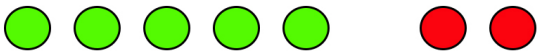
Problem 1. «Have a look and read!»



```
V R L E A T D _ I E M Q U
I I R P _ M K E O N T T _
E S L O N B I O K L O - P
V . , _ _ I S T O _ V W A
I S E _ T N _ O S T C _ D
I E E C N R T Y I P S T E
T D , _ _ D I U N R V I N
E G N _ T T E H D E _ _ S
T E H C E O _ N U D N _ W
I O Q R U L E D _ _ S W A
E R C .
```

Problem 2. «Two strings»

Carol takes inspiration from different strings and comes up with unusual ways to build them. Today, she starts with a binary string A_n constructed by induction in the following way. Let $A_1 = 0$ and $A_2 = 1$. For $n > 2$, the string A_n is defined by concatenating the strings A_{n-1} and A_{n-2} from left to right, i. e. $A_n = A_{n-1}A_{n-2}$.

Together with A_n consisting of "0"s and "1"s, Carol constructs a ternary string B_n consisting of "-1"s, "0"s and "1"s. Let $A_n = a_1...a_m$ for appropriate m, where $a_i \in \{0, 1\}$; then $B_n = b_1...b_\ell$, where $\ell = \lceil m/2 \rceil$ and $b_i \in \{-1, 0, 1\}$ is defined as follows:

$$b_i = a_{2i-1} - a_{2i} \text{ for } i = 1, ..., \ell \text{ (the exceptional case } b_\ell = a_m \text{ if } m \text{ is odd).}$$

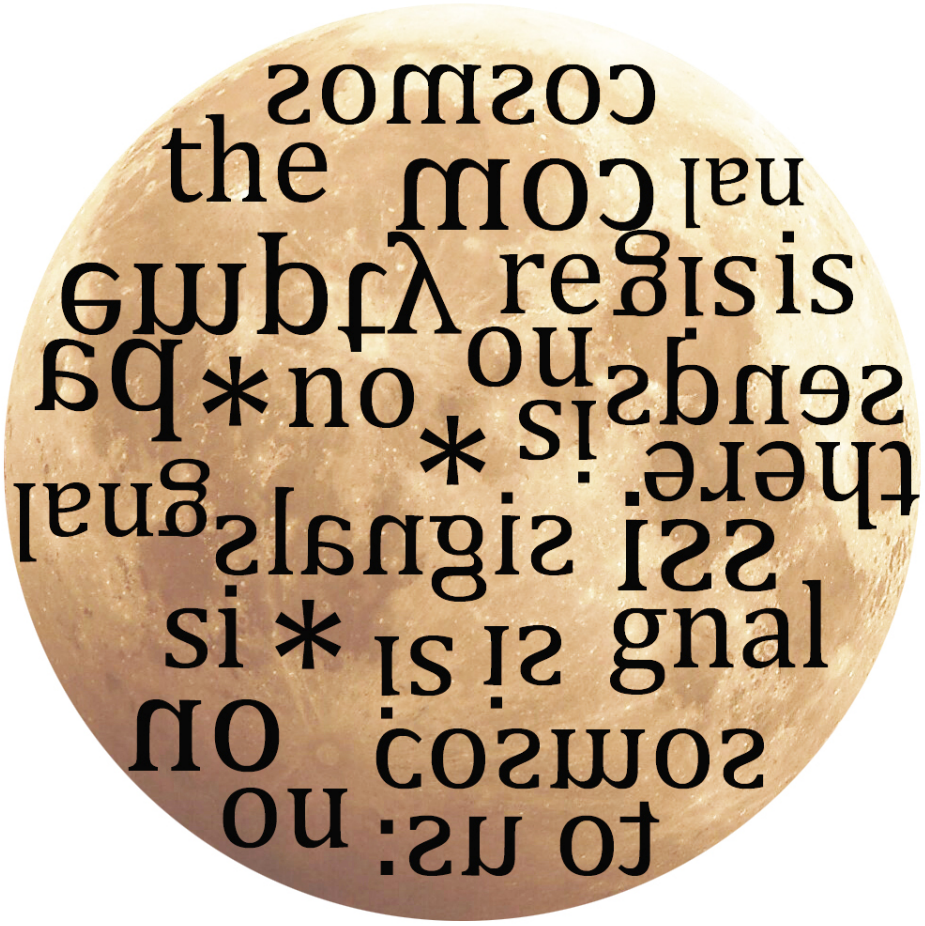
Help Carol to find all n such that B_n has the same number of "1"s and "-1"s.

Example. The strings A_n and B_n for small n are the following:

$A_3 = A_2A_1 = 10$,	$A_4 = A_3A_2 = 101$,	$A_5 = A_4A_3 = 10110$,	$A_6 = A_5A_4 = 10110101$.
$B_3 = 1$,	$B_4 = 11$,	$B_5 = 100$,	$B_6 = 10(-1)(-1)$.

Problem 3. «A space message»

What message do you get?



Problem 4. «Elliptic curve points»

Alice is studying elliptic curve cryptography. Her task for today is in practice with basic operations on elliptic curve points. Let $\mathbb{F}_p$ be the finite field with p elements ($p > 3$ prime). Let $E/\mathbb{F}_p$ be an elliptic curve in Weierstrass form, that is a curve with equation $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$. Recall that the affine points on E and the point $\mathcal{O}$ at infinity form an abelian group, denoted

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 \colon y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\} \ .$$

Assume that $b = 0$. Let $R \in E(\mathbb{F}_p)$ be an element of odd order, $R \neq \mathcal{O}$. Consider $H = \langle R \rangle$ that is the subgroup generated by R.

Help Alice to show that if $(u, v) \in H$, then u is a quadratic residue mod p.

Remark. For the Weierstrass form, $P_1 + P_2$ for $P_1, P_2 \in E(\mathbb{F}_p)$ is calculated as follows:

- $P_1 + \mathcal{O} = P_1$.
  Next, we assume that $P_1, P_2 \neq \mathcal{O}$ and $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$.
- $P_1 + (-P_1) = \mathcal{O}$. Note that $-(x_1, y_1) = (x_1, -y_1)$.
  Next, we assume that $P_1 \neq -P_2$.
- $P_1 + P_1 = P_3 = (x_3, y_3)$ can be calculated in the following way:

$$x_3 = \frac{(3x_1^2 + a)^2}{(2y_1)^2} - 2x_1, \qquad y_3 = -y_1 - \frac{3x_1^2 + a}{2y_1}(x_3 - x_1).$$

  Next, we assume that $P_1 \neq P_2$.
- $P_1 + P_2 = P_3 = (x_3, y_3)$ can be calculated in the following way:

$$x_3 = \frac{(y_2 - y_1)^2}{(x_2 - x_1)^2} - x_1 - x_2, \qquad y_3 = -y_1 - \frac{y_2 - y_1}{x_2 - x_1}(x_3 - x_1).$$

Problem 5. «The number of rounds»

A famous cryptographer often encrypts his personal data using his favourite block cipher. The block cipher has three variants with $r_1 = 10$, $r_2 = 12$ and $r_3 = 14$ rounds. On this occasion, the cryptographer no longer remembers which of the variants he used.

Fortunately, the cryptographer did ask his students to write down the number of rounds for him. However, in a creative mood, the students decided to encrypt it using a custom cipher E_k with a 4-bit block size. As illustrated in Figure below, round i of their construction XORs the i^{th} nibble k_i of the key $k = k_1 \| k_2 \| \ldots \| k_{r+1}$ with the state and then applies the function S given in Table below. Lacking confidence in their own abilities, the students decided to instantiate the cipher E_k with $r = r_1 \cdot r_2 \cdot r_3 + 1 = 1681$ rounds.

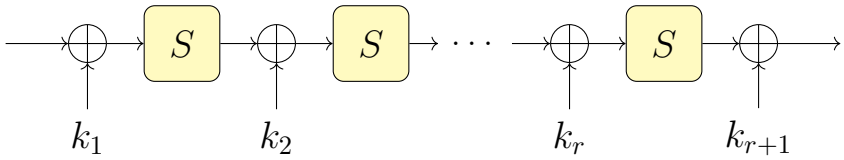


Figure: The students' encryption method.

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	3	e	6	8	0	c	b	4	1	d	5	a	7	9	f	2

Table: Lookup table for the function S (in hexadecimal notation).

The students wrote down that the encryption of $r_1 = 10$ is 5 and of $r_2 = 12$ is 0, that is $E_k(1,0,1,0) = (0,1,0,1)$ and $E_k(1,1,0,0) = (0,0,0,0)$. Of course, the students forgot the key, but they still remember that it was an ASCII-encoding of a passphrase consisting only of upper- and lower case English letters. After hearing this, the famous cryptographer exclaims that the students have made a mistake.

How did he know that something was wrong?

Problem 6. «A present for you!»

Alice wants to implement the lightweight block cipher PRESENT on a chip. She starts with the bit permutation that is defined in Table and illustrated in Figure below. Clearly, many lines are intersecting, and this would cause a short circuit if the lines were metal wires. Is it possible to avoid this problem by using several "layers," i.e., parallel planes? That is to draw the lines without intersections on each layer. We assume that

- the work area is a rectangle bounded by the lines where input and output bits are placed and the lines of the outermost connections $P(0) = 0$ and $P(63) = 63$;
- input and output bits are ordered; connections are represented by arbitrary curves;
- color of a line indicates the number of its layer, a line can change color several times;
- the point where a line changes color indicates a connection from one layer to another.

Q1 What is the minimun number of layers required for implementing in this way the PRESENT bit permutation?

Q2 Find a systematic approach how to draw a valid solution for the minimum number of layes found in **Q1** and present the drawing!

For your help (but not necessarily), you can use a specific online tool and download the PRESENT bit permutation as in Figure.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

Table: Definition of the bit permutation used in PRESENT.
Bit i is moved to bit position $P(i)$.

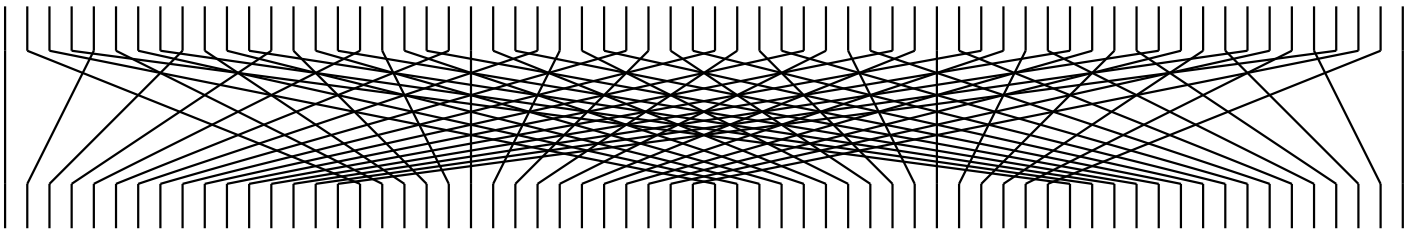
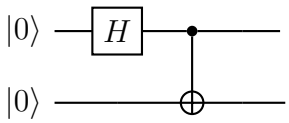


Figure: Illustration of the bit permutation used in PRESENT

Problem 7. «Try your quantum skills!»

In oder to use the quantum cryptanalysis techniques one should be able to work with quantum bits. Daniel knows little about quantum circuits but wants to try his hand at a new field! **A quantum circuit** is a scheme where we operate with some set of qubits. The operations include one- or multi-qubit transformations provided by so called **quantum gates**. They are characterized by unitary operators that act on the space of qubits. An example of a quantum circuit is the following:



$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

It transforms the state $|00\rangle$ to the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The upper wire corresponds to the action on the first qubit while the lower corresponds to the second one. Here, we have the following transformations: $|00\rangle \xrightarrow{H,\text{ 1st qubit}} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \xrightarrow{CNOT,\text{ both qubits}} \frac{1}{\sqrt{2}} CNOT\,|00\rangle + \frac{1}{\sqrt{2}} CNOT\,|10\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Q1 Given the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, design a circuit that transforms $|\psi\rangle$ to the state $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

Q2 Design the circuit that distinguishes between the entangled states $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ and $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Distinguishing means that after the measurement of the final state we can exactly say what the state from these three was given. Use the list of gates presented below.

Remark. 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 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 $|a\rangle \otimes |b\rangle \equiv |ab\rangle$.

Pauli-X gate	$\|x\rangle$ — X — $\|x \oplus 1\rangle$	acts on a single qubit in the state $\|x\rangle$, $x \in \{0, 1\}$
Pauli-Z gate	$\|x\rangle$ — Z — $(-1)^x \|x\rangle$	acts on a single qubit in the state $\|x\rangle$, $x \in \{0, 1\}$
Hadamard gate	$\|x\rangle$ — H — $\frac{\|0\rangle + (-1)^x \|1\rangle}{\sqrt{2}}$	acts on a single qubit in the state $\|x\rangle$, $x \in \{0, 1\}$
controlled NOT (CNOT) gate	$\|x\rangle$ — $\|x\rangle$; $\|y\rangle$ — $\|y \oplus x\rangle$	acts on a pair of qubits in the states $\|x\rangle, \|y\rangle$, $x, y \in \{0, 1\}$
SWAP gate	$\|x\rangle$ — $\|y\rangle$; $\|y\rangle$ — $\|x\rangle$	acts on a pair of qubits in the states $\|x\rangle, \|y\rangle$, $x, y \in \{0, 1\}$