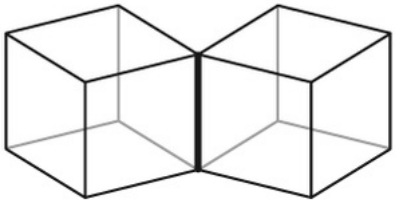
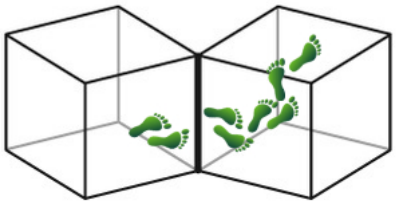
Problem 1. «Cubes and secrets»

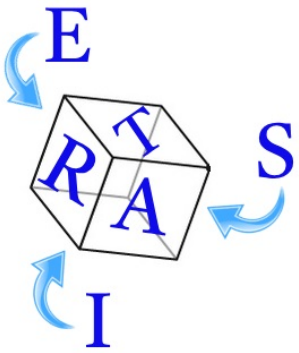
Alice is a beginner cryptographer. She was very impressed by the Scytale cipher, so she decided to invent her own simple cipher with the similar idea. Alice took two cubes with empty sides and joined them by an edge.



Then she wrote 12 letters of her secret message on empty sides of the cubes (one letter for one side). She did it in such a way that one can read the message just walking from side to side through edges. On every side it is possible to be only once.



She realized that the information about two joined edges and about the path on cubes form her secret key of encryption. At the same time letters on cubes form the resulting ciphertext. Could you read the secret message of Alice without the key? It is known also that the secret message is a meaningful text. Her cubes are



Problem 2. «AntCipher»

Sam studies microelectronics, while his hobbies are biology and cryptography. He decided to unite all these areas in a research project aimed at constructing a tiny GPS tracker for an ant to monitor its movements.

The tracker consists of 3 modules: GPS, encryption, transmission. Once a minute, coordinates are determined, encrypted, and transmitted to a Sam's computer, where they are automatically decrypted. Due to the size limitation, the encryption module takes only a 2-bit plaintext and produces a 2-bit ciphertext, so the coordinates are divided into 2-bit blocks which are given to the encryption module. Sam has just developed a symmetric cipher called **AntCipher** for this purpose.

The cipher must be represented by the equation CNF=True, where CNF is a conjunction of disjunctions of literals, yet literal is a Boolean variable or its negation. In the Sam's CNF, x_1 and x_2 correspond to the plaintext, x_9 and x_{10} correspond to the ciphertext, while the remaining 6 variables are auxiliary. The equation is as follows:

$$(x_1 \vee x_2 \vee x_9) \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_9) \wedge (\neg x_1 \vee x_2 \vee \neg x_9) \wedge (x_1 \vee \neg x_2 \vee x_9) \wedge$$
$$(x_1 \vee x_2 \vee x_3) \wedge (\neg x_9 \vee \neg x_{10} \vee \neg x_3) \wedge (x_1 \vee \neg x_2 \vee x_4) \wedge (\neg x_9 \vee x_{10} \vee \neg x_4) \wedge$$
$$(\neg x_1 \vee x_2 \vee x_5) \wedge (x_9 \vee \neg x_{10} \vee \neg x_5) \wedge (\neg x_1 \vee \neg x_2 \vee x_6) \wedge (x_9 \vee x_{10} \vee \neg x_6) \wedge$$
$$(x_1 \vee x_2 \vee x_3 \vee x_4 \vee \neg x_7) \wedge (x_2 \vee x_3 \vee x_4 \vee \neg x_7 \vee \neg x_8) = True$$

The problem is that, due to the limitations, the CNF must consist of at most 20 literals and at most 16 variables, while the presented one consists of 46 literals and 10 variables. Please, help Sam to construct an equivalent CNF that fits the limits. By equivalent it is meant that for each pair of plaintext-variables' values, the same pair of ciphertext-variables' values is derived in the equation.

Problem 3. «Mixed hashes»

Alice and Bob are exchanging with encrypted messages. To encrypt data, they use the **Present** cipher with an 80-bit secret key in ECB format. They record the information in the form of graphic files in `*.ppm` format.

The header of the `*.ppm` file consists of three lines of the form:

```
P6
X Y
255
```

where X and Y are the sizes of the graphic file in pixels horizontally and vertically, respectively.

So, in `mikki.ppm`, the header is:

```
P6
360 537
255
```

To be more secure, Alice and Bob decided that file headers should be removed before encryption. In order to be able to recover the file header, they agreed to transmit along with the encrypted file the hash value of the header itself, presented in **UTF-8** format. To do this, all header elements are written as a single line, using a space to separate the lines of the original header. The **sha-256** function is used as a hashing algorithm. So, for example, the following hash value will be generated for the header of `mikki.ppm`:

Heading `P6 360 537 255`

Sha-256 `999015795668c201db162926261ed979bc6e820aa1acfc385a0285685084d9f9`

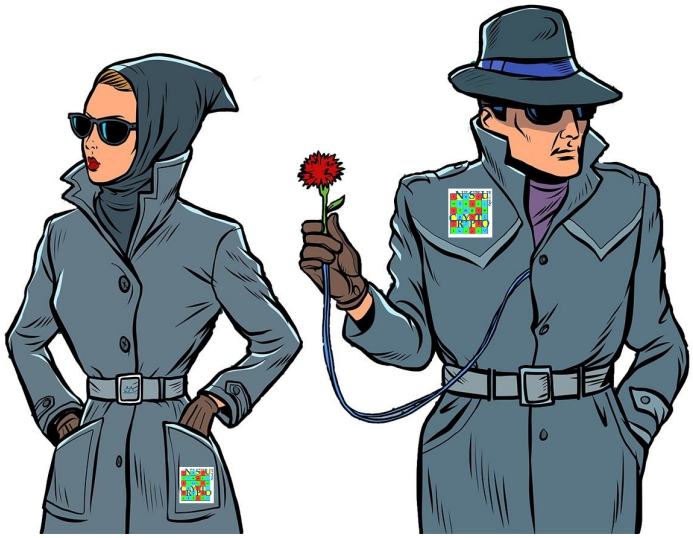
Bob prepared eight files for Alice without headers, encrypted using the **Present** algorithm with the same secret key in ECB mode. He has sent the files themselves and hash values of the headers to Alice. While sending, the hash values were mixed up. So, Alice received eight files and eight hash values, but she does not know which hash value corresponds to which encrypted file. Could you help Alice to read the message from Bob?

Hash values received are

```
602a4a8fff652291fdc0e049e3900dae608af64e5e4d2c5d4332603c9938171d
f40e838809ddaa770428a4b2adc1fff0c38a84abe496940d534af1232c2467d5
aa105295e25e11c8c42e4393c008428d965d42c6cb1b906e30be99f94f473bb5
70f87d0b880efcdbe159011126db397a1231966991ae9252b278623aeb9c0450
77a39d581d3d469084686c90ba08a5fb6ce621a552155730019f6c02cb4c0cb6
456ae6a020aa2d54c0c00a71d63033f6c7ca6cbc1424507668cf54b80325dc01
bd0fd461d87fba0d5e61bed6a399acdfc92b12769f9b3178f9752e30f1aeb81d
372df01b994c2b14969592fd2e78d27e7ee472a07c7ac3dfdf41d345b2f8e305
```

Problem 4. «Agents' meeting»

Alice and Bob, two special agents, were invited on the big meeting where they should find each other and communicate. Alice knows who is Bob (she was given a photo of him), but Bob has never seen Alice. Before the meeting the Boss has send them the secret password for communication: it is the square root of the first six digits of the number π modulo n, where $n = 15\,102\,023$ is a public information (known for all). Alice should find Bob and convince him that she knows the password without an announcement of it. Propose how it is possible to do. In other words, propose the zero-knowledge protocol for this specific situation. By the way, what is the sense of the number n?



Problem 5. «0, 1, 2, 3»

Decrypt the meaningful message:

```
1 0 2 0 0 1 0 0 0 3 0 0 0 0 0 1 0 0 2 0 0 0 0 0 1 0 0 1 0 0 1 0 1 0 0 1
0 0 1 0 2 0 0 3 0 0 0 0 3 0 0 0 0 2 0 3 0 1 0 0 0 2 0 0 3 0 0 0 2 0 0 3
2 0 0 0 0 0 0 0 3 0 0 0 3 0 0 0 0 0 0 3 0 0 0 0 0 0 0 0 0 0 0 2 0 0 0 0
0 0 1 1 0 0 0 2 2 0 0 0 3 0 0 0 1 1 0 0 0 2 0 2 2 0 0 0 3 0 0 2 2 2 2 0
3 1 0 0 0 0 2 3 0 2 0 0 3 0 0 1 0 0 1 0 0 2 2 0 0 0 0 0 3 0 0 0 2 0 0 0
0 1 0 0 0 0 2 0 0 2 0 0 3 0 0 1 3 0 1 0 0 2 0 0 0 1 0 0 3 0 0 0 2 0 0 2
0 1 0 0 0 0 2 0 0 2 0 0 3 0 0 1 0 0 1 0 0 2 0 0 2 0 0 0 3 0 0 0 2 0 0 0
0 0 1 1 0 0 0 2 2 0 0 0 3 0 0 0 1 1 0 0 0 2 0 0 0 0 0 0 3 0 0 0 0 2 2 0
2 0 0 0 0 0 1 0 0 0 1 1 0 0 2 0 0 0 0 0 3 0 0 0 1 0 3 0 0 0 1 0 0 0 0 3
```

Problem 6. «An aggregated signature»

Problem for a special prize!

Suppose that a big international organization, say **NSUCRYPTO association**, decided to organize its own news journal in the area of cryptography. The organization wants to publish only news that are verified by a large group of cryptographers. For this goal 10 000 leading experts in cryptography were invited to join the editorial board of the journal.

The following publishing politics was accepted. The news can be published if and only if it is signed by all members of the editorial board. But cryptographers do not want to use 10 000 individual signatures. Since they are cryptographers, they think about the aggregated postquantum signature that can not be divided into separate individual signatures.

So, **NSUCRYPTO association** kindly asks you to propose such a signature scheme. There are several requirements for it:

* the size of the signature should be not big. It can be about several kilobytes;
* the size of the public key (for checking the signature) should be small. It is desired that the key size will be constant (or close to constant) even if the number of experts is increased, say up to 20 000;
* signature verification should not take more than 2 minutes;
* the signature should be resistant to attacks that use quantum computers.

Problem 7. «Algebraic cryptanalysis»

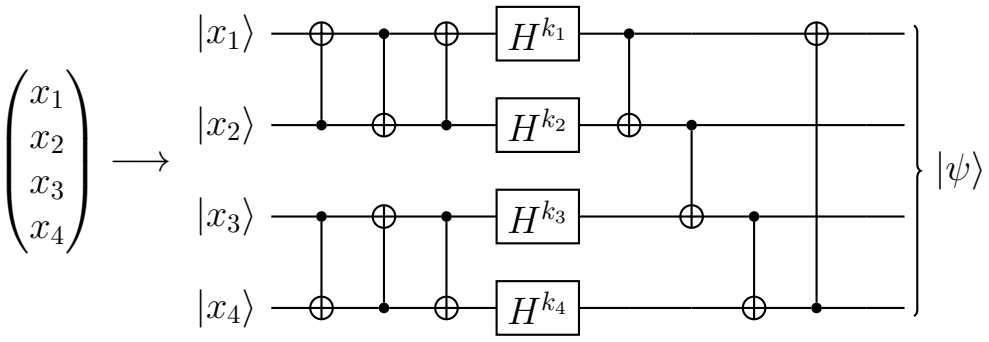
Bob decided to construct a new stream cipher **BOB-0.1**.

He used the binary key of length 8, say $K = (k_1, \ldots, k_8)$. Then he generated the binary sequence β such that $\beta_n = k_n$ for all $n = 1, \ldots, 8$ and for $n > 8$ it is defined as $\beta_n = \beta_{n-1} \oplus \beta_{n-8}$. Then Bob constructed the secret sequence γ for XORing it with a binary plaintext. The sequence γ is generated by the following rule: $\gamma_n = \beta_n \cdot \beta_{n+2} \oplus \beta_{n+7}$ for $n \geqslant 1$.

Alice intercepted the eight secret bits of γ after the first 1200 missed bits. These bits are `00100001`. Is she able to recover the original key K?

Problem 8. «Quantum encryption»

Bob works in a field of quantum mechanics and he has some ideas how it can be applied for the encryption of secret messages. He developed a toy cipher that encrypts 4-bit words by using 4-bit secret key (k_1, k_2, k_3, k_4) and the following quantum circuit:



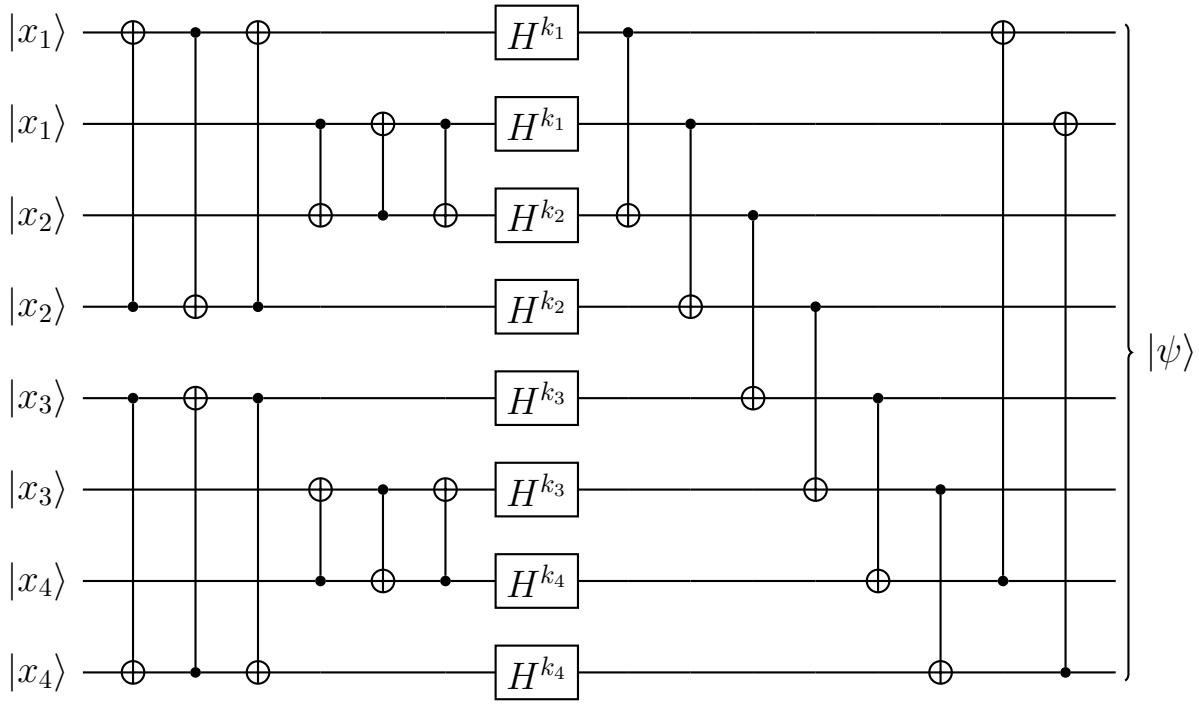
This cipher operates with 4-bit plaintext (x_1, x_2, x_3, x_4) that is initially encoded to the corresponding 4-qubit «plainstate» $|x_1, x_2, x_3, x_4\rangle$. This quantum state is an input of the circuit that consists of several single-qubit gates. Note that any quantum gate is a unitary operator that acts on the space of the states of the corresponding quantum system. The used gates are

Hadamard gate	$\|x\rangle$ — H — $\frac{\|0\rangle+(-1)^x\|1\rangle}{\sqrt{2}}$	acts on a single qubit in the state $\|x\rangle$, $x \in \{0,1\}$
CNOT gate	$\|x\rangle$ — $\|x\rangle$ $\|y\rangle$ — $\|y \oplus x\rangle$	acts on a pair of qubits in the states $\|x\rangle, \|y\rangle$, $x, y \in \{0,1\}$

The notation H^b, where $b \in \{0, 1\}$, means that if $b = 0$, the identity gate I is applied instead of H, while for $b = 1$ the gate H is considered.

The result of the encryption is the «cipherstate» $|\psi\rangle$ that is further transmitted via the quantum channel. The decryption procedure takes the state $|\psi\rangle$ and applies the inverse circuit.

Bob was advised to increase the number of qubits in order to reduce the effect of possible errors in quantum computation and quantum channel, so he decided to modify the circuit and make copies of qubits of the plainstate. The resulting circuit is the following:



Alice looked at the cipher and claimed that she would be able to reveal the secret key (k_1, k_2, k_3, k_4) if she knew some number N of certain amplitudes of the state $|\psi\rangle$. The state $|\psi\rangle$ is characterized by 256 amplitudes, so essentially we have $N \leqslant 256$.

Could you check the assumption of Alice and find the least possible value of N if the claim is correct?

Remark. Let us briefly formulate the key points of quantum circuits. A qubit is a two-level quantum mechanical system whose state $|\psi\rangle$ is the superposition of basis quantum states $|0\rangle$ and $|1\rangle$. The superposition is written as $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, where α_0 and α_1 are complex numbers, called amplitudes, that possess $|\alpha_0|^2 + |\alpha_1|^2 = 1$. The amplitudes α_0 and α_1 have the following physical meaning: after the measurement of a qubit which has the state $|\psi\rangle$, it will be found in the state $|0\rangle$ with probability $|\alpha_0|^2$ and in the state $|1\rangle$ with probability $|\alpha_1|^2$.

In order to operate with multi-qubit systems, we consider the bilinear operation $\otimes : |x\rangle, |y\rangle \to |x\rangle \otimes |y\rangle$ on $x, y \in \{0, 1\}$ which is defined on pairs $|x\rangle, |y\rangle$, and by bilinearity is expanded on the space of all linear combinations of $|0\rangle$ and $|1\rangle$. When we have two qubits in states $|\psi\rangle$ and $|\varphi\rangle$ correspondingly, the state of the whole system of these two qubits is $|\psi\rangle \otimes |\varphi\rangle$. In general, for two qubits we have $|\psi\rangle = \alpha_{00}|0\rangle \otimes |0\rangle + \alpha_{01} |0\rangle \otimes |1\rangle + \alpha_{10} |1\rangle \otimes |0\rangle + \alpha_{11} |1\rangle \otimes |1\rangle$. The physical meaning of complex numbers α_{ij} is the same as for one qubit, so we have the essential restriction $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. By induction, this process is expanded on the case of three qubits and more. Thus, the general form of the state of n qubits is

$$|\psi\rangle = \sum_{x \in \mathbb{F}_2^n} \alpha_x |x\rangle,$$

where amplitudes $\alpha_{00\ldots0}, \alpha_{00\ldots01}, \ldots, \alpha_{11\ldots1}$ have the same physical meaning as discussed before. Here we use more brief notation $|x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_n\rangle \equiv |x_1, x_2, \ldots, x_n\rangle \equiv |x_1 x_2 \ldots x_n\rangle$.