Problem 1. «A digital signature»

Alice uses a new digital signature algorithm that turns a text message M into a pair (M, s), where s is an integer and generated in the following way:

1. The special function h transforms M into a big positive integer $r = h(M)$.

2. The number $t = r^2$ is calculated, where $t = \overline{t_1 t_2 \dots t_n}$.

3. The signature s is calculated as $s = t_1 + t_2 + \dots + t_n$.

Bob obtained the signed message

(`Congratulations on the fifth year anniversary of NSUCRYPTO!`, 2018)

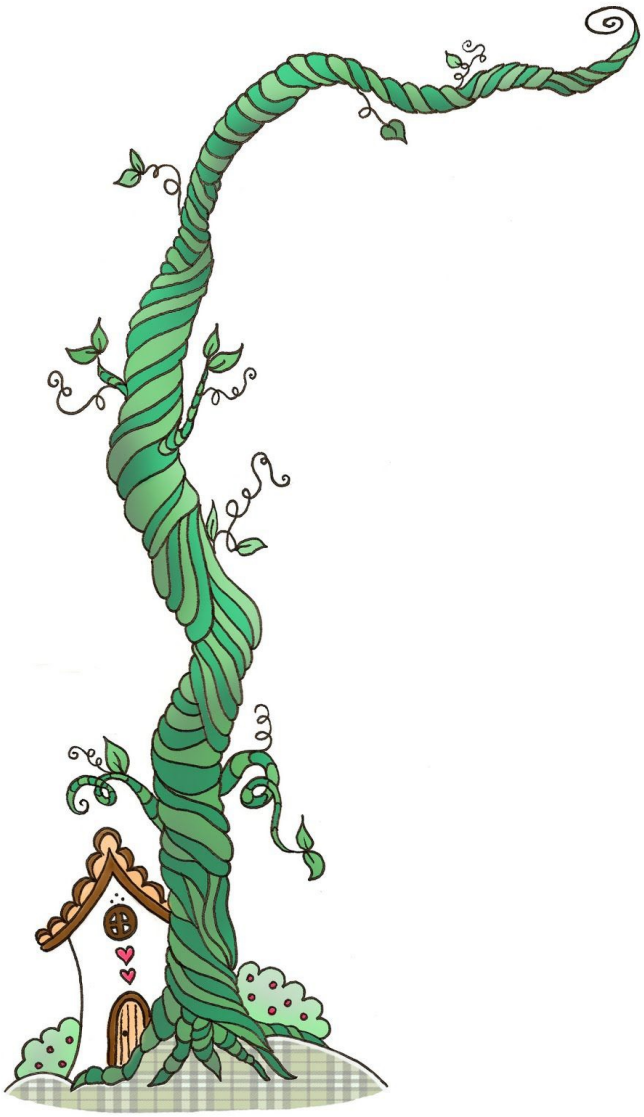
from Alice and immediately recognized that something was wrong with the signature! How did he discover it?

A remark. By $t = \overline{t_1 t_2 \dots t_n}$ we mean that $t_1, t_2, \dots, t_n$ are decimal digits and all digits over the bar form decimal number t.

Problem 2. «Jack and the Beanstalk»

Little Jack is only 7 years old and likes solving riddles involving the powers of 2. Recently, his uncle Bitoshi gave him sixteen BeanCoin seeds and promised that Jack can collect all BeanCoins which will grow from these seeds. But in order for BeanCoins to grow big and fruitful, Jack must plant the seeds in the garden in a special way. He have to draw eight lines on the ground and plant all sixteen seeds on these lines in such a way that each of the lines contains exactly four seeds.

Can you help Jack to achieve his goal and suggest how to plant the seeds?



Problem 3. «Key matrices»

Let n be an **odd** positive integer. In some cipher, a key is a binary $n \times n$ matrix

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{pmatrix},$$

where $a_{i,j}$ is either 0 or 1, such that each diagonal of any length $1, 2, \dots, n-1, n$ contains an **odd** number of 1s.

What is the minimal and the maximal number of 1s that can be placed in a key matrix A?

Example. For $n = 3$, diagonals are the following ten lines:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

Problem 4. «A sequence»

Two friends, Roman and Anton, are very interested in sequences and ciphers. Their new cryptosystem encrypts binary messages of length n, $X = (x_1, x_2, \ldots, x_n)$, where each x_i is either 0 or 1. A key K of the cipher is a set of n integers $a_1, a_2, \ldots, a_n$. The ciphertext C for the message X encrypted with the key K is the integer

$$Y = x_1 \cdot a_1 + x_2 \cdot a_2 + \ldots + x_n \cdot a_n.$$

Roman and Anton change their key regularly. Today, the key K is defined by

$$a_i = 2^i + (-1)^i \quad \text{for all } i = 1, \ldots, n.$$

The friends can easily decipher any message using the key defined by this sequence for any n!

1. Prove that the encryption is correct for this key K for any n: there are no two distinct input messages X^1 and X^2 such that their ciphertexts C^1 and C^2 are equal, i. e. $C^1 = C^2$.

2. Describe an algorithm which can be used to easily decipher any ciphertext C encrypted with today's key K. Here "easily" means that the algorithm should work much faster than checking all possible variants for an input message X.

Problem 5. «Solutions of the equation»

Alice is studying special functions that are used in symmetric ciphers. Let E^n be the set of all binary vectors $x = (x_1, x_2, \ldots, x_n)$ of length n, where x_i is either 0 or 1. Given two vectors x and y from E^n consider their sum $x \oplus y = (x_1 \oplus y_1, \ldots, x_n \oplus y_n)$, where $\oplus$ is addition modulo 2.

Example. If $n = 3$, then $E^3 = \{(000), (001), (010), (011), (100), (101), (110), (111)\}$. Let $x = (010)$ and $y = (011)$, then vector $x \oplus y$ is equal to $(010) \oplus (011) = (0 \oplus 0, 1 \oplus 1, 0 \oplus 1) = (001)$.

We will say that a function F maps E^n to E^n if it transforms any vector x from E^n into some vector $F(x)$ from E^n.

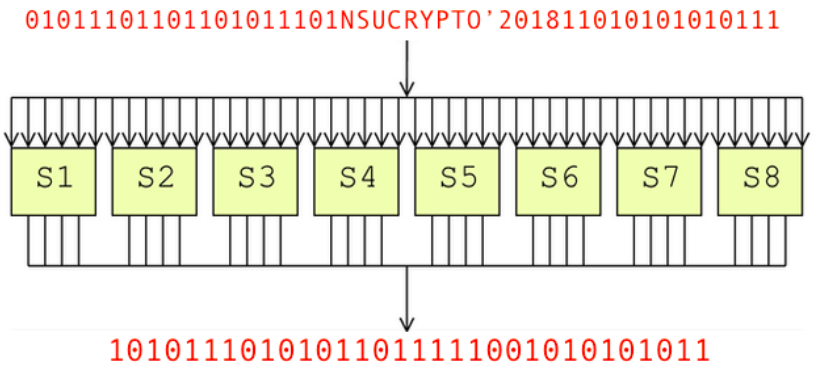
Example. Let $n = 2$. For instance, we can define F that maps E^2 to E^2 as follows: $F(00) = (00)$, $F(01) = (10)$, $F(10) = (11)$ and $F(11) = (10)$.

Alice found a function S that maps E^6 to E^6 in such a way that the vectors $S(x)$ and $S(y)$ are not equal for any nonequal vectors x and y. Also, S has another curious property: the equation

$$S(x) \oplus S(x \oplus a) = b$$

has either 0 or 2 solutions for any nonzero vector a from E^6 and any vector b from E^6.

Find the number of pairs (a, b) such that this equation has exactly **2** solutions!



Problem 6. «Stickers»

Bob always takes into account all the recommendations of security experts. He switched from short passwords to long passphrases and changes them every month. Bob usually chooses passphrases from the books he is reading. Passphrases are so lengthy and are changed so often! In order to not forget them, Bob decided to use stickers with hints. He places them on his monitors (ooh, experts...). The only hope is that Bob's hint system is reliable because it uses encryption. But is that true? Could you recover Bob's current passphrase from the photo of his workspace?