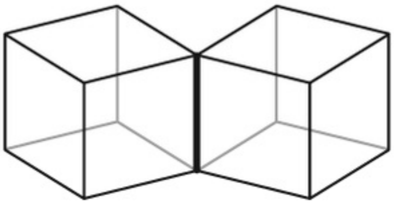
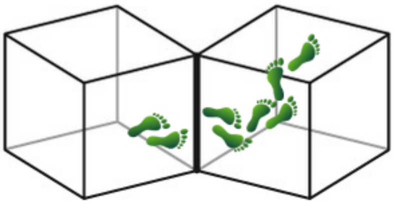
Problem 1. «Cubes and secrets»

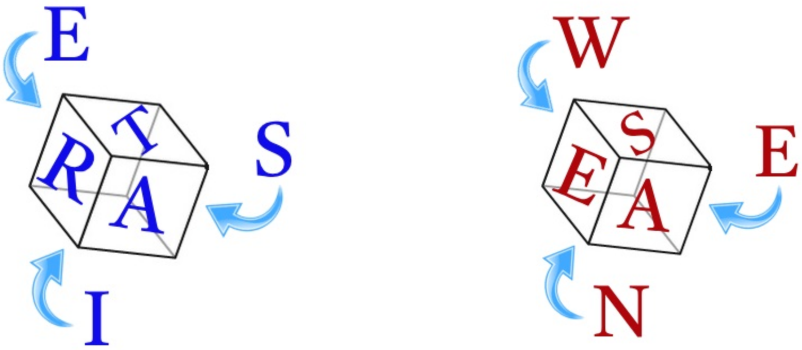
Alice is a beginner cryptographer. She was very impressed by the Scytale cipher, so she decided to invent her own simple cipher with the similar idea. Alice took two cubes with empty sides and joined them by an edge.



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.

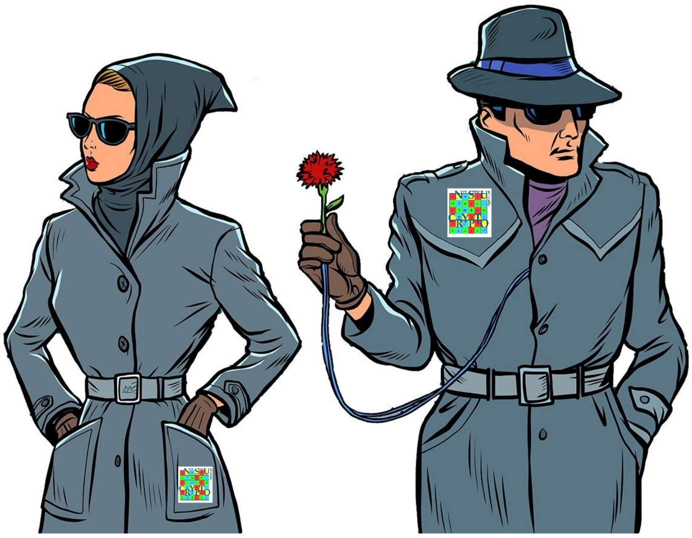


She realized that the information about two joined edges and about the path on cubes form her secret key of encryption. At the same time letters on cubes form the resulting ciphertext. Could you read the secret message of Alice without the key? It is known also that the secret message is a meaningful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



Problem 2. «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 3. «Affine cipher»

Consider a 29-character alphabet $\{A,\ldots, Z, \alpha, \beta, \gamma\}$. Letters A,. . . , Z have numerical equivalents $0, \ldots, 25$, while numbers 26, 27 and 28 correspond to symbols α, β, γ.

We use a cryptosystem with plaintexts and ciphertexts being two-letter blocks, i. e. bigrams. For each bigram it is easy to find a numerical equivalent, it is an integer from 0 to $840 = 29^2 - 1$, determined by the rule $x \cdot 29 + y$, where x and y are the numerical equivalents of the letters of the bigram.

Encryption is implemented as an affine transformation $C = a \cdot P + b \mod 841$, where P is a plaintext, C is the corresponding ciphertext and the pair (a, b) is a secret key. Here a and b are integer numbers between 0 and 840. For example, if $a = 2$ and $b = 27$, then the bigram DP will be encrypted as $H\gamma$. In fact, for the bigram DP we put into the correspondence the number $3 \cdot 29 + 15 = 102$. Encrypting we get $2 \cdot 102 + 27 = 231$ that corresponds to the bigram $H\gamma$, since $231 = 7 \cdot 29 + 28$.

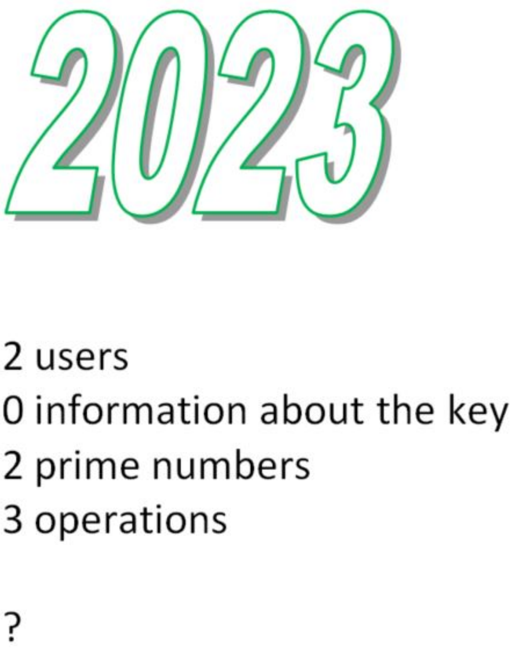
An analysis of the long ciphertext (for a fixed unknown key) showed that the bigrams "$\beta\ \gamma$", "UM" and "LC" are the most often found in this text. At the same time, we assume that the most frequent bigrams in English texts are "TH", "HE" and "IN".

Could you then decrypt the message "KEUDCR"? What about recovering of the key?

Problem 4. «Primes»

Marcus invented a new cryptosystem. To start to work with it one should choose two big prime numbers p and q, then calculate $n = p \cdot q$ and $m = p + q$. The number $n \cdot m$ will be used in the cryptosystem.

While testing the system Marcus has noticed that for the chosen numbers p and q the resulting number $n \cdot m$ ends with 2023. Is this possible?



2 users
0 information about the key
2 prime numbers
3 operations

?

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 3 0 0 0 0 0 0 0 0 0 0 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 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. «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?