УДК 519.7 DOI 10.17223/20710410/29/4

PROBLEMS, SOLUTIONS AND EXPERIENCE OF THE FIRST INTERNATIONAL STUDENT'S OLYMPIAD IN CRYPTOGRAPHY[1]

S. Agievich*, A. Gorodilova**, N. Kolomeec**,***, S. Nikova****, B. Preneel****,
V. Rijmen****, G. Shushuev**,***, N. Tokareva**,***, V. Vitkup**

*Belarusian State University, Minsk, Belarus,
**Sobolev Institute of Mathematics, Novosibirsk, Russia,
***Novosibirsk State University, Novosibirsk, Russia,
****University of Leuven, KU Leuven, Belgium

A detailed overview of the problems, solutions and experience of the first international student's Olympiad in cryptography, NSUCRYPTO'2014, is given. We start with the rules of participation and the description of rounds. All 15 mathematical problems of the Olympiad and their solutions are considered in detail. The problems are about differential characteristics of S-boxes, S-box masking, relations between cyclic rotation and additions modulo 2 and 2^n, special linear subspaces in $\mathbb{F}_2^n$, the number of solutions of the equation $F(x)+F(x+a)=b$ over the finite field $\mathbb{F}_{2^n}$ and APN functions. Some unsolved problems in symmetric cryptography are also considered.

Keywords: *cryptography, block ciphers, Boolean functions, AES, Olympiad, NSUCRYPTO.*

Introduction

The First Siberian Student's Olympiad in Cryptography with International participation — NSUCRYPTO'2014 was held on November 2014. There exist several school competitions in cryptography and information security, but this one is the first cryptographic Olympiad for students and professionals. The aim of the Olympiad was to involve students and young researchers in solving the curious and hard scientific problems of the modern cryptography. From the very beginning, the concept was not to stop on the training olympic tasks but to include unsolved research problems at the intersection of mathematics and cryptography.

In this article, we give a detailed overview of the Olympiad. We start with the rules of participation and the description of rounds. Then in two big sections, we discuss 15 problems of the Olympiad and their solutions. Among them, there are both some amusing tasks based on historical ciphers and hard mathematical problems.We consider mathematical problems related to cipher constructing such as studying differential characteristics of S-boxes, S-box masking, determining relations between cyclic rotation and additions modulo 2 and 2^n, constructing special linear subspaces in $\mathbb{F}_2^n$. Problems about the number of solutions of the equation $F(x) + F(x + a) = b$ over the finite field $\mathbb{F}_{2^n}$ and APN functions are discussed. Some unsolved problems are proposed. The problem about the special watermarking ciphers is one of them. All problems were developed by the Program committee of the Olympiad. Solution check was also its duty.

[1] Olympiad was supported by Novosibirsk State University. A. Gorodilova and N. Kolomeec thank RFBR grant No. 15-07-01328 and Grant NSh-1939.2014.1 of President of Russia for Leading Scientific Schools, G. Shushuev, N. Tokareva and V. Vitkup would like to thank RFBR grants No. 12-01-31097 and 15-31-20635 for the financial support.

Organizers of the Olympiad are Novosibirsk State University, Sobolev Institute of Mathematics (Novosibirsk), Tomsk State University, Belarusian State University and University of Leuven (KU Leuven, Belgium). Programm committee was formed by G. Agibalov, S. Agievich, N. Kolomeec, S. Nikova, I. Pankratova, B. Preneel, V. Rijmen, and N. Tokareva. Local organizing committee from Novosibirsk consisted of A. Gorodilova, N. Kolomeec, G. Shushuev, V. Vitkup, D. Pokrasenko and S. Filiyzin. N. Tokareva was the general chair of the Olympiad.

More than 450 participants from 12 countries were registered on the website of the Olympiad, `www.nsucrypto.nsu.ru`. Fifteen participants of the first round and eleven teams of the second round became winners and received prizes. The list of winners can be found in the last section of this paper.

NSUCRYPTO will be a regular annual Olympiad held on November. In 2015, it starts on November, 15. We invite pupils, students and professionals to participate!

1. Organization and rules of the Olympiad

Fig. 1.

Here we briefly formulate key points of the Olympiad. Its emblem is shown in Fig. 1.

Rounds of the Olympiad. There were two independent Internet rounds. The First round (duration 4 hours 30 minutes) was individual and consisted of two sections: school and student's. It was held on November, 16. Theoretical problems in mathematics of cryptography were offered to participants. The second, team, round (duration 1 week; November, 17–24) was devoted to hard research and programming problems of cryptography.

Everybody can participate! To become a participant of the Olympiad, it was necessary and sufficient to register on the website `www.nsucrypto.nsu.ru`. There were no restrictions on status and age of the participants. It means that senior pupils, students and all the others who are interested in cryptography were able to participate. Participants from any countries were welcome. During the registration, every participant had to choose his category: "senior pupil", "student" or "other / professional" and the section of the first round: "school" or "student's". The second round was common for all the participants.

Language of the Olympiad. All problems were given in English. But solutions could be written in English or Russian.

Format of the solutions. We accepted solutions in any electronic format (pdf, jpg, txt, rtf, docx, tex, etc). For example, a participant was able to write his solutions on a paper and send us a picture of it. Solutions should be written with all necessary details.

Prizes. There were several groups of prizes:

- for senior pupils — winners of the school section of the first round;
- for students — winners of the student's section of the first round;
- for participants in category "other / professional" — winners of the student's section of the first round;
- for participants (for every category separately) — winners of the second round;
- special prizes from the Programm committee for unsolved problems.

Interesting moments. Sometimes we were asked: "The Olympiad is via Internet. Are not you afraid that participants will use everything: supercomputers, books, articles, websites on cryptography?" In fact, we only welcome such an active mobilization of all possible resources in purpose of solving the tasks! We hope that, in a future, such a brainstorm will help to solve really hard cryptographic problems.

2. Problem structure of the Olympiad

There were 15 problems on the Olympiad. Some of them were included in both rounds.

Thus the school section of the first round consisted of 6 problems, whereas the student's section contained 8 problems. The first three problems were the same in each section (Tables 1, 2).

Table 1

Problems of the first round (school section)

N	Problem title	Maximal scores
1	A hidden message	4
2	A crypto room	4
3	The musical notation	4
4	Boolean cubes	4
5	A broken cipher machine	4
6	The Snowflake cipher	4

Table 2

Problems of the first round (student's section)

N	Problem title	Maximal scores
1	A hidden message	4
2	A crypto room	4
3	The musical notation	4
4	Linear subspaces	12
5	Number of solutions	8
6	A special parameter	10
7	S-box masking	8
8	Add–Rotate–Xor	10

The second round was composed of 11 problems (Table 3); it was common for all the participants. Three problems presented on the second round are unsolved (with declared special prizes from the Program Committee).

Table 3

Problems of the second round

N	Problem title	Maximal scores
1	Watermarking cipher	Special prize
2	APN permutation	Special prize
3	The Snowflake cipher	4
4	Number of solutions	8
5	Super S-box	Special prize
6	Boolean cubes	4
7	A special parameter	10
8	A pseudo-random generator	6
9	Add–Rotate–Xor	10
10	Linear subspaces	12
11	The musical notation	4

3. Problems

3.1. Problem “A hidden message” (4 scores)

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 “ ”, “.”, “,”, “!”, “?”, “’”.

3.2. Problem “A crypto room” (4 scores)

You are in a crypto room with a secret message in hands (Fig. 2). Decrypt it!

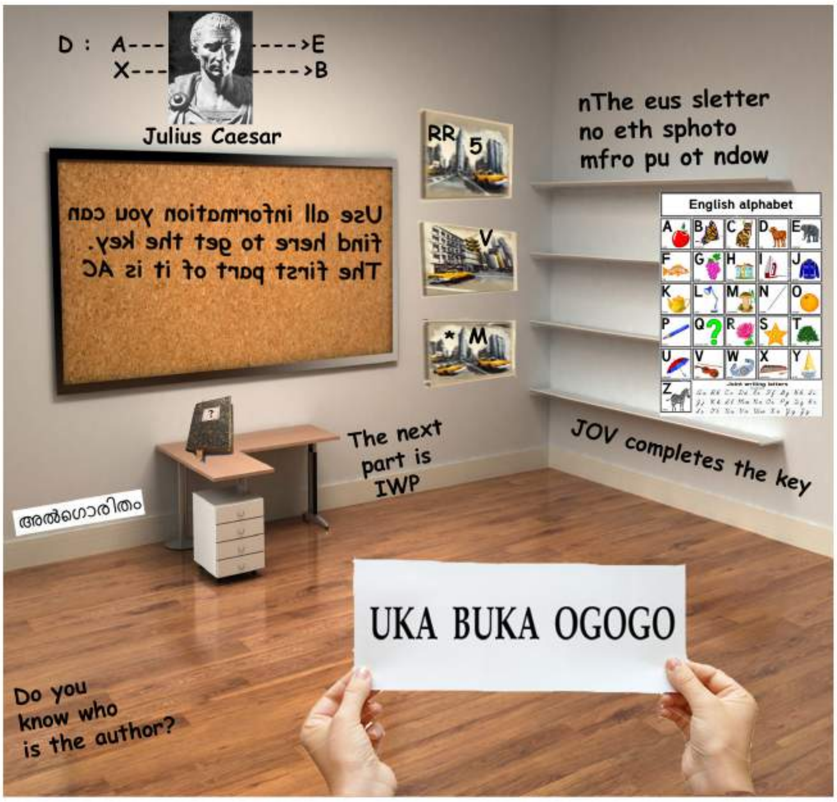
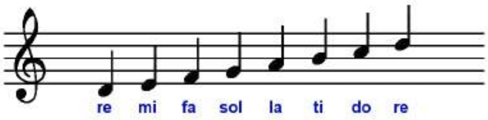


Fig. 2.

3.3. Problem “The musical notation” (4 scores)

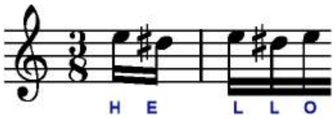
Alice and Bob invented a new way for encrypting messages based on musical notations of melodies. They are not very good in musical notations, but they know the basic notes “do”, “re”, “mi”, “fa”, “sol”, “la”, “ti” and their places in the staff:



To encrypt a message of length n in English alphabet, Alice chooses a melody consisting of n notes. She writes the 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 writes the row of the corresponding letters, takes a random integer number k_i for each $i = 1, \ldots, 7$, and cyclically shifts letters in the i-th row by k_i positions to the right. Finally, Alice forms the ciphertext, writing letters of the shifted sets under the musical notation again.

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

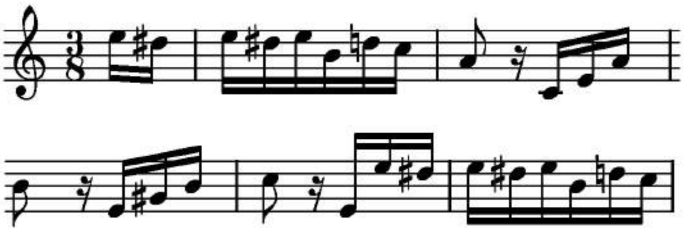
The row for "re" is (`E L`); for "mi" — (`H L O`). Alice takes random numbers 2 and 1 for "re" and "mi" respectively. After cyclical shifting to the right the first row by 2 positions and the second row by 1 position, she gets rows (`E L`) and (`O H L`). Hence, the ciphertext for the message is `O E 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.



3.4. Problem "Boolean cubes" (4 scores)

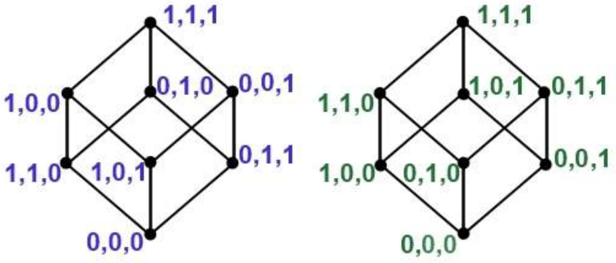
Alice has two cubes E_1 and E_2 of dimension 3 (Fig. 3). Their vertices have labels consisting of three integers; for example, (1,0,1) consists of integers 1, 0, 1. Consider an operation A that can be applied to a cube. The operation A contains three steps:

Step 1. Take an arbitrary edge of the cube;

Step 2. Take a number a which equals 1 or -1;

Step 3. Add a to an arbitrary position of the first vertex of the chosen edge. Add a to an arbitrary position of the second vertex of the edge.

Is it possible to get the cube E_2 from the cube E_1 by applying the operation A as many times as necessary? Give your arguments.



The cube E_1 **The cube E_2**

Fig. 3.

An example of applying the operation. Step 1. Take the edge $((1,0,0);(1,1,0))$. Step 2. Let $a=-1$. Step 3. For the vertex $(1,0,0)$, we choose the position 2 and, for the vertex $(1,1,0)$, we choose the position 1; after adding, the edge $((1,0,0);(1,1,0))$ becomes $((1,-1,0);(0,1,0))$ (Fig. 4).

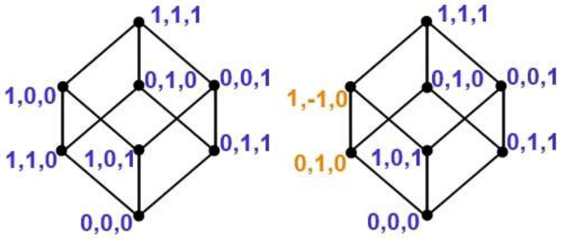


Fig. 4. An illustration of the example

3.5. Problem "A broken cipher machine" (4 scores)

Mary operates a cipher machine that encrypts messages like this:

Step 1. It represents a message as a natural number $n=\overline{abcdef\ldots}$;

Step 2. Then it adds all the digits in the number, $S_n=a+b+c+d+e+f+\ldots$;

Step 3. It inverts the order of digits in the number n and gets the number $n'=\overline{\ldots fedcba}$;

Step 4. As a result of the encryption, the machine prints the number $m=n'+2S_n$.

But now the cipher machine is broken: sometimes it works correctly, sometimes it prints a random number.

After encryption of her secret number n, Mary found out that the result m is the power of two,that is, $m=2^k$ for some integer k.

Determine: was the encryption correct in this case?

3.6. Problem "The Snowflake cipher" (4 scores)

Alice wants to encrypt some text using the Snowflake cipher. The encryption is described by the following algorithm:

Step 1. Choose an arbitrary small triangle in the snowflake (see Fig. 5);

Step 2. Put the first letter of your message into this triangle;

Step 3. Write the next letter of the message (without spaces) into an arbitrary empty neighbouring triangle. Neighbouring means having a common edge. Repeat this step until the end of the message.

Step 4. After inserting all the letters, write down the text from snowflake in horizontal order from top to bottom and from left to right.

Determine what is the maximal possible length of a message that can be encrypted with the Snowflake cipher?

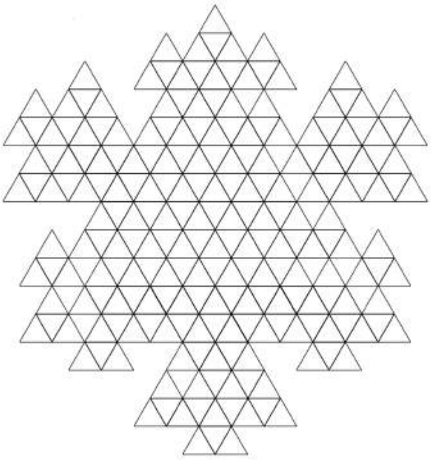


Fig. 5.

An example. We want to encrypt the message: `LOOK HOW IT WORKS`. As a result, we can get the ciphertext: `LHOWOOKITSKROW` (Fig. 6).

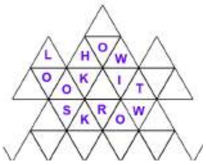


Fig.6.

3.7. Problem "A pseudo-random generator" (6 scores)

Alice and Bob communicate in Russia through the Internet, using some protocol. In the process of communication, Bob sends random numbers to Alice. It is known that Bob's pseudo-random generator works in the following way:

- it generates a binary sequence $u_0, u_1, u_2, \ldots$ such that, for some secret $c_0, \ldots, c_{15} \in \mathbb{F}_2$,
$$u_{i+16} = c_{15}u_{i+15} \oplus c_{14}u_{i+14} \oplus \ldots \oplus c_0 u_i \text{ for all integer } i \geqslant 0;$$
- i-th random number r_i, $i \geqslant 1$, is calculated as
$$r_i = u_{16i} + u_{16i+1}2 + u_{16i+2}2^2 + \ldots + u_{16i+15}2^{15};$$
- Bob initializes $u_0, u_1, \ldots, u_{15}$, using some integer number IV (initial value) from the interval $(1, 2^{16} - 1)$ in the same way, that is,
$$IV = u_0 + u_1 2 + u_2 2^2 + \ldots + u_{15}2^{15};$$
- it is known that, as the value of IV, Bob uses the number t modulo 2^{16}, where t is the number of seconds from January 1, 1970, 00:00 (in Bob's time zone) to his current time (in his time zone too).

Eve has intercepted the third and the fourth random numbers, namely $r_3 = 9\,731$ and $r_4 = 57\,586$. She lives in Novosibirsk and knows that Bob has initialized the generator on November 17, 2014, at about 12:05 UTC+6 up to several minutes. The number of seconds from January 1, 1970, 00:00 UTC+6 to November 17, 2014, 12:05 UTC+6 is equal to 1 416 225 900. Help Eve to detect Bob's time zone.

3.8. Problem "Number of solutions" (8 scores)

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 block cipher. But before doing this, 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 parameters a and b with nonzero values from $\mathbb{F}_{256}$?
- How many solutions does the equation (1) have for the function $F(x) = x^{2^n-2}$ over the field $\mathbb{F}_{2^n}$ with an arbitrary n?

  Please, help Alice!

3.9. Problem “S-box masking” (8 scores)

To provide the security of a block cipher against the side channel attacks, some ideas of masking elements of the cipher are exploited. Here, we discuss masking 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 in such a way that

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

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 Bob to give the arguments.

3.10. Problem “A special parameter” (10 scores)

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

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

The sum of $a = (a_1, \ldots, a_m)$ and $b = (a_1, \ldots, b_m)$ in $\mathbb{F}_{2^n}^m$ is defined as $a + b = (a_1 + b_1, \ldots, a_m + b_m)$.

The *special parameter* P of a function $\varphi : \mathbb{F}_{2^n}^m \to \mathbb{F}_{2^n}^m$ is defined to be

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

- Rewrite (simplify) the definition of $P(\varphi)$ when the function φ is linear (recall that a function ℓ is linear if $\ell(x + y) = \ell(x) + \ell(y)$ for any x, 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. $\varphi(x) = M \cdot x$.
- Find the least 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?

3.11. Problem “Add–Rotate–Xor” (10 scores)

Let $\mathbb{F}_2^n$ be the vector space of a dimension n over $\mathbb{F}_2 = \{0, 1\}$ and $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$. The vector x 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 produce hardware implementations for the following functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$:

1) $f_a(x) = x \boxplus a$ — the addition modulo 2^n of vectors x and a as integers for any fixed $a \in \mathbb{F}_2^n$;
2) $g_r(x) = x \lll r$ — the cyclic rotation of a vector x to the left by r positions for any fixed positive integer r, $0 < r < n$;
3) $h_b(x) = x \oplus b$ — the coordinate-wise sum modulo 2 of vectors x and b for any fixed $b \in \mathbb{F}_2^n$.

- Bob asks Alice to construct hardware implementations for the functions S_1 and S_2 from $\mathbb{F}_2^2$ to $\mathbb{F}_2^2$ given by their truth table (Table 4).

Table 4

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

Can Alice do this? 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 last the cases $n = 2, 3, 4$.
- Is it possible to compute every function h_b, using only functions f_a and g_r?

3.12. Problem "Linear subspaces" (12 scores)

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

Problem. 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 $\mathbb{F}_2 = \{0, 1\}$ that is the prime field of characteristic 2.

Do subsets $L_1, \ldots, L_{2^n+1}$ of $\mathbb{F}_2^{2n}$ satisfying the following conditions exist?

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

If "yes", show how to construct these subspaces for an arbitrary positive integer n.

For example, in the vector space $\mathbb{F}_2^4$, we can choose the following five required subspaces:

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

3.13. Problem "Watermarking cipher" (unsolved)

The problem was stated by Gennady Agibalov.

Problem. Let X, Y, and K be the sets of plaintexts, ciphertexts, and keys respectively, $X = Y = \{0, 1\}^n$ and $K = \{0, 1\}^m$ for some integers n and m. Recall that two functions $E : X \times K \to Y$ and $D : Y \times K \to X$ are called *an encryption algorithm* and *a decryption algorithm* respectively if, for any $x \in X$, $k \in K$, the equallity $D(E(x, k), k) = x$ takes place. Together E and D form *a cipher*.

Let us call a cipher *watermarking* if for any key $k \in K$ and any subset $I \subseteq \{1, 2, \ldots, n\}$, there exists a key k_I such that, for any $x \in X$,

$$D(E(x, k), k_I) = x'$$

where x' differs from x in all bits with coordinates from I.

An example of a trivial watermarking cipher. Let $m = n$ and encryption and decryption algorithms be the following: $E(x, k) = x \oplus k$ and $D(y, k_I) = y \oplus k_I$ where k_I is obtained from k by changing all bits with coordinates from I. The main disadvantage of such a cipher is that the every key should be used only once.

How can we use a watermarking cipher? Suppose you own some digital product (for example, video) that you want to sell. Let x represent a binary code of the product.

For each customer of x, you choose an unique set I of bit coordinates in x, encrypt the plaintext x, using a predetermined key k, and send the resulting ciphertext y and the corresponding key k_I to him. Then after receiving y and k_I, the customer decrypts y and gets x'. The difference between the original x and x' is not significant; thus the customer does not know about it. If someone illegally spreads the product x' bought from you, you can easily identify him by the set I.

Summarize the ideas we need to construct a cipher that has to put something like a "watermark" into a video. Let's try! So the problem is to construct a non-trivial watermarking cipher. Please, think about the easy usage of it by an owner and a customer.

3.14. Problem "APN permutation" (unsolved)

Suppose we have a mapping F from $\mathbb{F}_2^n$ to itself (recall that $\mathbb{F}_2^n$ is the vector space of all binary vectors of length n). This mapping is called a *vector Boolean function in n variables.* Such functions are used, for example, as S-boxes in block ciphers and should have special cryptographic properties. In this problem, we consider the following two properties and the problem of combining them.

- A function F in n variables is a *permutation* if, for all distinct vectors $x, y \in \mathbb{F}_2^n$, it has distinct images, i. e. $F(x) \neq F(y)$.
- A function F in n variables is called *Almost Perfect Nonlinear* (APN) if, for any nonzero vector $a \in \mathbb{F}_2^n$ and any vector $b \in \mathbb{F}_2^n$, the equation $F(x) \oplus F(x \oplus a) = b$ has at most 2 solutions. Here, $\oplus$ is the coordinate-wise sum modulo 2 of vectors.

Try to find an APN permutation in 8 variables or prove that it doesn't exist.

History of the problem. The question "Does an APN permutation in even number of variables exist?" has been studied for more than 20 years. If the number of variables is odd, APN permutations exist as it was proved by K. Nyberg in 1994 [1]. It is known that, for 2 and 4 variables, the answer is "No". But for 6 variables, K. Browning, J. F. Dillon, M. McQuistan, and A. J. Wolfe have found such a function in 2009 [2]. You can see it bellow:

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

This function is presented as the list of its values, i. e. $G(0) = 0$, $G(4) = 15$, $G(16) = 59$ and so on. For brevity, we use integers instead of binary vectors. A binary vector $x = (x_1, \ldots, x_n)$ corresponds to the integer $k_x = x_1 \cdot 2^{n-1} + x_2 \cdot 2^{n-2} + \ldots + x_{n-1} \cdot 2 + x_n$.

Thus you are welcome to study the next case, $n = 8$.

3.15. Problem "Super S-box" (unsolved)

Another unsolved problem is directly related to AES construction. J. Daemen and V. Rijmen, the designers of AES (Rijndael), have introduced the Super-Sbox representation of two rounds of AES in order to study differential properties [3]. The function G used in the problem can be considered as a simplified Super-Sbox model of two rounds of AES. To study security of AES against the differential cryptanalysis, we welcome you to start with the differential characteristics of the function G.

Problem. Let $\mathbb{F}_{256}$ be the finite field of 256 elements and α be a primitive element (it means that, for any nonzero $x \in \mathbb{F}_{256}$, there exists $i \in \mathbb{N}$ such that $x = \alpha^i$). Let $\mathbb{F}_{256}^4$ be the vector space of dimension 4 over $\mathbb{F}_{256}$. Thus any element $x \in \mathbb{F}_{256}^4$ is $x = (x_1, x_2, x_3, x_4)$ where $x_i \in \mathbb{F}_{256}$. An arbitrary function from $\mathbb{F}_{256}^4$ to $\mathbb{F}_{256}^4$ can be considered as the set of 4 coordinate functions from $\mathbb{F}_{256}^4$ to $\mathbb{F}_{256}$. Introduce the following auxiliary functions $F_4, M : \mathbb{F}_{256}^4 \to \mathbb{F}_{256}^4$:

$$F_4(x_1, x_2, x_3, x_4) = (x_1^{254}, x_2^{254}, x_3^{254}, x_4^{254});$$

$$M(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, x_4) \times \begin{bmatrix} \alpha+1 & 1 & 1 & \alpha \\ \alpha & \alpha+1 & 1 & 1 \\ 1 & \alpha & \alpha+1 & 1 \\ 1 & 1 & \alpha & \alpha+1 \end{bmatrix}.$$

Define the function $G : \mathbb{F}_{256}^4 \to \mathbb{F}_{256}^4$ by the following combination of F_4 and M:

$$G(x_1, x_2, x_3, x_4) = F_4(M(F_4(x_1, x_2, x_3, x_4))).$$

Find the number of solutions of the equation $G(x + a) = G(x) + b$ with the parameters a and b running all nonzero values from $\mathbb{F}_{256}^4$.

4. Solutions of the problems

Here, we would like to discuss solutions of the problems. Our special attention is payed to (right/wrong and beautiful) solutions given by the participants.

4.1. Problem "A hidden message" (4 scores)

Solution. The famous Bacon‘s cipher was used here. First of all, everyone can get from the text that the alphabet of the message consists of 32 symbols (26 English letters and 6 punctuation marks) and notice that there are upper and lower case letters in the text. Such observations suggest that a binary code was used and a letter case means either 0 or 1. Since the cardinality of the alphabet is $32 = 2^5$, a string of five 0s and 1s is needed to code each letter of a secrete message. Thus if we delete all spaces and punctuation marks and divide the sequence obtained into words of 5 letters, we get the following text:

```
CrYPt  ogRap  HYiSa  ScIEn  ceOfs  eCrET  wriTi  nGFOr  aTLea  stTwo
THoUs  ANdye  aRSTh  ErEha  VEbEe  NpeOP  lEWHo  WAnTe  DtoSE  ndMES
saGes  WHiCh  coUlD  oNlyb  EenrE  AdbYt  HepEO  PLeFo  RwhOm  tHeyw
ereiN  teNde  DaloT  oFdif  feren  tMEtH  ODsFo  RcoNc  EalIN  GmEss
ageSW  erEin  vENtE  DstAR  TINGW  IthAn  CIeNt  cIPHe  rSlIK  ESkyt
aLEan  dATBA  sHand  endin  gwiTH  MOdEr  nSymm  eTRiC  ANdPu  bliCk
EyenC  RYpti  oNALG  OriTH  mSSUc  haSAe  SandR  sathe  dEVEL  opMEN
TOfcr  YPtOg  RaPHy  cOnti  NueSA  ndNEV  ERsTo  pSdec  rYPtT  HemES
saGet  HatiS  hIDdE  ninth  EteXT  oFthi  sTASk  tHEaL  phabe  tFoRT
HEmEs  sAGEC  onsis  TsofA  LltWE  nTysi  xenGl  iShle  tTERS  froma
TozAN  dSixp  uNCTu  aTIoN  MARkS
```

If the upper case is coded by 0 and the lower case by 1, we get the strange beginning of the text: "`J,FJ,`" and so on. Hence, we should use 0 and 1 for the lower and upper cases respectively. In this way, you get "`We welcome you to the first Siberian student's Olympiad in cryptography with international participation!`". We supposed that the letters are coded in alphabetic order with the numbers from 0 to 25, and the punctuation marks with the numbers from 26 to 31.

This problem was completely solved by 34 participants.

Some ideas and typical mistakes of participants are listed below:

- the most part of those participants who sent their answers for this problem succeeded in its solving; as a rule, they wrote a program in order to decode the message more faster;

- some participants mentioned in their solutions that Bacon‘s cipher was used;
- a few participants used the standard decoder BASE32 for decoding the binary string, but they did not substituted the punctuation marks from the alphabet of this problem;
- the most surprising comment for this problem was “Mendeleyev’s periodic table was somehow used there!”.

4.2. Problem “A crypto room” (4 scores)

The answer to the question “Who is the author?” is Anton Pavlovich Chekhov, a Russian classical writer. The encrypted message hides the name of his famous play “Three sisters”. **Solution.** Let us consider the steps of solution. The information contained in the picture allows to find the key needed for decryption. At first, we reflect from right to left the text written on the blackboard. It says “Use all information you can find here to get the key. The first part of it is AC”. It becomes clear that the key starts with AC. “The next part is IWP”, as it is written below in the picture. In the upper right corner, there is the sentence in which each word starts with the last letter of the original correct word. The result of the letters permutation to the initial positions is the sentence “Then use letters on the photos from up to down”. Let us do it. We get the third part of the key RRVM. The final part of the key is JOV because of “JOV completes the key”.

As a result, we obtain the key ACIWPRRVMJOV. Observe that its length is equal to 12 letters, that is exactly equal to the length of the encrypted message.

The Vigenere cipher was used for encryption. Each letter has its position number in the alphabet: A — 1, B — 2, ..., Z — 26, or 0. Using the example of ciphering above the portrait of Julius Caesar, we determine the rule of encryption:

$$\mathtt{A}+\mathtt{D}=\mathtt{E};\ \text{that is } 1+4=5 \pmod{26};$$
$$\mathtt{X}+\mathtt{D}=\mathtt{B};\ \text{that is } 24+4=2 \pmod{26}.$$

To decrypt the ciphertext, you need to subtract the key from the ciphertext according to the same rule. The decryption of two first letters of the message is given here:

$$\mathtt{U}-\mathtt{A}=\mathtt{T}\ \text{since } 21-1=20 \pmod{26};$$
$$\mathtt{K}-\mathtt{C}=\mathtt{H}\ \text{since } 11-3=8 \pmod{26}.$$

Thus we obtain the secret message THREESISTERS. This problem was completely solved by one pupil and 30 students. And only one participant has read the last strange lettering in the picture: it was a word “algorithm” written in Malayalam.

This problem was completely solved by 33 participants. The most detailed solution, illustrated with the step-by-step pictures, was proposed by O. Smirnov (Saratov State University).

Typical mistakes were:

- the inclusion of symbols 5 and * into the third part of the key (actually they are not letters);
- using the Caesar cipher with the key being equal to 4, although it was only a helpful (or unhelpful) example.

4.3. Problem “The musical notation” (4 scores)

Solution. This is a classical permutation cipher. At first, according to the ciphertext and the used musical notation, we should form the rows corresponding to all different notes “do”, “re”, ..., “ti” (Table 5).

Table 5

do								E		E							V									N
re		O		E			S													B		E			O	
mi	R		L		L						E			T				C	P		D		F			
fa																										
sol															O											
la									O			E														
ti						I							H			M								S		

Our next task is to find the right cyclical shifts for all the rows to form a readable message. The number of all possible variants is equal to $9 \cdot 6 \cdot 4 \cdot 4 \cdot 2 \cdot 1 = 1728$. Fortunately, we do not need to check all these variants because if we start with two the biggest rows ("mi" and "re"), we find that the beginning and the end of the plaintext could be "`LBEET*O`" and "`DFOREL*S*`" respectively. To find the rest, we cyclically shift other rows. Thus we get the secrete message: `L. Beethoven composed` "`For Elise`".

This problem was presented in both rounds and was solved by 33 participants. It is interesting to note some creative ways for solving. The extraordinary majority of solutions were programming. The participants generated all possible variants of row shifts and then filtered them according to some rules:

- tests for invalid combination of three or four consecutive alphabetic letters. Some participants used the known such combinations, but one participant, D. Zajcev (Saratov State University), generated invalid combinations by himself using the novel "War and peace" by Leo Tolstoy in English. The team of P. Hvoryh and V. Laptev (the winners of the second round of NSUCRYPTO in category "students") used a formula for naturalness of the language;
- one participant (S. Shabelnikov from Saratov State University) wrote a program that puts the next variant into the Internet for a search and then considered the number of results obtained.

There were also solutions made by hand. The list of some ideas is here:

- as well as in the solution presented above, some participants began with determining possible shifts for the biggest rows "mi" and "re". For example, the team of pupils S. Derevyanchenko and E. Klochkova (Specialized Educational Scientific Center of NSU) did this in details;
- we are pleased to tell that many participants have recognized the musical notation and its composer L. V. Beethoven; they tried to find shifts in order to form any of words "Beethoven", "Elise", and "composed". So the team of V. Marchuk, D. Emelyanov, and A. Gusakova (Belarusian State University) mentioned that the mistake of Alice was in taking the famous musical fragment.

4.4. Problem "Boolean cubes" (4 scores)

Solution. In the first cube, let us assign vertices $(0,0,0), (1,0,0), (0,1,0), (0,0,1)$ with "+" and vertices $(1,1,1), (1,1,0)$, $(0,1,1), (1,0,1)$ with "$-$". If we add all the coordinates of vertices in both subsets "+" and "$-$" taken with the plus and minus signs respectively, we obtain the following results: for the subset "+", we have $0+1+1+1=3$ (since there is one zero vector and three vectors each with only one nonzero coordinate), for the subset "$-$", we have $-3-2-2-2=-9$, and the total sum is -6. Consider the operation A. We can see that A adds 1 or -1 in both sums of subsets "+" and "$-$" simultaneously. This fact means that the total sum is invariant under the multiple applying the operation A and is equal to -6. If we repeat the assignment of vertices in matching layers of the second cube, we will see that the total sum is equal to 0. Thus we can not get the cube E_2 from the cube E_1 by applying the operation A any number of times.

In the first round, two pupils solved this problem with maximal scores, both used the idea of the sum's invariant property. The solution of N. Dobronravov (Lyceum 130, Novosibirsk) was very compact and logical.

This problem was also included in the second round and was properly solved by 18 teams. We want to outline some interesting non-trivial ideas of solutions. The team of G. Beloshapko, A. Taranenko, and E. Fomenko (Novosibirsk State University) introduced the following value for a cube C:

$$\lambda(C) = \left|\sum_{v\in C}(-1)^{|x(v)|}\mathrm{wt}(v)\right|$$

where $\mathrm{wt}(v)$ is the weight of vector v, $x(v)$ is the number of edges between vector v and null vector. They proved that this value does not depend on which vertex is considered to be the zero vertex. After this proof, the team underlined that $\lambda(C)$ is invariant under operation A and since $\lambda(E_1) = 6$ and $\lambda(E_2) = 0$, we can not obtain E_2 from E_1.

The most nontrivial and clear solution belongs to the team of A. Udovenko (Saint Petersburg). The participant divided vertices into 4 subsets with no edges inside each subset and with all edges between neighboring subsets:

1. (0,0,0); 2. (1,1,0), (1,0,1), (0,1,1); 3. (1,0,0), (0,1,0), (0,0,1); 4. (1,1,1).

Any application of the operation A adds or subtracts 1 from sums of two neighboring subsets. We can write this operations as vectors: $(1, 1, 0, 0)$, $(0, 1, 1, 0)$, $(0, 0, 1, 1)$. Then the participant proved that none of the vectors of differences between sums of the subsets for all possible positions of (0,0,0) in E_2 can be obtained as a linear combination of operation's vectors. So it is impossible to get the cube E_2 from E_1, using operation A.

The team of S. Skresanov, A. Miloserdov, and D. Kirin (Novosibirsk State University) found a short and nice solution via colorings of the vertices. O. Smirnov, P. Razumovsky, and A. Ripinen (Saratov State University) transformed the problem to the task about two special segments and showed that one cannot be obtained from the other.

4.5. Problem "A broken cipher machine" (4 scores)

Solution. It is well known that any positive integer n and the sum S_n of its digits are congruent modulo 3, i. e. $n = S_n(\mathrm{mod} 3)$. It follows from the algorithm that $m = 0(\mathrm{mod} 3)$, since $n = n'(\mathrm{mod}3)$ and $m \bmod 3 = n' + 2S_n \bmod 3 = n + 2n \bmod 3 = 0$.

Since the result got by Mary was a power of two, we conclude that she obtained an incorrect encrypted message.

This problem was completely solved by 6 pupils. The five of them have sent solutions that are very close to the presented one. For example, such a solution was proposed by the youngest participant A. Dorokhin (Novosibirsk school 159) — the winner of the first round of NSUCRYPTO in category "senior pupil". One participant solved the problem through the implicit proof of the property of congruence between an integer and its sum of digits.

4.6. Problem "The snowflake cipher" (4 scores)

Solution. We may see that the problem is equivalent to finding the longest path through triangles with common edge such that every triangle can be found in this path only once. Let us consider nine *ledges* each consisting of three triangles with only one common edge with the rest of snowflake. Clearly, if some of these ledges is crossed by our path, then it can be only the beginning or the end of the path. So the path may contain not more than 4 triangles from 2 chosen ledges.

Let us paint triangles in the rest part of snowflake in black and white colours such that neighbouring triangles have different colours. Among them, there are 93 black triangles and 114 white, but since colours of triangles in the path should alternate, not more than 93 black triangles and 94 white triangles can be in the longest path. So we can say that length of a path in the snowflake is not more than $93 + 94 + 4 = 191$. We present an example (Fig. 7) of such a path constructed by the team of G. Beloshapko, A. Taranenko, and E. Fomenko (Novosibirsk State University).

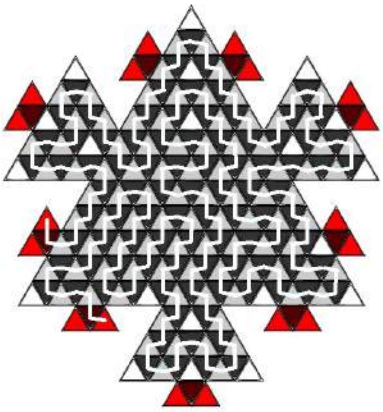


Fig. 7.

Unfortunately, the pupils did not cope with this problem on the highest score, nevertheless, three of them got some scores due to the right but incomplete ideas of estimation.

In the second round, 6 teams have solved this problem with full possible scores.

Let us consider an interesting solution proposed by A. Udovenko (Saint Petersburg).

- At the first stage, two kinds of ledges were introduced, the first one, P1, is the same as in the solution above, consisting of three triangles, but there are only 6 such ledges in the group, because the rest three of them are supposed to be the part of the second type bigger ledges, P2. We may see that ledges of the type P2 consist of 24 triangles. Define the P3 as the main big triangle, obtained by deleting all P1 and P2 ledges from the original snowflake.
- At the second stage, the author also painted P3 in black and white so that any moving between triangles is possible only if they have different colours. Then he got an estimate that the longest path in P3 will skip at least 11 triangles.
- At third, the author considered all possible pairs "start-end" and, for each pair, counted minimal number of skipped triangles. He obtained that the lower bound on this number is 43 and gave a right example of path with 191 length.

The team of V. Marchuk, D. Emelyanov, and A. Gusakova (Belarusian State University) proposed very nice solution by transforming the problem to the following one: find a Hamilton cycle in a special graph corresponding to the snowflake.

4.7. Problem "A pseudo-random generator" (6 scores)

Solution. It is a simple task. First of all, the binary sequence from r_3 and r_4 is `11000000011001000100111100000111`. Because the length of the generator is 16, linear complexity of the sequence is not more than 16. Next, we have the sequence of 32 consecutive bits and can uniquely restore its recurrent relation using, for example, the Berlekamp — Massey algorithm. This relation is

$$u_{i+16} = u_{i+5} \oplus u_{i+3} \oplus u_{i+1} \oplus u_i.$$

Since we know the recurrent relation, we obtain: IV is 58 390. We also know that the generator was initialized on November 17, 2014, at 12:05 UTC+6. Therefore, IV would be 58 476. In Russia, there are time zones from UTC+2 to UTC+12. So Bob initialized the generator $58\,476 - 58\,390 = 86$ seconds to November 17, 2014, 12:05 UTC+6, i. e. at 12:03:34. Consequently, both Bob and Eve live in Novosibirsk time.

There were 18 solutions from the teams and only one solution was wrong, the most of teams just solved a system of linear equations and have not used the Berlekamp — Massey algorithm.

4.8. Problem "Number of solutions" (8 scores)

Solution. Consider a general case, i. e. $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $F(x) = x^{2^n-2}$ (and $F(x) = x$ for $n = 1$). We need to determine how many solutions the equation $F(x + a) = F(x) + b$ may have for all different pairs of nonzero parameters a and b where $a, b \in \mathbb{F}_{2^n}$. Since characteristic of $\mathbb{F}_{2^n}$ is 2, the operations "$-$" and "$+$" coincide.

First of all, note that, for $n = 1$, there exists only one pair $(a, b) = (1, 1)$. In this case, there are 2 solutions of the equation. In what follows let $n > 1$.

Note that the function $F_a(x) = F(x)+F(x+a)$ has some symmetry: $F_a(x) = F_a(x+a)$. This means that 2 divides the number of solutions and, at least for 2^{n-1} distinct $b \in \mathbb{F}_{2^n}$, $F_a(x) \neq b$ for all $x \in \mathbb{F}_{2^n}$.

Therefore, for all $n > 1$, there exist $b \neq 0$ and $a \neq 0$ such that the equation has no solutions. That is why the number of solutions of the equation $F(x + a) = F(x) + b$ can be 0. Consider other possibilities.

Simplify the given equation. For this, note that $y^{2^n-1} = 1$ for all $y \in \mathbb{F}^*_{2^n}$. Then after multiplying the equation $(x + a)^{2^n-2} + x^{2^n-2} = b$ by $x(x + a)$, we get the equation $bx^2 + abx + a = 0$. After multiplying the last by $a^{-2}b^{-1}$, we get $x^2/a^2 + x/a + (ab)^{-1} = 0$. Note that the number of solutions of the equation $x^2/a^2 + x/a + (ab)^{-1} = 0$ only depends on ab, and the values $x = 0$, $x = a$ are not its solutions. Rewrite this equation as

$$z^2 + z + (ab)^{-1} = 0$$

where $z = x/a$. Then we have two cases:

- $x = 0$ and $x = a$ are solutions of $F(x) + F(x + a) = b$. Then $a = b^{-1}$ and $ab = 1$. We already have 2 solutions. Next, solve the equality $z^2 + z + 1 = 0$. Both roots of the polynomial $z^2 + z + 1$ belong to the field $\mathbb{F}_{2^2}$. This field is contained in $\mathbb{F}_{2^n}$ if and only if n is even. So in the case of even n, the equation $F(x) + F(x + a) = b$ has exactly 4 solutions. In the case of odd n, there are exactly 2 solutions of the equation $F(x) + F(x + a) = b$.
- $x = 0$ and $x = a$ are not solutions of $F(x)+F(x+a) = b$. Therefore, $ab \notin \mathbb{F}_2$. Note that the equation $z^2 + z = z(z + 1) = (ab)^{-1}$ has 0 or 2 solutions. Since $(ab)^{-1}$ can be an arbitrary element from $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$, at least for $2^{n-1} - 2$ distinct ab, there are exactly two solutions. So if $n > 2$, then 2 solutions can be in this case. If $n = 2$, then $z^2 + z \in \mathbb{F}_2$, i. e. for $ab \notin \mathbb{F}_2$, there is no solution.

The answer is the following. For $n = 1$, there are always 2 solutions; for $n = 2$, there can be 0 or 4 solutions; for odd n $(n > 1)$, there can be 0 or 2 solutions; for even n $(n > 2)$, there can be 0, 2 or 4 solutions.

This problem was completely solved during the second round. The teams of P. Hvoryh and V. Laptev (Omsk State Technical University), A. Udovenko (Saint Petersburg), A. Oblaukhov (Novosibirsk State University), S. Belov and G. Sedov (Moscow State University) proposed the right and complete solutions.

4.9. Problem "S-box masking" (8 scores)

Solution. We would like to give the solution proposed by L. Qu et al. in the first variant of the paper [4]. Let us represent an arbitrary bijective function $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ by the sum $S'(x) \oplus S''(x)$ where $S', S'' : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are bijective too. Consider $\mathbb{F}_2^n$ as $\mathbb{F}_{2^n}$. Let $\alpha \in \mathbb{F}_{2^n}$ and $\alpha \neq 0, 1$. If $n > 1$, such an element α does exist. It is clear that $S(x) = \alpha S(x)+(\alpha+1)S(x)$. Note that $\alpha S(x)$ and $(\alpha + 1)S(x)$ are bijective, since each of them is a composition of two bijective mappings. So for $n > 1$, the required representation exists. If $n = 1$, there are only two bijective functions $S(x) = x$ and $S(x) = x \oplus 1$; their sum is a constant and hence there is no the required representation in this case.

There were two complete combinatorial solutions proposed by S. Godzhaev (Moscow State University) and A. Udovenko (Saint Petersburg).

4.10. Problem "A special parameter" (10 scores)

A special parameter that we consider in this problem is called the *differential branch number* of a transformation, see for example book [3]. In differential cryptanalysis of block ciphers, this parameter is used to measure the diffusion strength of a cipher. Some properties of it are discussed in the problem.

Solution. Let $\varphi : \mathbb{F}_{2^n}^m \to \mathbb{F}_{2^n}^m$ be a linear function and $a, b \in \mathbb{F}_{2^n}^m$.

• Since φ is linear, i. e. $\varphi(x + y) = \varphi(x) + \varphi(y)$ for all $x, y \in \mathbb{F}_{2^n}^m$, and the condition $a \neq b$ is equivalent to $a + b \neq 0$, we can rewrite the definition of $P(\varphi)$ in the following way:

$$P(\varphi) = \min_{a+b\neq 0} \{\mathrm{wt}(a + b) + \mathrm{wt}(\varphi(a + b))\}.$$

• Let us consider vectors $(x, \varphi(x)) = (x, M \cdot x)$ of length $2m$ where $x \in \mathbb{F}_{2^n}^m$. Then the set $C = \{(x, M \cdot x) \mid x \in \mathbb{F}_{2^n}^m\}$ is a linear code. Since we have $\mathrm{wt}(a + b) + \mathrm{wt}(\varphi(a + b)) = \mathrm{wt}((a + b, \varphi(a) + \varphi(b))) = \mathrm{dist}((a, \varphi(a)), (b, \varphi(b)))$, where $\mathrm{dist}(x, y)$ means the Hamming distance between vectors x and y, the parameter $P(\varphi)$ is equal to the minimal distance between distinct codewords of the code C.

• Since $a \neq b$, the minimal value of $\mathrm{wt}(a + b)$ is equal to 1. The maximal possible value of $\mathrm{wt}(\varphi(a) + \varphi(b))$ is m by the definition. Thus the maximal possible value of $P(\varphi)$ is not more than $m + 1$.

• One can construct an example of such a transformation using a Maximal Distance Separable code with parameters $[2m, m, m + 1]$ (for example, Reed — Solomon code).

This problem was completely solved by two teams: P. Hvoryh and V. Laptev (Omsk State Technical University); K. Kogos and S. Kyazhin (Moscow Engineering Physics Institute).

4.11. Problem "Add–Rotate–Xor" (10 scores)

The complicated algebraic solution of this problem was given by T. Zieschang in 1997 [5]. Here, we introduce a simple solution proposed by the participants of the Olympiad.

Solution.

- $S_1(x) = g_1(f_1(g_1(f_2(x))))$. It is obvious that the functions f_a, g_r, and h_b are all bijective. Therefore, any its composition is bijective too. The function S_2 is not bijective, so it can not be represented as a composition of them.
- Only permutations on $\mathbb{F}_{2^n}$ can be constructed in this way. It is well known that the compositions of the function f_1 (a cycle of length 2^n) and the transpositions of adjacent elements in the cycle give us all the permutations on $\mathbb{F}_{2^n}$. The following construction gives a certain transposition τ: $\tau(x) = g_1(f_{2^n-1}(g_{n-1}(f_2(x))))$. Indeed, $g_{n-1}(y) = 2^{n-1}y_n + \lfloor y/2 \rfloor$ and if $x < 2^n - 2$, then $f_2(x) = x + 2$, so

$$g_{n-1}(f_2(x)) = g_{n-1}(x + 2) = 2^{n-1}(x + 2)_n + \lfloor (x + 2)/2 \rfloor = \\ = 2^{n-1}x_n + \lfloor x/2 \rfloor + 1 = (x_n, x_1, \ldots, x_{n-1}) + 1.$$

  Next, f_{2^n-1} eliminates "+1" and g_1 cyclically rotates $(x_n, x_1, \ldots, x_{n-1})$ to the left by one position. That is, $\tau(2^n - 1) = 2^n - 2$. Also, $\tau(2^n - 2) = 2^n - 1$ because $f_2(2^n - 2) = 0$, $g_{n-1}(0) = 0$, $f_{2^n-1}(0) = 2^n - 1$, $g_1(2^n - 1) = 2^n - 1$. Therefore, τ transposes $2^n - 1$ with $2^n - 2$ and does not change all other elements.

- Yes. The third item is obvious, since we can construct any permutation on $\mathbb{F}_{2^n}$ using the mentioned functions.

In the second round, there were 7 right solutions. The most of teams have found a full cycle and a transposition. The solution given above is based on the solution that was presented by the team of G. Beloshapko, A. Taranenko, and E. Fomenko (Novosibirsk State University). Very clear and simple solution was proposed by the team of R. Zhang and A. Luykx (KU Leuven, Belgium); they constructed all transpositions in an explicit way.

4.12. Problem “Linear subspaces” (12 scores)

Here, the solution given by the program committee is presented.

Solution. Consider $\mathbb{F}_2^{2n}$ as 2-dimensional vector space V over Galois field $\mathbb{F}_{2^n}$ consisting of 2^n elements. Define the following family of sets:

$$L_\alpha = \{(x, \alpha x) : x \in \mathbb{F}_{2^n}\},\ \alpha \in \mathbb{F}_{2^n};\quad L_{2^n+1} = \{(0, y) : y \in \mathbb{F}_{2^n}\}.$$

It is obvious that every such a set is a linear subspace in V and contains exactly 2^n elements. Let us show that an arbitrary element $(x, y) \in V$ is covered by the union of these subspaces. If $x = 0$, it is covered by L_{2^n+1}. Otherwise, $(x, y) = (x, (y/x)x)$ belongs to the subspace $L_{y/x}$. Note that every two subspaces have only one common element, $\mathbf{0}$, since the cardinality of V is exactly $2^{2n} = (2^n + 1)(2^n - 1) + 1$. Thus, the answer for the problem is “yes” and the system is constructed.

Another approach (but still using Galois fields) was proposed by the team of P. Hvoryh and V. Laptev (Omsk State Technical University) during the second round. They constructed linear subspaces in the following way:

$$L_0 = \{0, \alpha^{0\cdot(2^n+1)}, \alpha^{1\cdot(2^n+1)}, \ldots, \alpha^{(2^n-2)(2^n+1)}\} \text{ and } L_i = \{\alpha^i x : x \in L_0\},\ i = 1, \ldots, 2^n,$$

where α is a generating element of $\mathbb{F}^*_{2^{2n}}$.

There was also a nice right solution obtained by the team of S. Skresanov, A. Miloserdov, and D. Kirin (Novosibirsk State University). This is more close to the solution above.

Some teams proposed algorithms for constructing subspaces, but they made mistakes in their constructions.

4.13. Problem “Watermarking cipher” (unsolved)

The most deep analysis of this problem was proposed by R. Zhang and A. Luykx (winners of the second round of NSUCRYPTO in category “professional”), but nobody has introduced a concrete solution. May be you can do it?

Some details on this problem and some non-trivial watermarking ciphers based on symmetric stream ciphers with functional keys are considered in the talk of G. P. Agibalov on the conference Sibecrypt’15 and published in [6].

4.14. Problem “APN permutation” (unsolved)

This is another unsolved problem of the Olympiad; it is the well known long standing problem of cryptography. Some ideas on it were proposed by the team of G. Beloshapko, A. Taranenko, and E. Fomenko (winners of the second round of NSUCRYPTO in category “students”). They proved some basic properties of APN functions; namely, if a permutation is an APN function, then its inverse function is APN too.

One participant, D. Svitov from NSU, has proposed an online service for distributed search of APN permutations [7]. But till now this problem is unsolved.

4.15. Problem "Super S-box" (unsolved)

The problem is still unsolved. Only one team of G. Beloshapko, A. Taranenko, and E. Fomenko from Novosibirsk State University has sent a solution with an analysis of the problem for smaller field. They considered $\mathbb{F}_{16}$ and found the exact number of pairs a, b for each number of solutions. It seems that any even number between 0 and 44 can be the number of solutions. They proposed a hypothesis that the same result is true for $\mathbb{F}_{256}$: it may be any even number of solutions bounded by some number.

5. Awarding

Awarding of the winners was held on December 2014 in Novosibirsk State University (Fig. 8).

Fig. 8.

6. Winners of the Olympiad-2014

In this section, we publish the names of winners of NSUCRYPTO-2014 and some information about them. There are 15 winners in the first round and 11 teams in the second one (Tables 6–11).

Table 6

Winners of the first round in school section (“senior pupils”)

Place	Name	Country	City	School	Class	Scores
1	Alexander Dorokhin	Russia	Novosibirsk	MOU 159	8	12
2	Nikita Dobronravov	Russia	Novosibirsk	Lyceum 130	9	10
3	Artem Uskov	Russia	Novosibirsk	Gymnasium 3	11	8
3	Egor Dobronravov	Russia	Novosibirsk	Lyceum 130	9	8

Table 7

Winners of the first round in student’s section (in category “students”)

Place	Name	City	University	Department	Course	Scores
1	George Beloshapko	Novosibirsk, Russia	Novosibirsk State University	Mechanics and Mathematics	6	23
2	Roman Lebedev	Novosibirsk, Russia	Novosibirsk State University	Physics	2	14
3	Dmitry Zajcev	Saratov, Russia	Saratov State University	Computer Science and Information Technology	5	12
3	Gleb Shalyganov	Saratov, Russia	Saratov State University	Computer Science and Information Technology	4	12
3	Samir Godzhaev	Moscow, Russia	Moscow State University	Mechanics and Mathematics	1	12
3	Alexander Shein	Saratov, Russia	Saratov State University	Computer Sciences and Information Technologies	5	12
3	Pavel Grachev	Saratov, Russia	Saratov State University	Computer Sciences and Information Technologies	5	12
3	Sergey Shabelnikov	Saratov, Russia	Saratov State University	Computer Sciences and Information Technologies	5	12
3	Angelina Sadohina	Saratov, Russia	Saratov State University	Computer Sciences and Information Technologies	4	12
3	Alexander Tkachev	Novosibirsk, Russia	Novosibirsk State University	Information Technologies	2	12

Table 8

Winners of the first round in student’s section (in category “professionals”)

Place	Name	Country	City	Organization	Scores
1	Alexey Udovenko	Russia	Saint-Petersburg	—	12

Table 9

Winners of the second round (in category “senior pupils”)

Place	Name	Country	City	School	Class	Scores
1	Stepan Derevyanchenko, Elizaveta Klochkova	Russia	Novosibirsk	Specialized Educational Scientific Center of NSU	11	6

Table 10

Winners of the second round (in category "students")

Place	Names	City	University	Department	Course	Scores
1	George Beloshapko, Anna Taranenko, Evarist Fomenko	Novosibirsk, Russia	Novosibirsk State University	Mechanics and Mathematics	5-6	55
1	Pavel Hvoryh, Vladimir Laptev	Omsk, Russia	Omsk State Technical University	Information Technologies and Computer Systems, RTF	3	55
2	Saveliy Skresanov, Alexey Miloserdov, Denis Kirin	Novosibirsk, Russia	Novosibirsk State University	Mechanics and Mathematics	2	36
3	Alexey Oblaukhov	Novosibirsk, Russia	Novosibirsk State University	Mechanics and Mathematics	3	33
3	Vadim Marchuk, Dmitry Emelyanov, Anna Gusakova	Minsk, Belarus	Belarusian State University	Applied Mathematics and Computer Science	6	33
3	Oleg Smirnov, Peter Razumovsky, Alexey Ripinen	Saratov, Russia	Saratov State University	Computer Science and Information Technology	4	29
3	Sergey Belov, Grigory Sedov	Obninsk, Moscow, Russia	Moscow State University	Computational Mathematics and Cybernetics	5	28

Table 11

Winners of the second round (in category "professional")

Place	Names	Country	City	Organization	Scores
1	Ren Zhang, Atul Luykx	Belgium	Leuven	KU Leuven, COSIC	65
2	Konstantin Kogos, Sergey Kyazhin	Russia	Moscow	Moscow Engineering Physics Institute	41
3	Alexey Udovenko	Russia	Saint-Petersburg	—	37

Acknowledgements

We thank Novosibirsk State University for the financial support of the Olympiad and invite you to take part in the next NSUCRYPTO that starts on November 15, 2015. Your ideas on the mentioned unsolved problems are also very welcome and can be sent to `olymp@nsucrypto.ru`.

We are very grateful to Gennadiy Agibalov and Irina Pankratova for their valuable contribution to this paper.

REFERENCES

1. *Nyberg K.* Differentially uniform mappings for cryptography. Eurocrypt'93, LNCS, 1994, vol. 765, no. 2, pp. 55–64.
2. *Browning K. A., Dillon J. F., McQuistan M. T., and Wolfe A. J.* An APN Permutation in Dimension Six. Post-proceedings of the 9-th Intern. Conf. on Finite Fields and Their Applications Fq'09, Contemporary Math., AMS, 2010, vol. 518, pp. 33–42.
3. *Daemen J. and Rijmen V.* The Design of Rijndael: AES — The Advanced Encryption Standard. Springer, 2002. 238 p.

4. *Qu L., Fu S., Dai Q., and Li C.* When a Boolean Function can be Expressed as the Sum of two Bent Functions. Cryptology ePrint Archive, 2014/048.

5. *Zieschang T.* Combinatorial Properties of Basic Encryption Operations. Eurocrypt'97, LNCS, 1997, vol. 1233, pp. 14–26.

6. *Agibalov G. P.* Shifry s vodyanymi znakami [Watermarking Ciphers]. Prikladnaya diskretnaya matematika. Prilozhenie, 2015, no. 8, pp. 54–59. (in Russian)

7. `http://writeupsd.blogspot.ru/2014/11/apn-permutation-finder.html.`