Problem 1. «CP Problem»

Let $\mathbb{G} = \langle g \rangle$ be a group of prime order q, κ is the bit length of q. Let us consider two known modifications of the discrete logarithm problem over $\mathbb{G}$, namely, s-DLOG problem and ℓ-OMDL problem. Both of them are believed to be difficult.

s-DLOG problem (with parameter $s \in \mathbb{N}$)

Unknown values: x is chosen uniformly at random from $\mathbb{Z}_q^*$.
Known values: $g^x, g^{x^2}, \ldots, g^{x^s}$.
Access to oracles: no.
The task: to find x.

ℓ-OMDL (One-More Discrete Log) problem (with parameter $\ell \in \mathbb{N}$)

Unknown values: $x_1, x_2, \ldots, x_{\ell+1}$ are chosen uniformly at random from $\mathbb{Z}_q^*$.
Known values: $g^{x_1}, g^{x_2}, \ldots, g^{x_{\ell+1}}$.
Access to oracles: at most ℓ queries to O_1 that on input $y \in \mathbb{G}$ returns x such that $g^x = y$.
The task: to find $x_1, x_2, \ldots, x_{\ell+1}$.

Consider another one problem that is close to the s-DLOG and ℓ-OMDL problems:

(k,t)-CP (Chaum—Pedersen) problem (with parameters $k, t \in \mathbb{N}$)

Unknown values: $x_1, x_2, \ldots, x_{t+1}$ are chosen uniformly at random from $\mathbb{Z}_q^*$.
Known values: $g^{x_1}, g^{x_2}, \ldots, g^{x_{t+1}}$.
Access to oracles: at most k queries to O_1 that on input $(i, z) \in \{1, \ldots, t+1\} \times \mathbb{G}$ returns z^{x_i}, and at most t queries to O_2 that on input $(\alpha_1, \ldots, \alpha_{t+1}) \in \mathbb{Z}_q^{t+1}$ returns $\alpha_1 x_1 + \ldots + \alpha_{t+1} x_{t+1}$.
The task: to find $x_1, x_2, \ldots, x_{t+1}$.

It is easy to see that if there exists a polynomial (by κ) algorithm that solves the s-DLOG problem, then there exists a polynomial algorithm that solves the $(s-1,t)$-CP problem for any $t \in \mathbb{N}$.

Problem for a special prize! Prove or disprove the following conjecture: if there exists a polynomial algorithm that solves (k,t)-CP problem, then there exists a polynomial algorithm that solves at least one of the s-DLOG and ℓ-OMDL problems, where k, t, s, ℓ are upper bounded by polynomial of κ.

Problem 2. «Interpolation with Errors»

Let $n = 2022$ and let $\mathbb{Z}_n$ be the ring of integers modulo n. Given $x_i, y_i \in \mathbb{Z}_n$ for $i \in \{1, \ldots, 324\}$, find monic polynomials

$$f(x) = x^{16} + \alpha_{15}x^{15} + \ldots + \alpha_1 x + \alpha_0,$$
$$g(x) = x^{16} + \beta_{15}x^{15} + \ldots + \beta_1 x + \beta_0$$

of degree $d = 16$ and coefficients from $\mathbb{Z}_n$ such that the relation

$$y_i = \frac{f(x_i)}{g(x_i)} = \frac{x_i^{16} + \alpha_{15}x_i^{15} + \ldots + \alpha_1 x_i + \alpha_0}{x_i^{16} + \beta_{15}x_i^{15} + \ldots + \beta_1 x_i + \beta_0}$$

holds for at least 90 of the indices $i \in \{1, \ldots, 324\}$.

Note. The coefficients $\beta_0, \ldots, \beta_{15}$ are such that the denominator of the above fraction is invertible for all possible values of $x_i \in \mathbb{Z}_n$. It can be assumed that they are sampled uniformly at random from all such sets of values. Furthermore, the positions and error values can be also assumed to be sampled uniformly at random.

The attachment contains a CSV file with 324 triplets (i, x_i, y_i).

Problem 3. «HAS01»

Bob is a beginner cryptographer. He read an article about the new hash function HAS01 (see a description here). Bob decided to implement the HAS01 function in order to use it for checking the integrity of messages being forwarded. However, he was inattentive and made a mistake during the implementation. In the function f_1, he did not notice the sign «'» in the variable a and used the following set of formulas:

```
for $i = 0$ to 7 do
    for $j = 0$ to 6 do
        $a_{(i+1) \bmod 8, j} \leftarrow \mathrm{SBox}(((a_{i,j} \oplus a_{(i+1) \bmod 8, j}) \ll 3) \oplus ((a_{i,j+1} \oplus a_{(i+1) \bmod 8, j+1}) \gg 5))$
    end for
    $a_{(i+1) \bmod 8, 7} \leftarrow \mathrm{SBox}(((a_{i,7} \oplus a_{(i+1) \bmod 8, 7}) \ll 3) \oplus ((a_{i,0} \oplus a_{(i+1) \bmod 8, 0}) \gg 5) \oplus 7)$
end for
```

Q1 Prove that Bob's version of the hash function is cryptographically weak.

Q2 Find a collision to the following message (given in hexadecimal format):
316520393820336220323620343720316320373820386520.

The test set value for the original HAS01 hash function is given here.
The test set value for Bob's implementation is given here.

Problem 4. «Weaknesses of the PHIGFS»

A young cryptographer Philip designs a family of lightweight block ciphers based on a 4-line type-2 Generalized Feistel scheme (GFS) with better diffusion effect.

Its block is divided into four m-bit subblocks, $m \geqslant 1$. For better diffusion effect, Philip decides to use a (4×4)-matrix A over $\mathbb{F}_{2^m}$ instead of a standard subblocks shift register in each round. The family $\mathrm{PHIGFS}_\ell(A, b)$ is parameterized by a non-linear permutation $b\colon \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, the matrix A and the number of rounds $\ell \geqslant 1$. The one-round keyed transformation of $\mathrm{PHIGFS}_\ell(A, b)$ is a permutation g_k on $\mathbb{F}_{2^m}^4$ defined as:

$$g_k(x_3, x_2, x_1, x_0) = A \cdot (x_3, x_2 \oplus b(x_3 \oplus k_1), x_1, x_0 \oplus b(x_1 \oplus k_0))^T,$$

where $x_0, x_1, x_2, x_3 \in \mathbb{F}_{2^m}$, $k = (k_1, k_0)$ is a $2m$-bit round key, $k_0, k_1 \in \mathbb{F}_{2^m}$.

The ℓ-round encryption function $f_{k^{(1)},\ldots,k^{(\ell)}}\colon \mathbb{F}_{2^m}^4 \to \mathbb{F}_{2^m}^4$ under a key $(k^{(1)}, \ldots, k^{(\ell)}) \in \mathbb{F}_{2^m}^\ell$ is given by

$$f_{k^{(1)},\ldots,k^{(\ell)}}(\mathbf{x}) = g_{k^{(\ell)}} \ldots g_{k^{(1)}}(\mathbf{x}) \text{ for all } \mathbf{x} \in \mathbb{F}_{2^m}^4.$$

For effective implementation and security, Philip chooses two binary matrices A', A'' with the maximum branch number among all binary matrices of size 4, where

$$A' = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \quad A'' = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

For approval, he shows the cipher to his friend Antony who claims that A', A'' are bad choices because ciphers $\mathrm{PHIGFS}_\ell(A', b)$, $\mathrm{PHIGFS}_\ell(A'', b)$ are insecure against distinguisher attacks for all $b\colon \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $\ell \geqslant 1$.

Help Philip to analyze the cipher $\mathrm{PHIGFS}_\ell(A, b)$. Namely, for any $b\colon \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ and any $\ell \geqslant 1$, show that $\mathrm{PHIGFS}_\ell(A, b)$ has

(a) ℓ-round differential sets with probability 1;
(b) ℓ-round impossible differential sets;

for the following cases: **Q1** $A = A'$; and **Q2** $A = A''$. In each case, construct these nontrivial differential sets and prove the corresponding property.

Turn to the next page.

Remark. Let us recall the following definitions.

- Let $\delta, \varepsilon \in \mathbb{F}_{2^n}$ be fixed nonzero input and output differences. The *differential probability* of $s\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined as

  $$p_{\delta,\varepsilon}(s) = 2^{-n} \cdot \left|\{\alpha \in \mathbb{F}_{2^n} | s(\alpha \oplus \delta) \oplus s(\alpha) = \varepsilon\}\right|.$$

- If $s\colon \mathbb{F}_{2^n} \times K \to \mathbb{F}_{2^n}$ depends on a key space K, then the *differential probability* of s is defined as

  $$p_{\delta,\varepsilon}(s) = |K|^{-1} \sum_{k \in K} p_{\delta,\varepsilon}(s_k),$$

  where $s(x, k) = s_k(x)$, $x \in \mathbb{F}_{2^n}$, $k \in K$.

- Let $\Omega, \Delta \subseteq \mathbb{F}_{2^n} \backslash \{0\}$ and Ω, Δ are nonempty. If $p_{\delta,\varepsilon}(s) = 0$ for any $\delta \in \Omega$, $\varepsilon \in \Delta$, then (Ω, Δ) are *impossible differential sets*. But if

  $$\sum_{\delta \in \Omega, \varepsilon \in \Delta} p_{\delta,\varepsilon}(s) = 1,$$

  then (Ω, Δ) are *differential sets with probability* 1. We call (Ω, Δ) trivial (impossible) differential sets if $\Omega \in \{\emptyset, \mathbb{F}_{2^n} \backslash \{0\}\}$ or $\Delta \in \{\emptyset, \mathbb{F}_{2^n} \backslash \{0\}\}$.

Problem 5. «Super dependent S-box»

Harry wants to find a super dependent S-box for his new cipher. He decided to use a permutation that is strictly connected with every of its variables. He tries to estimate the number of such permutations.

A vectorial Boolean function $F(x) = (f_1(x), f_2(x), \ldots, f_n(x))$, where $x \in \mathbb{F}_2^n$, is a *permutation* on $\mathbb{F}_2^n$ if it is a one-to-one mapping on the set $\mathbb{F}_2^n$. Its coordinate function $f_k(x)$ (that is a Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$), *essentially depends* on the variable x_j if there exist values $b_1, b_2, \ldots, b_{j-1}, b_{j+1}, \ldots, b_n \in \mathbb{F}_2$ such that

$$f_k\left(b_1, b_2, \ldots, b_{j-1}, 0, b_{j+1}, \ldots, b_n\right) \neq f_k\left(b_1, b_2, \ldots, b_{j-1}, 1, b_{j+1}, \ldots, b_n\right).$$

In other words, the essential dependence on the variable x_j of a function f means the presence of x_j in the algebraic normal form of f (the unique representation of a function in the basis of binary operations AND, XOR, and constants 0 and 1).

An example. Let $n = 3$. Then the Boolean function $f(x_1, x_2, x_3) = x_1x_2 \oplus x_3$ essentially depends on all its variables; but $g(x_1, x_2, x_3) = x_1x_2 \oplus x_2 \oplus 1$ essentially depends only on x_1 and x_2.

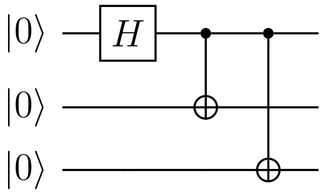
The problem. Find the number of permutations on $\mathbb{F}_2^n$ such that all their coordinate functions essentially depend on all n variables, namely

Q1 Solve the problem for $n = 2, 3$.

Q2 Problem for a special prize! Solve the problem for arbitrary n.

Problem 6. «Quantum entanglement»

The Nobel Prize in Physics in 2022 was awarded to researchers who experimentally investigated quantum *entanglement*. One of their studies was devoted to a Greenberger–Horne–Zeilinger state $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, which is an entangled state of three qubits. This state can be created using the following quantum circuit:



After the measurement, the probability to find the system described by $|GHZ\rangle$ in the state $|000\rangle$ or in the state $|111\rangle$ is equal to $1/2$.

When we make measurements in quantum physics, we are able to make *post-selection*. For example, if we post-select the events when the first qubit was in state $|0\rangle$, the second and the third qubits will also be found in the state $|0\rangle$ for sure, this is actually what entanglement means. We also see that the post-selection destroys entanglement of two remaining qubits.

Q1 But what will happen, if we post-select the events when the first qubit is in the Hadamard state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$? How can we perform this kind of post-selection if the result of each measurement of a qubit state can be only 0 or 1 and we can only post-select these events? Will the two remaining qubits be entangled after post-selection? Design the circuit which will provide an answer.

Q2 **Problem for a special prize!** There are two different classes of three-qubit entanglement. One of them is

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle),$$

and the other is

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle).$$

Discuss the possible ideas how the difference between these states can be found with the usage of post-selection and measurement. Don't forget that you need to verify entanglement for both types of states!

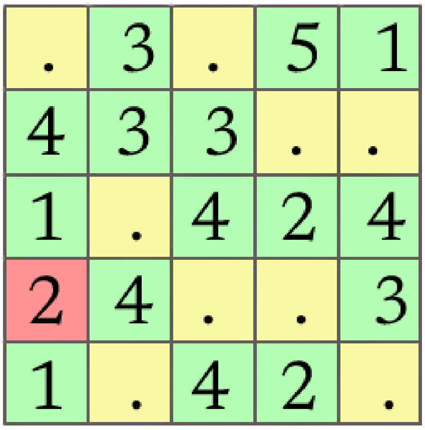
Turn to the next page.

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 $|\alpha_1|^2$. Note that we can measure qubit, initially given in the state $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, in other basis, for example Hadamard basis $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. In order to do this, we consider the state in the form $|\psi\rangle = \alpha'_0 |+\rangle + \alpha'_1 |-\rangle$, where complex amplitudes α'_0, α'_1 have the same physical meaning as α_0 and α_1. Then we can calculate the probability that the qubit will be in the state $|+\rangle$ or $|-\rangle$ after the measurement and consider the process of post-selection in this case. 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 $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. We use more brief notation $|a\rangle \otimes |b\rangle \equiv |ab\rangle$. By induction, this process is expanded on the case of three qubits and more. Mathematically, the entanglement of n-qubits state means that we can not consider this state in the form $|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$, where $|\varphi_1\rangle$ and $|\varphi_2\rangle$ are some states of m and $n - m$ qubits, correspondingly. In order to verify your circuits, you can use different quantum circuit simulators, for example `https://algassert.com/quirk`.

Problem 7. «Numbers and points»

Decrypt the message!

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z



.	3	.	5	1
4	3	3	.	.
1	.	4	2	4
2	4	.	.	3
1	.	4	2	.

Problem 8. «Bob's symbol»

Bob learned the Goldwasser–Micali cryptosystem at the university. Now, he is thinking about functions over finite fields that are similar to Jacobi symbol.

He chose a function $B_n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (Bob's symbol) defined as follows for any $a \in \mathbb{F}_{2^n}$:

$$B_n(a) = \begin{cases} 1, & \text{if } a = x^2 + x \text{ for some } x \in \mathbb{F}_{2^n}, \\ 0, & \text{otherwise.} \end{cases}$$

Bob knows that finite fields may have some subfields. Indeed, it is well known that $\mathbb{F}_{2^k}$ is a subfield of $\mathbb{F}_{2^n}$ if and only if $k|n$. Bob wants to exclude the elements of subfields. In other words, he considers the restriction of B_n to the set

$$\widehat{\mathbb{F}}_{2^n} = \mathbb{F}_{2^n} \setminus \bigcup_{k|n,\, k\neq n} \mathbb{F}_{2^k}.$$

Here, by $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$ we mean the removal from $\mathbb{F}_{2^n}$ the elements forming the field of order 2^k.

Finally, Bob is interested in the sets

$$B_n^0 = \{y \in \widehat{\mathbb{F}}_{2^n} : B_n(y) = 0\} \quad \text{and} \quad B_n^1 = \{y \in \widehat{\mathbb{F}}_{2^n} : B_n(y) = 1\}.$$

Q1 Help Bob to find $|B_n^0|/|B_n^1|$ if n is odd.

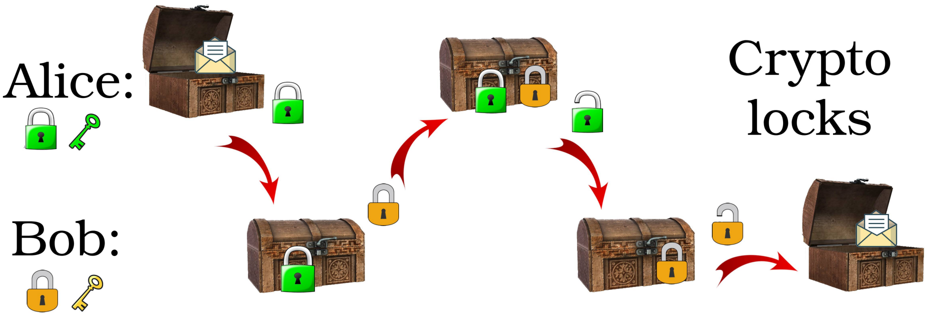
Q2 Help Bob to find $|B_n^0|$ and $|B_n^1|$ for an arbitrary n.

Problem 9. «Crypto locks»

Alice and Bob are wondering about the creation of a new version for the Shamir three-pass protocol. They have several ideas about it.

The Shamir three-pass protocol was developed more than 40 years ago. Recall it. Let p be a big prime number. Let Alice take two secret numbers c_A and d_A such that $c_Ad_A = 1 \bmod (p-1)$. Bob takes numbers c_B and d_B with the same property. If Alice wants to send a secret message m to Bob, where m is an integer number $1 < m < p-1$, then she calculates $x_1 = m^{c_A} \bmod p$ and sends it to Bob. Then Bob computes $x_2 = x_1^{c_B} \bmod p$ and forwards it back to Alice. On the third step, Alice founds $x_3 = x_2^{d_A} \bmod p$ and sends it to Bob. Finally, Bob recovers m as $x_3^{d_B} \bmod p$ according to Fermat's Little theorem.

It is possible to think about action of c_A and d_A over the message as about locking and unlocking, see the picture below.



Alice and Bob decided to change the scheme by using symmetric encryption and decryption procedures instead of locking and unlocking with c_A, c_B, d_A and d_B.

Q1 Propose some simple symmetric ciphers that would be possible to use in such scheme. What properties for them are required? Should Alice and Bob use the same cipher (with different own keys) or not?

Q2 Problem for a special prize! Could you find such symmetric ciphers that make the modified scheme to be secure as before? Please, give your reasons and proofs.

Problem 10. «Public keys for e-coins»

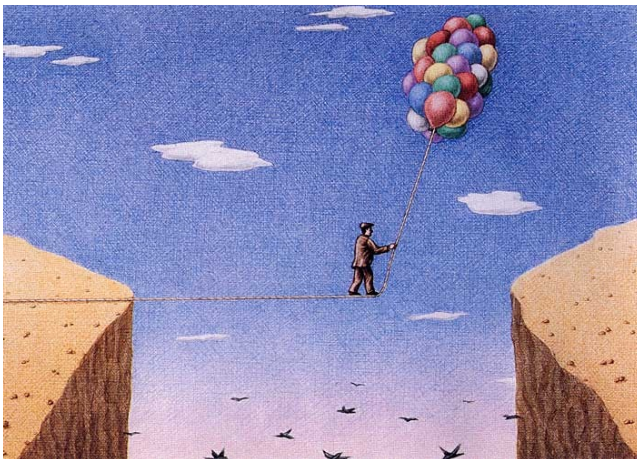
Alice has n electronic coins that she would like to spend via some public service S (bank). The service applies some asymmetric algorithm of encryption $E(,)$ and decryption $D(,)$ in its work. Namely, for the pair of public and private keys (PK, SK) and for any message m it holds: if $c = E(m, PK)$, then $m = D(c, SK)$ and visa versa: if $c' = E(m, SK)$, then $m = D(c', PK)$.

To spend her money, Alice generates a sequence of public and private key pairs $(PK_1, SK_1), \ldots, (PK_n, SK_n)$ and sends the sequence of public keys $PK_1, \ldots, PK_n$ to the service S. By this she authorizes the service S to control her n coins.

If Alice would like to spend a coin with number i in the shop of Bob, she just gives the secret key SK_i to Bob and informs him about the number i. To get the coin with number i, Bob sends to the service S three parameters: number i, some non secret message m, and its electronic signature $c' = E(m, SK_i)$. The service S checks whether the signature c' corresponds to the message m, i.e. does it hold the equality $m = D(c', PK_i)$. If it is so, the service accepts the signature, gives the coin number i to Bob and marks it as «spent».

Problem for a special prize! Propose a *modification of this scheme* related to generation of public and private key pairs. Namely, is it possible for Alice not to send the sequence of public keys $PK_1, \ldots PK_n$ to the service S, but send only some initial information enough for generating all necessary public keys on the service's side? Suppose that Alice sends to the service S only some initial key PK (denote it also as PK_0), some function f and a set of parameters T such that $PK_{i+1} = f(PK_i, T)$ for all $i \geqslant 0$. Propose your variant of this function f and the set T. Think also what asymmetric cryptosystem it is possible to use in such scheme.

Requirements to the solution. Knowing PK, f and T, it is impossible to find any private key SK_i, where $i = 1, \ldots, n$. It should be impossible to recover SK_i even if the secret keys $SK_1, \ldots, SK_{i-1}$ are also known, or even if all other secret keys are known (more strong condition).



The picture of Gürbüz Doğan Ekşioğlu.

Problem 11. «A long-awaited event»

Bob received from Alice the secret message

`L78V8LC7GBEYEE`

informing him about some important event.

It is known that Alice used an alphabet with 37 characters from `A` to `Z`, from `0` to `9` and a space. Each of the letters is encoded as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	SPACE
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36

For the encryption, Alice used a function f such that $f(x) = ax^2 + bx + c \pmod{37}$ for some integers a, b, c and f satisfies the property

$$f(x - y) - 2f(x)f(y) + f(1 + xy) = 1 \pmod{37} \text{ for any integers } x, y.$$

Decrypt the message that Bob has received.