Task 1. «A hidden message»

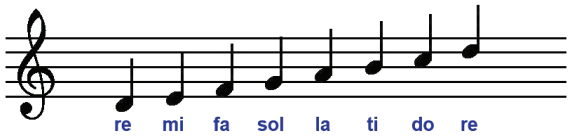
CrYPtogRapHY iS a ScIEnce Of «seCrET wriTinG». FOr aT Least Two THoUsANd yeaRS ThErE haVE bEeN peOPlE WHo WAnTeD to SEnd MESsaGes WHiCh coUlD oNly bEen rEAd bY tHe pEOPLe FoR whOm tHey were iNteNdeD. a loT oF different MEtHODs FoR coNcEalING mEssageS WerE invENtED stARTING WIth AnCIeNt cIPHerS lIKE «SkytaLE» and «ATBAsH» and ending wiTH MOdErn SymmeTRiC ANd PubliC-kEy enCRYptioN ALGOriTHmS SUch aS AeS and Rsa. the dEVELopMENT Of crYPtOgRaPHy cOntiNueS And NEVER sTopS! decrYPt THe mESsaGe tHat iS hIDdEn in thE teXT oF this TASk! tHE aLphabet FoR THE mEssAGE ConsisTs of ALl tWEnTy six enGliSh letTERS from «a» To «z» ANd Six puNCTuaTIoN MARkS « », «.», «,», «!», «?», «'».

Task 2. «A crypto room»

You are in a crypto room with a secret message in hands. Decrypt it!

Task 3. «The musical notation»

Alice and Bob invented a new way for encrypting messages based on musical notations of melodies. They are not very good in musical notations but they know the basic notes «do», «re», «mi», «fa», «sol», «la», «ti», and their places in the staff:



To encrypt a message of length n in English alphabet Alice chooses a melody consisting of n notes. She writes a message under the musical notation of the melody in such a way that each letter of the message corresponds to exactly one note's position in the musical notation. Then for each note («do», «re», ..., «ti») Alice forms the ordered group of corresponding letters. Further she takes a random integer number k_i, $i = 1, \ldots, 7$, and cyclically shifts letters in the i-th group on k_i positions to the right. After that Alice forms the ciphertext by writing letters of the shifted groups under the musical notation again.

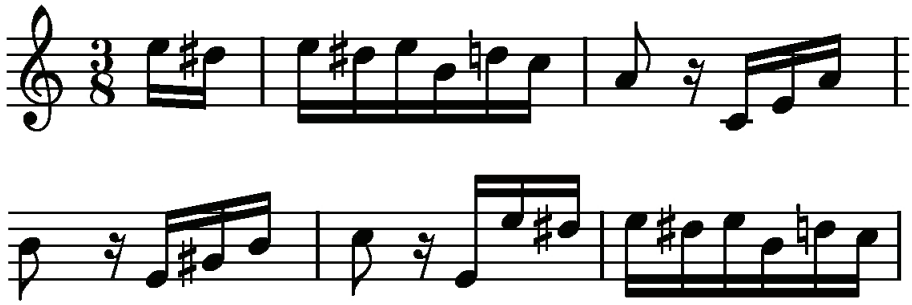
An example. Suppose that Alice wants to send the message `H E L L O`.

The group for «re» is (`E`, `L`); for «mi» — (`H`, `L`, `O`). Alice takes random numbers 2 and 1 for «re» and «mi» respectively. After shifting she gets groups (`E`, `L`) and (`O`, `H`, `L`).
Hence the ciphertext for the message is `O E H L L`.

Decrypt the following ciphertext sent to Bob by Alice:

`R O L E L I S E O E E E H T O M V C P B D E F S O N`

It is known that Alice used the musical notation below.



Task 4. «Linear subspaces»

For constructing a new secret sharing scheme Mary has to solve the following task on binary vectors. Let n be an integer number, $n \geqslant 2$. Let $\mathbb{F}_2^{2n}$ be a $2n$-dimensional vector space over $\mathbb{F}_2$, where $\mathbb{F}_2 = \{0, 1\}$ is a prime field of characteristic 2.

Do there exist subsets $L_1, \ldots, L_{2^n+1}$ of $\mathbb{F}_2^{2n}$ such that the following conditions hold

1. L_i is a linear subspace of dimension n for every $i \in \{1, \ldots, 2^n + 1\}$;
2. $L_i \cap L_j = \{\mathbf{0}\}$ for all $i, j \in \{1, \ldots, 2^n + 1\}$, $i \neq j$;
3. $L_1 \cup \ldots \cup L_{2^n+1} = \mathbb{F}_2^{2n}$?

If «yes», show how to construct these subspaces for an arbitrary integer n.

Remark I. Recall several definitions and notions. Each element $x \in \mathbb{F}_2^k$ is a binary vector of length k, i. e. $x = (x_1, \ldots, x_k)$, where $x_1, \ldots, x_k \in \mathbb{F}_2$. For two vectors x and y of length k their sum is $x \oplus y = (x_1 \oplus y_1, \ldots, x_k \oplus y_k)$, where $\oplus$ stands for XOR operation. Let $\mathbf{0}$ be the zero element of the vector space, i. e. vector with all-zero coordinates. A nonempty subset $L \subseteq \mathbb{F}_2^k$ is called a *linear subspace* if for any $x, y \in L$ it holds $x \oplus y \in L$. It is easy to see that zero vector belongs to every linear subspace. A linear subspace L of $\mathbb{F}_2^k$ has *dimension* n if it contains exactly 2^n elements.

Remark II. For example the case $n = 2$ we consider together. In the vector space $\mathbb{F}_2^4$ we can choose the following 5 required subspaces:

$$L_1 = \{(0000), (0001), (1110), (1111)\};$$
$$L_2 = \{(0000), (0010), (1001), (1011)\};$$
$$L_3 = \{(0000), (0011), (0100), (0111)\};$$
$$L_4 = \{(0000), (0101), (1000), (1101)\};$$
$$L_5 = \{(0000), (0110), (1010), (1100)\}.$$

Task 5. «The number of solutions»

Let $\mathbb{F}_{256}$ be the finite field of characteristic 2 with 256 elements. Consider the function

$$F : \mathbb{F}_{256} \to \mathbb{F}_{256} \text{ such that } F(x) = x^{254}.$$

Since $x^{255} = 1$ for all nonzero $x \in \mathbb{F}_{256}$, we have $F(x) = x^{-1}$ for all nonzero elements of $\mathbb{F}_{256}$. Further, we have $F(0) = 0$.

Alice is going to use the function F as an S-box (that maps 8 bits to 8 bits) in a new block cipher. But before she wants to find answers to the following questions.

- How many solutions may the equation

$$F(x + a) = F(x) + b \tag{1}$$

  have for all different pairs of nonzero parameters a and b, where $a, b \in \mathbb{F}_{256}$?

- How many solutions does the equation (1) have for the function $F(x) = x^{2^n-2}$ over the finite field $\mathbb{F}_{2^n}$ for an arbitrary n?

Please, help to Alice!

Task 6. «A special parameter»

In differential cryptanalysis of block ciphers a special parameter P is used to measure the diffusion strength. In this task we study its properties.

Let n, m be positive integer numbers. Let $a = (a_1, \ldots, a_m)$ be a vector, where a_i are elements of the finite field $\mathbb{F}_{2^n}$. Denote by $\mathrm{wt}(a)$ the number of nonzero coordinates a_i, $i = 1, \ldots, m$, and call this number the *weight* of a.

We say that $a, b \in \mathbb{F}_{2^n}^m$ represent *states*. The sum of two states a, b is defined as $a + b = (a_1 + b_1, \ldots, a_n + b_n)$.

Thus, the *special parameter* P of a function $\varphi : \mathbb{F}_{2^n}^m \to \mathbb{F}_{2^n}^m$ is given by

$$P(\varphi) = \min_{a,\, b,\, \text{such that } a \neq b} \{\mathrm{wt}(a + b) + \mathrm{wt}(\varphi(a) + \varphi(b))\}.$$

- Rewrite (simplify) the definition of $P(\varphi)$ when the function φ is linear (recall that a function ℓ is linear if for any x, y it holds $\ell(x + y) = \ell(x) + \ell(y)$).
- Rewrite the definition of $P(\varphi)$ in terms of linear codes, when the linear transformation φ is given by a $m \times m$ matrix M over $\mathbb{F}_{2^n}$, i. e. $\varphi(x) = M \cdot x$.
- Let φ be an arbitrary function. Find a tight upper bound for $P(\varphi)$ as a function of m.
- Can you give an example of the function φ with the maximal possible value of P?

Task 7. «S-box masking»

To provide the security of a block cipher to the side channel attacks, some ideas on masking of elements of the cipher are exploited. Here we discuss masking of S-boxes.

Alice takes a bijective function S (S-box) that maps n bits to n bits. Bob claims that for every such a function S there exist two bijective S-boxes, say S' and S'', mapping n bits to n bits, such that it holds

$$S(x) = S'(x) \oplus S''(x) \text{ for all } x \in \mathbb{F}_2^n.$$

Hence, Alice is able to mask an arbitrary bijective S-box by "dividing it into parts" for realization. But Alice wants to see the proof of this fact. Please help to Bob in giving the arguments.

Task 8. «Add-Rotate-Xor»

Let $\mathbb{F}_2^n$ be the vector space of dimension n over $\mathbb{F}_2 = \{0, 1\}$. A vector $x \in \mathbb{F}_2^n$ has the form $x = (x_1, x_2, \ldots, x_n)$, where $x_i \in \mathbb{F}_2$. This vector can be interpreted as the integer $x_1 \cdot 2^{n-1} + x_2 \cdot 2^{n-2} + \ldots + x_{n-1} \cdot 2 + x_n$.

Alice can implement by hardware the following functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ for all vectors $a, b \in \mathbb{F}_2^n$ and all integers r, $0 < r < n$:

1) $f_a(x) = x \boxplus a$ — addition of vectors x and a as integers modulo 2^n for a fixed a;

2) $g_r(x) = x \lll r$ — cyclic rotation of a vector x to the left by r positions for a fixed positive integer r;

3) $h_b(x) = x \oplus b$ — coordinate-wise sum of vectors x and b modulo 2 for a fixed b.

- Bob asks Alice to construct two devices that compute the functions S_1 and S_2 from $\mathbb{F}_2^2$ to $\mathbb{F}_2^2$ given by their truth table:

x	(00)	(01)	(10)	(11)
$S_1(x)$	(01)	(00)	(10)	(11)
$S_2(x)$	(01)	(11)	(00)	(01)

  Can Alice do it? If «yes», show how it can be done; if «no», give an explanation!

- Generalizing the problem above: can we construct any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ using only a finite number of compositions of functions f_a, g_r and h_b?

  And what about any permutation over $\mathbb{F}_2^n$?

  Consider at least the cases $n = 2, 3, 4$.

- Is it possible to compute every function h_b using only functions f_a and g_r?