Problem 1. «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.

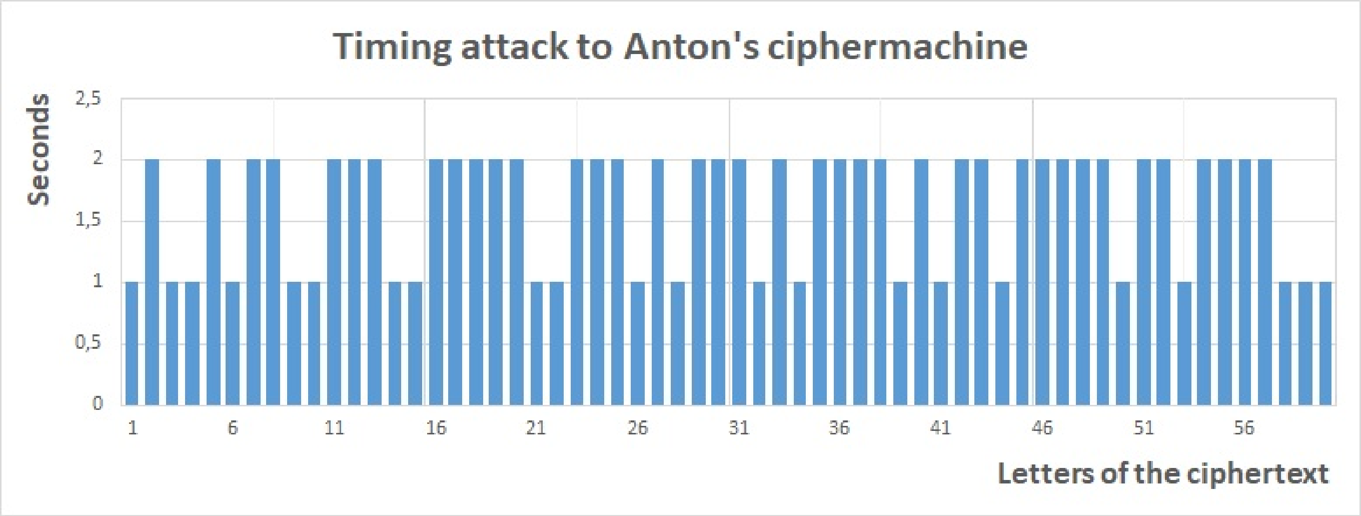
Anton's classmate Evgeny is interested in different kinds of cryptanalysis that use some physical information about the encryption process. He measured the amount of time that is required for each letter encryption by Anton's ciphermachine and found out that a timing attack can be applied to it!

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?

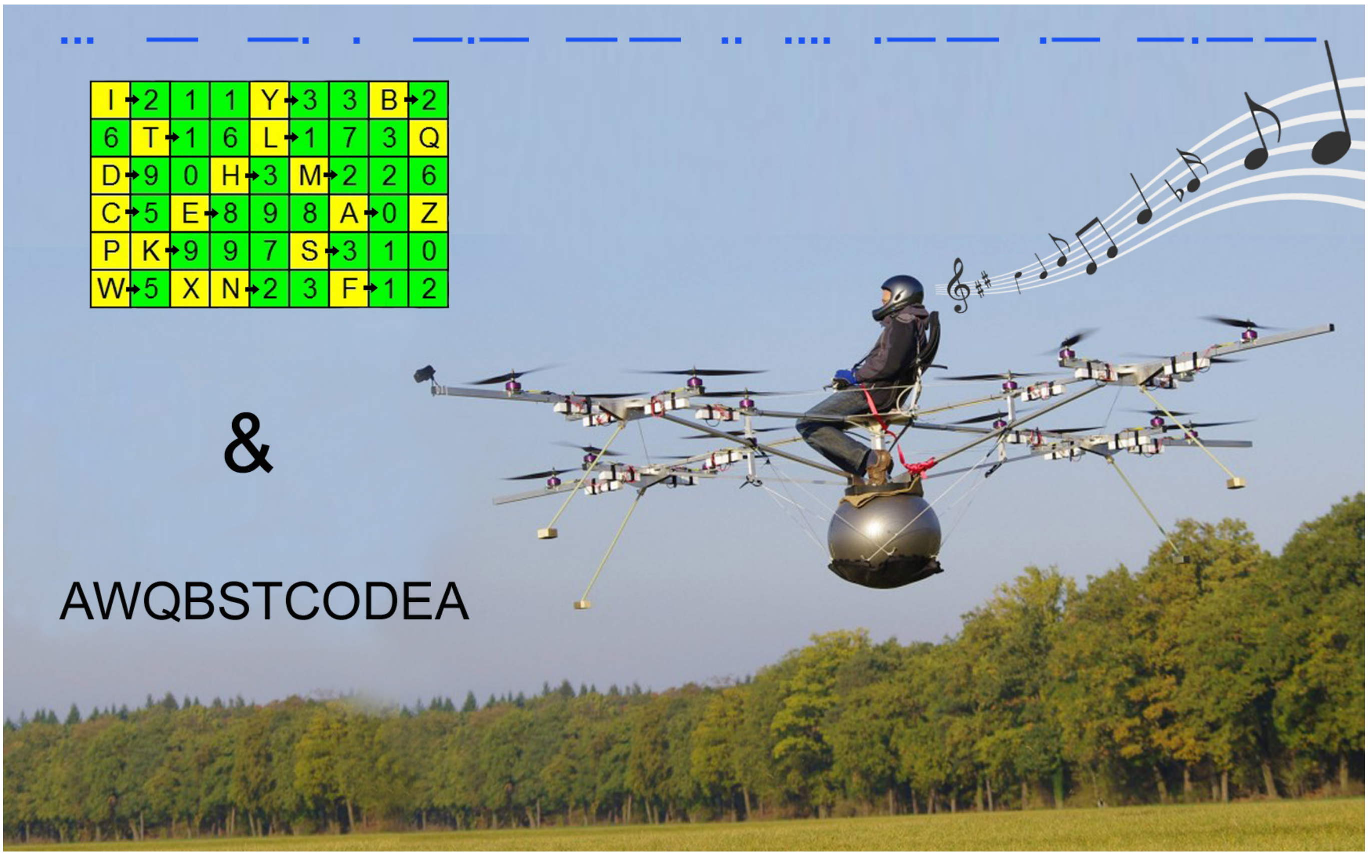


Problem 2. «Treasure chests»

We have seven 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». But he may possibly lie in his answers but not more than twice. List fifteen 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 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

&

AWQBSTCODEA

Problem 4. «An infinite set of collisions»

Bob is very interested in blockchain technology, so he decided to create his own system. He started with the construction of a hash function. His first idea for a hash function was the function H with a hash value of length 16.

It works as follows.

- Let $u_1, u_2, \ldots, u_n \in \mathbb{F}_2$ be a data representation, n is arbitrary.
- Bob calculates $z^0, \ldots, z^n \in \mathbb{F}_2^{32}$, $z^0 = (0, \ldots, 0)$, and z^{i+1} is obtained from z^i in the following way:

$$z' = \begin{cases} (z_1^i, z_2^i, \ldots, z_{16}^i, z_1^i \oplus z_{17}^i, z_2^i \oplus z_{18}^i \ldots, z_{16}^i \oplus z_{32}^i) & \text{if } u_i = 1, \\ (z_1^i \oplus z_{17}^i, z_2^i \oplus z_{18}^i, \ldots, z_{16}^i \oplus z_{32}^i, z_{17}^i, z_{18}^i, \ldots, z_{32}^i) & \text{if } u_i = 0, \end{cases}$$

$$z'' = \begin{cases} z' & \text{if } u_i \neq z'_{32}, \\ (z'_1 \oplus 1, z'_2 \oplus 1, \ldots, z'_{32} \oplus 1) & \text{if } u_i = z'_{32}, \end{cases}$$

$$z^{i+1} = (z''_2, z''_3, \ldots, z''_{32}, u_i).$$

- Finally, $H(u_1, \ldots, u_n) = (z_1^n \oplus z_{17}^n, z_2^n \oplus z_{18}^n, \ldots, z_{16}^n \oplus z_{32}^n)$.

But then Bob found out that his hash function is weak for using in cryptographic applications. Prove that Bob was right by constructing an infinite set $C \subset \bigcup_{n=1}^{\infty} \mathbb{F}_2^n$ such that all elements of C have the same hash value H.

An example. Let us calculate $H(0, 1, 0)$:

$$\begin{aligned} z^1 &= (\underbrace{1, 1, \ldots, 1}_{31}, 0), \\ z^2 &= (\underbrace{0, \ldots, 0}_{15}, \underbrace{1, \ldots, 1}_{15}, 0, 1), \\ z^3 &= (\underbrace{1, \ldots, 1}_{13}, 0, 0, \underbrace{1, \ldots, 1}_{14}, 0, 1, 0), \\ H(0, 1, 0) &= (\underbrace{0, \ldots, 0}_{14}, 1, 1). \end{aligned}$$

Problem 5. «One more parameter»

There are several parameters in cryptanalysis of block ciphers that are used to measure the diffusion strength. In this problem, we study properties of one of them.

Let n, m be positive integers. Let $a = (a_1, \ldots, a_m)$ be a vector with coordinates a_i taken from the finite field $\mathbb{F}_2$. Denote the number of nonzero coordinates a_i, $i = 1, \ldots, m$, by $\mathrm{wt}(a)$ and call this number the **weight** of the vector a.

The inner product of $a = (a_1, \ldots, a_m)$ and $b = (b_1, \ldots, b_m)$ in $\mathbb{F}_2^m$ is defined as

$$a \cdot b = a_1 b_1 \oplus \ldots \oplus a_m b_m.$$

For a Boolean function $f : \mathbb{F}_2^m \to \mathbb{F}_2$, we define the function *weight* wt as follows:

$$\mathrm{wt}(f) = \#\{a \in \mathbb{F}_2^m \mid f(a) = 1\}$$

The **special parameter** Q of a vectorial Boolean function $\varphi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is defined to be

$$Q(\varphi) = \min_{a,\, b,\, b\neq 0,\, \mathrm{wt}(a\cdot x \oplus b\cdot \varphi(x))\neq 2^{m-1}} \{\mathrm{wt}(a) + \mathrm{wt}(b)\}.$$

- Rewrite (simplify) the definition of $Q(\varphi)$ when the function φ is linear (recall that a function ℓ is linear if $\ell(x \oplus y) = \ell(x) \oplus \ell(y)$ for any x, y).

- Rewrite the definition of $Q(\varphi)$ in terms of linear codes, when the linear function φ is given by an $m \times m$ matrix M over $\mathbb{F}_2$, i. e. $\varphi(x) = Mx$.

- Find the tight upper bound for $Q(\varphi)$ as a function of m.

- Can you give an example of the function φ with the maximal possible value of Q?

Problem 6. «Scientists»

Two young cryptographers and very curious students Alice and Bob studied different cryptosystems and attacks on them. At the same time they were very interested in biographies of famous scientists and found out one interesting **property** that can be used in cryptosystems. They choose three pair of scientists:

Charles Darwin and **Michael Faraday**,
Werner Heisenberg and **Johannes Kepler**,
Hans Christian Orsted and **Mikhail Lomonosov**.

Alice and Bob choose a cryptosystem and an attack they would like to study. They constructed three sets of parameters for the cryptosystem: one set according to each pair of scientists. Then Alice choose a phrase consisting of 18 English letters (spaces were omitted) and divided it into three parts of 6 letters. She represented each part as a hexadecimal number using ASCII code. Alice encrypted the first part by the cryptosystem for each set of parameters, then the same actions she made for the second and the third parts. Finally, Alice got the following three groups of three ciphertexts (in hexadecimal notation):

	Part 1	Part 2	Part 3
Set of parameters 1	2512 1F5A 0079	B494 222D 3E1C	275E B751 4FDB
Set of parameters 2	3D0D 6812 0443	5111 5BFD 9398	0815 6223 2698
Set of parameters 3	1EDC 4856 8CE2	9C18 2A32 B9AB	9A1C AD5C 25D7

and asked Bob to decrypt it using the attack! Bob successfully read the secret phrase. Could you

- find the property like Alice and Bob,
- understand what is the cryptosystem and the attack chosen,
- decrypt the ciphertext by applying this attack?

*What word should be added at the beginning of the decrypted text according to the famous words of Mikhail Lomonosov?

Problem 7. «Masking»

It is known that there are attacks on cryptosystems that use information obtained from the physical implementation of a cryptosystem, for example, timing information, power consumption, electromagnetic leaks or even sound. To protect cryptosystems from such attacks cryptographers can use a countermeasure known as **masking**.

Correlation immune Boolean functions can reduce the masking cost. Therefore, we need to search for Boolean functions satisfying the following conditions: they should have **small Hamming weight** and **high correlation immunity**.

Let f be a non-constant Boolean function in 12 variables of correlation immunity 6.

- What is the lowest possible Hamming weight k of f?
- Give an example of such a function f with Hamming weight k.

Remark I. Hamming weight $\mathrm{wt}(f)$ of a Boolean function f in n variables is the number of vectors $x \in \mathbb{F}_2^n$ such that $f(x) = 1$.

Remark II. A Boolean function f in n variables is called *correlation immune of order* t, where t is an integer such that $1 \leqslant t \leqslant n$, if

$$\mathrm{wt}(f_{i_1,\ldots,i_t}^{a_1,\ldots,a_t}) = \mathrm{wt}(f)/2^t$$

for any set of indexes $1 \leqslant i_1 < \ldots < i_t \leqslant n$ and any set of values $a_1, \ldots, a_t \in \mathbb{F}_2$. Here $f_{i_1,\ldots,i_t}^{a_1,\ldots,a_t}$ denote the subfunction of f in $n - t$ variables that is obtained from $f(x_1, \ldots, x_n)$ by fixing each variable x_{i_k} by the value a_k, $1 \leqslant k \leqslant t$.