Problem 1. «Numbers and points»

Decrypt the message!

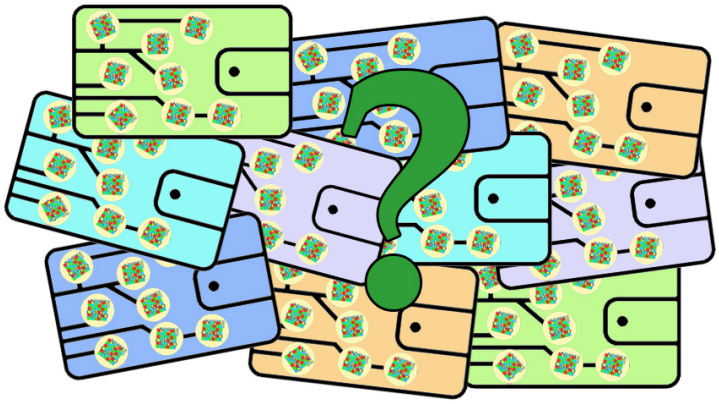
	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

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

Problem 2. «Wallets»

Bob has a wallet with 2022 NSUcoins. He decided to open a lot of new wallets and spread his NSUcoins among them. The platform that operates his wallets can distribute content of any wallet between 2 newly generated ones, charging 1 NSUcoin commission and removing the initial wallet.

He created a lot of new wallets, but suddenly noticed that all of his wallets contain exactly 8 NSUcoins each. Bob called the platform and told that there might be a mistake. How did he notice that?



Problem 3. «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

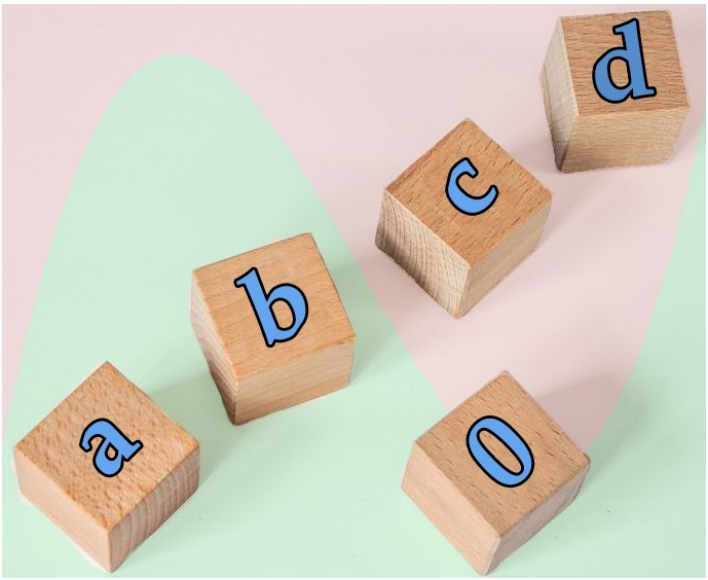
$$f(x-y) - 2f(x)f(y) + f(1+xy) = 1 \pmod{37} \text{ for any integers } x, y.$$

Decrypt the message that Bob has received.

Problem 4. «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 5. «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.

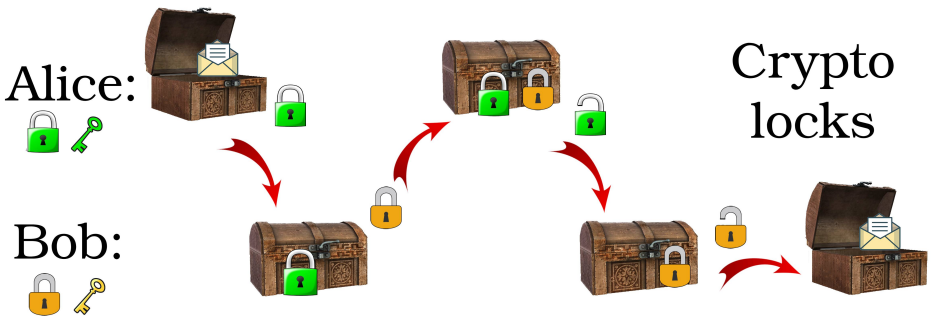
Unfortunately, Eve was eavesdropping in the next apartment and, after Charlie had left, she immediately found out Alice pin code despite that she had never seen those chandelier and bookshelf. Could you find the pin code too?

Problem 6. «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.