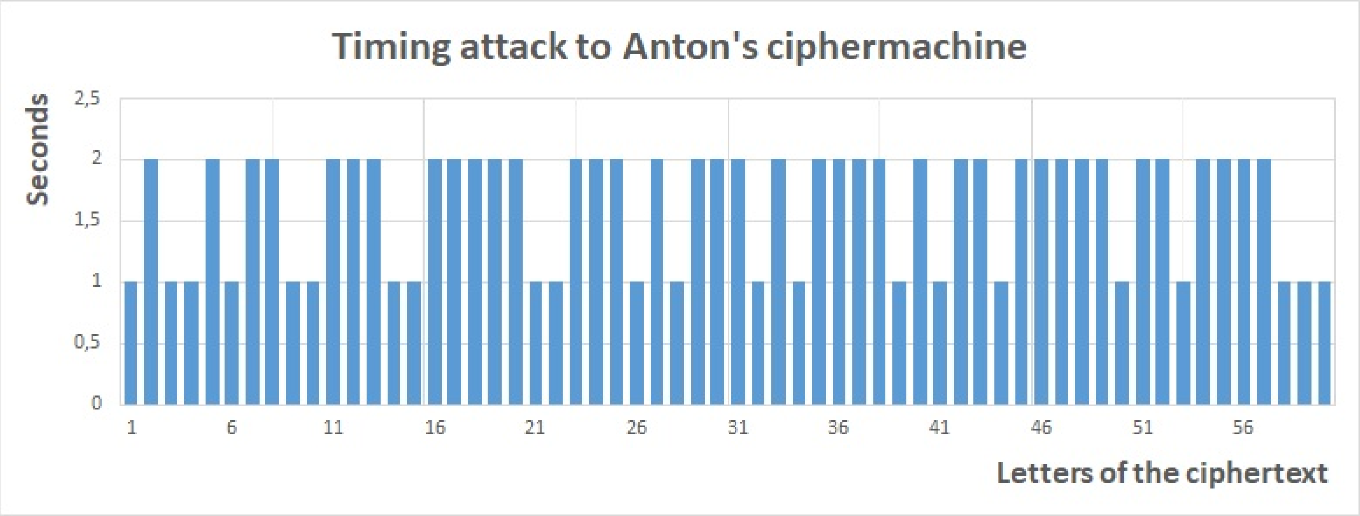
Anton's classmate Evgeny is interested in different kinds of cryptanalysis that use some physical information about the encryption process. He measured the amount of time that is required for each letter encryption by Anton's ciphermachine and found out that a timing attack can be applied to it!

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?



Problem 5. «The shortest addition chain»

In many cryptographic systems we need to calculate the value $B = A^c \bmod p$, where A is an integer, $1 \leqslant A \leqslant p-1$, c is an arbitrary positive integer, and p is a large prime number. One possible way of reducing the computational load of calculating is to minimize the total number of multiplications required to compute the exponentiation. Since the exponent in equation is additive, the problem of computing powers of the base element A can also be formulated as an addition calculation, for which addition chains are used.

An **addition chain** for an integer n is a sequence of positive integers

$$a_0 = 1, a_1, \ldots, a_{r-1}, a_r = n,$$

where r is a positive integer (that is called the **length** of the addition chain) and the following relation holds for all i, $1 \leqslant i \leqslant r$:

$$a_i = a_j + a_k \text{ for some } k, j \text{ such that } k \leqslant j < i.$$

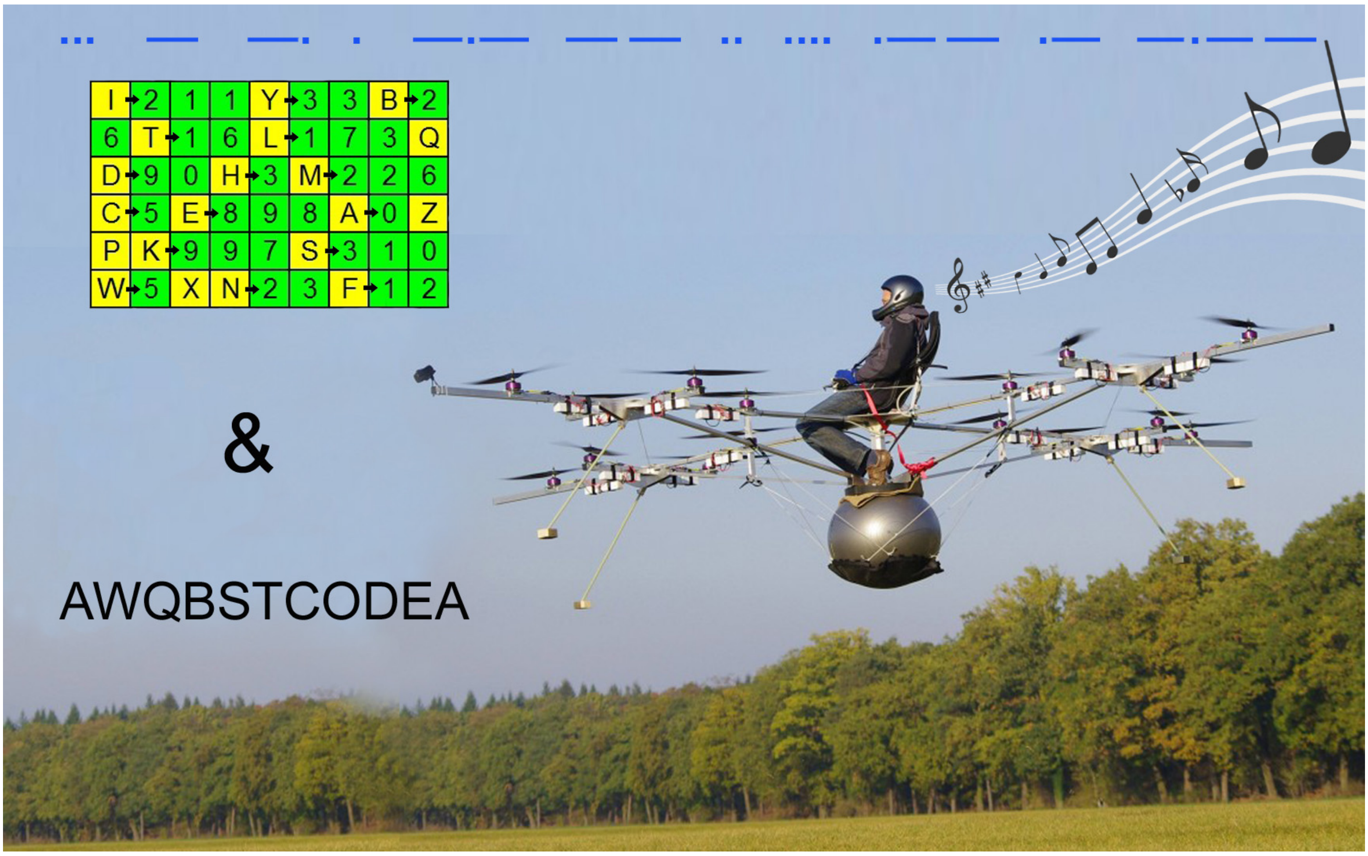
Find an addition chain of length as small as possible for the value 81, present it as a list of values and mathematically prove that it can not be shorter!

An example. For the value 15 the shortest additional chain has length 5 and its list of values is $1, 2, 3, 6, 12, 15$. So, to optimally calculate $B = A^{15} \bmod p$, one can use just five multiplications:

$$\begin{aligned} A^2 &= A \cdot A \mod p \\ A^3 &= A^2 \cdot A \mod p, \\ A^6 &= A^3 \cdot A^3 \mod p, \\ A^{12} &= A^6 \cdot A^6 \mod p, \\ A^{15} &= A^{12} \cdot A^3 \mod p. \end{aligned}$$

Problem 6. «A music lover»

As usual Alex listens to music on the way to university. He chooses it applying one secret code to the second one in his mind. Could you understand what music he is listening to right now?



I	→2	1	1	Y	→3	3	B	→2
6	T	→1	6	L	→1	7	3	Q
D	→9	0	H	→3	M	→2	2	6
C	→5	E	→8	9	8	A	→0	Z
P	K	→9	9	7	S	→3	1	0
W	→5	X	N	→2	3	F	→1	2