Problem 1. «Numbers and points»

Decrypt the message!

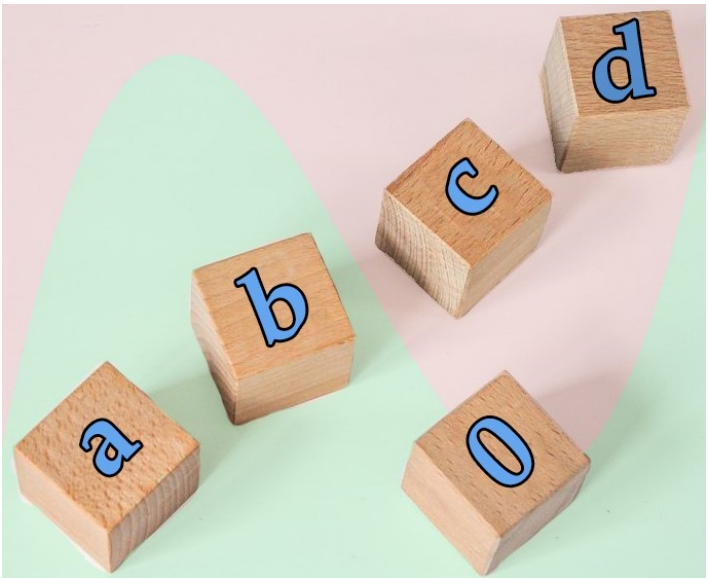
	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

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

Problem 2. «Hidden primes»

The Olympiad team rented an office at the Business Center, 1-342 room, on 1691th street for NSUCRYPTO-2022 competition for 0 nsucoins (good deal!). Mary from the team wanted to create a task for the competition and she needed to pick up three numbers for this task. She used to find an inspiration in numbers around her and various equations with them. After some procedure she found three prime numbers! It is interesting that when Mary added the smallest number to the largest one and divided the sum by the third number, the result was also the prime number.

Could you guess these numbers she found?



Problem 3. «Face-to-face»

Alice picked a new pin code (4 pairwise distinct digits from $\{1, 2, \ldots, 9\}$) for her credit card such that all digits have the same parity and are arranged in increasing order. Bob and Charlie wanted to guess her pin code. Alice said that she can give each of them a hint but face-to-face only.

Bob alone came to Alice and she told him that the sum of her pin code digits is equal to the number of light bulbs in the living room chandelier. Bob answered that there is still no enough information for him to guess the code, and left. After that, Charlie alone came to Alice and she told him that if we find the product of all pin code digits and then sum up digits of those product, this result number would be equal to the amount of books on the shelf. Charlie also answered that there is still no enough information for him to guess the code, and left.

Unfortunately, Eve was eavesdropping in the next apartment and, after Charlie had left, she immediately found out Alice pin code despite that she had never seen those chandelier and bookshelf. Could you find the pin code too?

Problem 4. «Matrix and reduction»

Alice used an alphabet with 30 characters from `A` to `Z` and `0`, `1`, «`,`», «`!`». Each of the letters is encoded as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
P	Q	R	S	T	U	V	W	X	Y	Z	0	1	,	!
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

Encryption. The plaintext is divided into consequent subwords of length 4 that are encrypted independently via the same encryption (2×2)-matrix F with elements from $\mathbb{Z}_{30}$. For example, let the j-th subword be `WORD` and the encryption matrix F be equal to

$$F = \begin{pmatrix} 11 & 9 \\ 11 & 10 \end{pmatrix}.$$

The matrix that corresponds to `WORD` is denoted by P_j and the matrix that corresponds to the result of the encryption of `WORD` is C_j and calculated as follows:

$$C_j = F \cdot P_j = \begin{pmatrix} 11 & 9 \\ 11 & 10 \end{pmatrix} \cdot \begin{pmatrix} 22 & 17 \\ 14 & 3 \end{pmatrix} = \begin{pmatrix} 8 & 4 \\ 22 & 7 \end{pmatrix} \pmod{30},$$

that is the j-th subword of the ciphertext is `IWEH`.

Eve has intercepted a ciphertext that was transmitted from Alice to Bob:

`CYPHXWQE!WNKHZOZ`

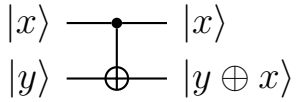
Also, she knows that the third subword of the plaintext is `FORW`. Will Eve be able to restore the original message?

Problem 5. «Reversing a gate»

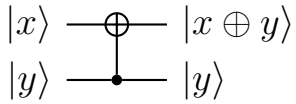
Daniel continues to study quantum circuits. A controlled NOT (CNOT) gate is the most complex quantum gate from the universal set of gates required for quantum computation. This gate acts on two qubits and makes the following transformation:

$$|00\rangle \to |00\rangle\,, \quad |01\rangle \to |01\rangle\,, \quad |10\rangle \to |11\rangle\,, \quad |11\rangle \to |10\rangle\,.$$

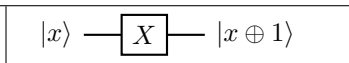
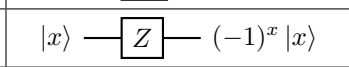
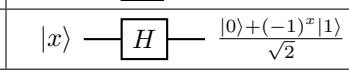
This gate is clearly asymmetric. The first qubit is considered as control one, and the second is as a target one. CNOT is described by the following quantum circuit ($x, y \in \mathbb{F}_2$):



The problem. Help Daniel to design a circuit in a special way that reverses CNOT gate:



It makes the following procedure: $|00\rangle \to |00\rangle\,,\ |01\rangle \to |11\rangle\,,\ |10\rangle \to |10\rangle\,,\ |11\rangle \to |01\rangle$. To do this you should modify the original CNOT gate without re-ordering the qubits but via adding some single-qubit gates instead from the following ones:

Pauli-X gate		acts on a single qubit in the state $\|x\rangle$, $x \in \{0,1\}$
Pauli-Z gate		acts on a single qubit in the state $\|x\rangle$, $x \in \{0,1\}$
Hadamard gate		acts on a single qubit in the state $\|x\rangle$, $x \in \{0,1\}$

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 $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. We use more brief notation $|a\rangle \otimes |b\rangle \equiv |ab\rangle$. In order to verify your circuits, you can use different quantum circuit simulators, for example `https://algassert.com/quirk`.

Problem 6. «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.

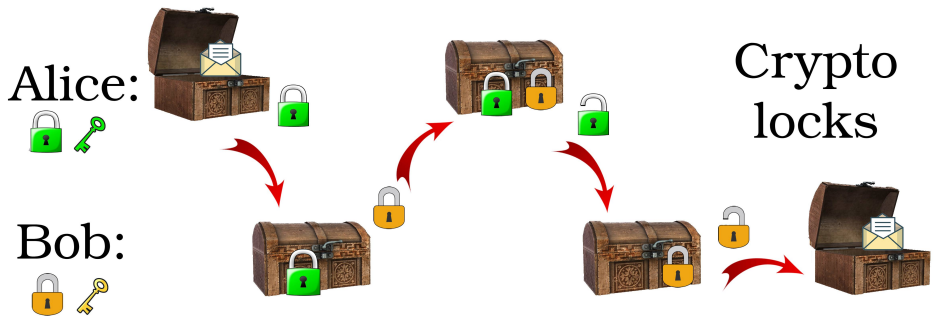
Q2 Help Bob to find $|B_n^0|$ and $|B_n^1|$ for an arbitrary n.

Problem 7. «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 $c_A d_A = 1 \bmod (p-1)$. 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 8. «Public keys for e-coins»

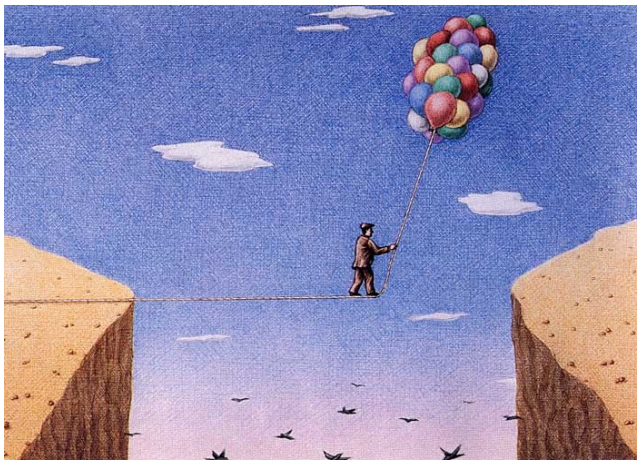
Alice has n electronic coins that she would like to spend via some public service S (bank). The service applies some asymmetric algorithm of encryption $E(,)$ and decryption $D(,)$ in its work. Namely, for the pair of public and private keys (PK, SK) and for any message m it holds: if $c = E(m, PK)$,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