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	.									

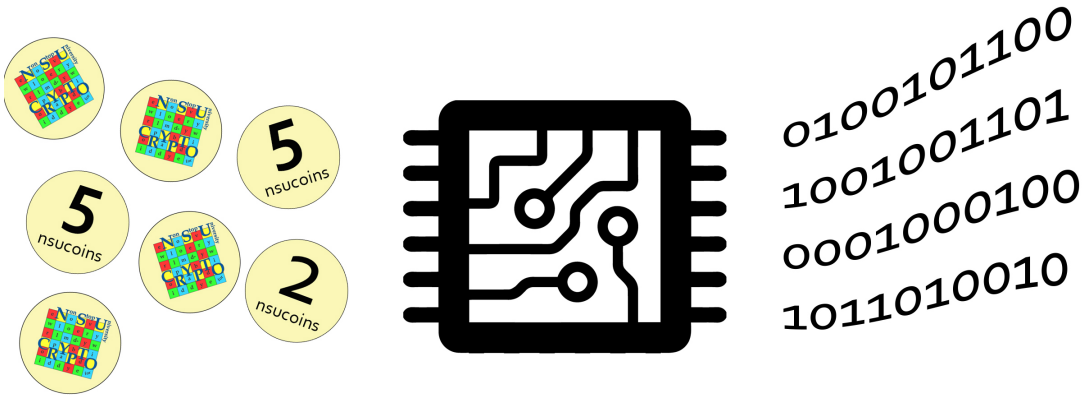
Problem 2. «2021-bit key»

A pseudo-random generator produces sequences of bits (that is of 0 and 1) step by step. To start the generator, one needs to pay 1 *nsucoin* and the generator produces a random bit (that is a sequence of length 1). Then, given a generated sequence S of length ℓ, $\ell \geqslant 1$, one of the following operations can be applied on each step:

1. A random sequence of 4 bits is added to S, so a new sequence S' has length $\ell + 4$. The charge for using this operation is 2 *nsucoins*.

2. A random sequence of 2ℓ bits is added to S, so a new sequence S' has length 3ℓ. The charge for using this operation is 5 *nsucoins*.

Bob needs to generate a secret key of length exactly 2021 bits for his new cipher. What is the minimal number of *nsucoins* that he has to pay for the key?



Problem 3. «A conundrum»

Can you crack a conundrum?

b tn ztwobfc twxfc t hutek vptbwbfc t svbeo hukbfq nu vx ntpo xlv
wbfus b ztwo 6 nuvpus fxpvk vkuf 2 nuvpus zusv 5 nuvpus utsv 6 nuvpus sxlvk
3 nuvpus utsv 6 nuvpus fxpvk 4 nuvpus utsv 3 nuvpus sxlvk 3 nuvpus zusv
3 nuvpus fxpvk 6 nuvpus sxlvk 3 nuvpus fxpvk 4.24 nuvpus sxlvkutsv
3 nuvpus utsv 1 nuvpu zusv 6 nuvpus fxpvk 1 nuvpu zusv 3 nuvpus utsv
6 nuvpus sxlvk 6 nuvpus fxpvk 6.49 nuvpus sxlvksxlvkutsv 6 nuvpus fxpvk
4 nuvpus utsv 3 nuvpus zusv 6 nuvpus sxlvk 3 nuvpus utsv 3 nuvpus fxpvk tfq
1 nuvpu zusv zktv bs vku ftnu vktv b ktau zpbvvuf bf vku stfq?

Above is the conundrum sent by Alice to Bob. Find an answer to Alice's question!

Problem 4. «Related passwords»

Tim and Ann want to create curiously related passwords for their cryptosystem. A password is a 9-digit decimal number. To start, they choose a random number $e_1e_2...e_9$ that has nine (not necessarily distinct) decimal digits.

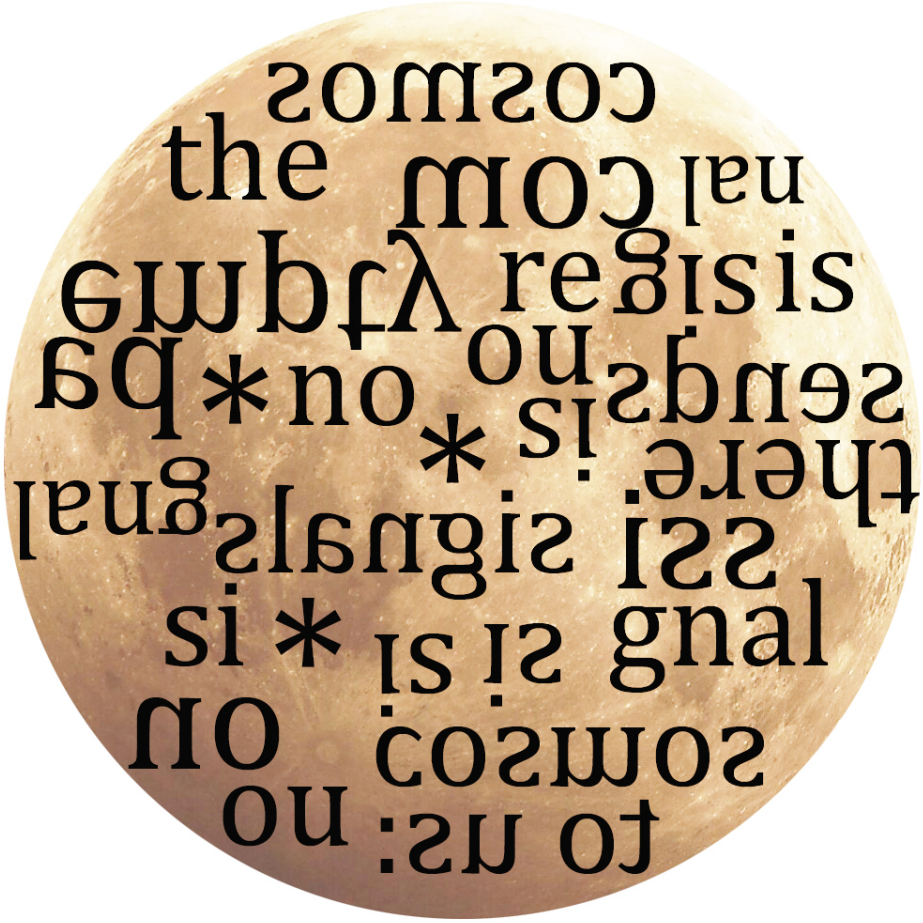
- Tim finds a password $d_1d_2...d_9$ such that each of the numbers formed by replacing just one of the digits d_i in $d_1d_2...d_9$ by the corresponding digit e_i is divisible by 7.
- Ann finds a password $f_1f_2...f_9$ in similar but not the same way: each of the nine numbers formed by replacing one of the e_i in $e_1e_2...e_9$ by f_i is divisible by 7.

Show that for each i, $d_i - f_i$ is divisible by 7 for any of Tim's and Ann's passwords!

Example. Let $e_1e_2...e_9 = 448259545$. Then Tim's password can be $d_1d_2...d_9 = 199501996$ and Ann's password can be $f_1f_2...f_9 = 822571226$.

Problem 5. «A space message»

What message do you get?



Problem 6. «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:

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

Problem 7. «A small present for you!»

Alice wants to implement the lightweight block cipher SMALL-PRESENT on a chip. She starts with the bit permutation that is illustrated in Figure below. For example, the input bit number 4 is moved to the output bit number 1, bit 6 is moved to 9 and so on. 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 $0 \to 0$ and $15 \to 15$;
- 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 SMALL-PRESENT bit permutation?

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

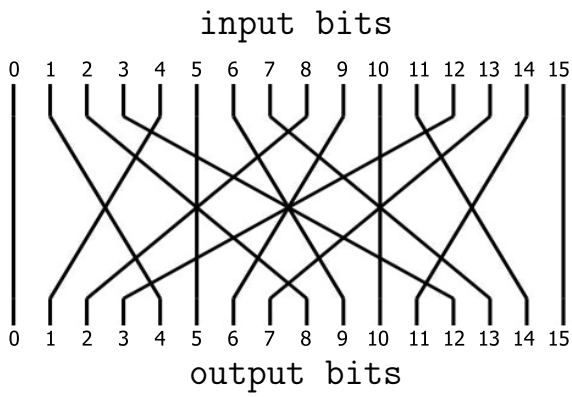


Figure: Illustration of the bit permutation used in SMALL-PRESENT