CRYPTOLOGIA
http://dx.doi.org/10.1080/01611194.2016.1260666

Taylor & Francis
Taylor & Francis Group

Mathematical problems of the Second International Students' Olympiad in Cryptography

S. Agievich, A. Gorodilova, V. Idrisova, N. Kolomeec, G. Shushuev, and N. Tokareva

ABSTRACT
A detailed overview of the mathematical problems and their solutions for the Second International Students' Olympiad in Cryptography (NSUCRYPTO'2015) is given. The authors consider mathematical problems related to the construction of special discrete structures associated with cryptographic applications, highly nonlinear functions, points on an elliptic curve, crypto machines, solving the Diffie-Hellman problem, performing any bijective mapping on a binary tape, modifications of ciphers, and so forth. Some unsolved problems are also discussed.

KEYWORDS
Boolean functions; competition; NSUCRYPTO; Olympiad

1. Introduction

Mathematical problems occupy a special place in cryptography. It is well-known that mathematical ideas and results often serve as a stimulus for the creation of modern cryptographic systems. Here, one can mention concepts of public-key cryptography, algebraic foundations of many symmetric ciphers, applications of cryptographic Boolean functions, and so on. It is worth mentioning that the language of cryptography is rather mathematical.

In this article, we discuss mathematical problems from the Second International Students' Olympiad in Cryptography (NSUCRYPTO'2015) (www.nsucrypto.nsu.ru). It is an annual event devoted to mathematics in cryptography without restrictions: It is held via the Internet, is comprised of unsolved mathematical problems, and is open to professionals as well as for students and senior pupils.

One should note that there are several school competitions in cryptography such as the Interregional Olympiad in Mathematics and Cryptography for high school students (www.cryptolymp.ru), the Olympiad in Mathematics

CONTACT N. Tokareva tokareva@math.nsc.ru Laboratory of Discrete Analysis, Sobolev Institute of Mathematics, Novosibirsk State University, pr. ac. Koptyuga 4, Novosibirsk 630090, Russia.
Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/ucry.

and Cryptography for high school students of Belarusian State University (www.uni.bsu.by/arrangements/kripto/), and so forth. Cryptographic tasks can also be found at main and preparatory stages of the International Olympiad in Informatics for school students, for example at the Australian national preparatory stage Burton (2008). Numerous competitions in the area of information security, called Capture The Flag (CTFs) (www.ctftime.org/ctfs), competitions for breaking codes and solving ciphers, such as Alan Turing cryptography competition (http://www.maths.manchester.ac.uk/cryptography_competition) for students from the United Kingdom, National Cipher Challenge University of Southampton (www.cipher.maths.soton.ac.uk/), and mysterious Cicada 3301 puzzles (Bell 2013) can be found worldwide. NSUCRYPTO is the unique cryptographic Olympiad containing scientific mathematical problems for students and professionals from any country. Its aim is to involve young researchers in solving curious and tough scientific problems of modern cryptography. From the very beginning, the concept of the Olympiad was not to focus on solving olympic tasks but on including unsolved research problems at the intersection of mathematics and cryptography.

In this article, we provide a detailed overview of the mathematical problems of the Olympiad.

We start with the registration process and the description of rounds. Then, we discuss all 17 mathematical problems of the Olympiad and their solutions. Among them, there are both amusing tasks based on historical ciphers and hard mathematical problems. We consider mathematical problems related to the construction of special discrete structures associated with cryptographic applications, highly nonlinear functions and points on an elliptic curve, crypto machines, solving the Diffie-Hellman problem, performing any bijective mapping on a binary tape, modifications of ciphers, and so forth. Some unsolved problems are also discussed.

The 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). More than 700 participants from 24 countries registered on the website of the Olympiad, (www.nsucrypto.nsu.ru). The list of winners can be found in the last part of this article.

The mathematical problems of the First International Olympiad NSUCRYPTO'2014 can be found in Agievich and colleagues (2015).

2. Organization and rules of the Olympiad

Here, we briefly formulate the key points of the Olympiad.

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 (**section A**) and student (**section B**). It was held on 16 November. Theoretical problems in the mathematics of cryptography were offered to participants. The second round (duration 1 week; 17–24 November) was devoted to research and programming problems of cryptography, solved in teams.

Everybody could 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 the status or age of participants. Participants from all countries were welcome. During the registration, every participant had to choose a corresponding category: **"senior pupil"** (for pupils and school students), **"student"** (for participants who were currently studying at universities), or **"other/professional"** (for participants who already completed their education or just want to be in the restriction-free category). There were particular prizes for each category, respectively, so if you were a pupil of some school you should have chosen the category "senior pupil" during registration because you would have had higher chances of winning in it.

The first round was divided into sections: A and B. The problems of section A were prepared for participants from the "senior pupil" category, and the problems of section B were offered for participants from categories "student" and "other/professional." The second round was general for all participants.

Language of the Olympiad. All problems were given in English.

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 paper and send us a picture. Solutions should have been written with all necessary details.

Prizes. There were several categories of prizes:

- For senior pupils: winners of section A of the first round;
- For students: winners of section B of the first round;
- For participants in the category other/professional: winners of section B of the first round;
- For participants (for every category separately): winners of the second round; and
- Special prizes from the Program Committee, if one proposes a correct solution of the problem marked as unsolved.

3. Problem structure of the Olympiad

The Olympiad was comprised of 17 problems. Some of them were included in both rounds.

Thus, the school section of the first round consisted of six problems, whereas the student section contained seven problems. Three problems were common to both sections. The following table shows the highest score one could get for solving each problem.

Problems of the first round (A: school section)

N	Problem title	Maximum scores
1	Key sharing	4
2	RSA numbers	4
3	Bigrams	4
4	An encryption table	4
5	Crypto street	4
6	An elliptic curve	8

Problems of the first round (B: student section)

N	Problem title	Maximum scores
1	An encryption table	4
2	Crypto street	4
3	An elliptic curve	10
4	Give an answer	4
5	A binary tape	6
6	Covering radius	4
7	The machine DH-d	10

The second round was composed of ten problems; they were common to all the participants. Two of the problems presented in the second round were marked as unsolved (and to be awarded special prizes from the Program Committee).

Problems of the second round

N	Problem title	Maximum scores
1	A secret sharing	Unsolved
2	The machine DH-d	10
3	A modification of PRESENT	6
4	Guess the cipher	4
5	Hypothesis	Unsolved
6	A binary tape	6
7	Palindrome cipher	10
8	Highly nonlinear functions	8
9	Covering radius — 2	8
10	Bigrams	4

4. Problems

4.1. Problem "Key sharing"

A bank safe can be opened with nine keys inserted in its keyholes in the right order. The keyholes are arranged in a circle. The order of keys is *right* if the sum of the keys (each key is associated with a natural number) in every three consecutive keyholes is divisible by 3.

The safe has two special features: If you insert a key in a keyhole, you cannot get it back until all nine keys are inserted; if the order of the nine inserted keys is wrong, the safe sends the "SOS signal" and blocks itself.

The keys are shared by three people: Alice, Bob, and Caroline. All together they can insert their keys in the right order and then open the bank safe. Their keys are the following:

– Alice: {4,14,24};
– Bob: {34,44,54};
– Caroline: {64,74,84}.

Today, Alice, Bob, and Caroline are going to open the safe. One of them forgot the rule of the right order for the keys and has already inserted two of his keys into consecutive keyholes, when he was stopped by his friends. Prove that Alice, Bob, and Caroline still are able to open the safe in this situation.

4.2. Problem "RSA numbers"

RSA is one of the most popular cryptosystems with a public key. We know that it operates with two big prime numbers p and q that should be kept secret by each user.

Eve is a malefactor who likes to steal the secret RSA parameters of users and then sell them via the Internet. Today, she sells a new pair of primes p and q satisfying the following relation:

$p^{4x} + 4 \cdot 2015 = q^{4y}$ for some natural numbers x and y.

Should the clients of Eve buy these numbers?

4.3. Problem "Bigrams"

Users of a communication system send messages to each other. Every message is written in English. Eve is a malefactor who intercepts messages in this channel and replaces them with new ones. In detail, she does the following: intercepts a message, removes all spaces and punctuation marks from it, and splits the message into bigrams starting from the beginning. Then, she makes several iterations of message destruction. The number of iterations is random.

All bigrams are divided into three types:

I. Bigram that contains only vowels (e.g., AA, EI, IO, UO, YU, ...).
II. Bigram that contains only consonants (e.g., BN, TR, LL, PW, SD, ...).
III. Bigram that contains one vowel and one consonant (e.g., QA, EC, HI, KO, ...).

For each iteration, Eve takes two random bigrams B_1 and B_2 of different types and removes them from the message; at the same time, she adds a new random bigram B_3 of the third type at the beginning of the message. If she chooses bigrams of types I and II (II and III; I and III), she will add an arbitrary bigram of type III (I; II).

For example, the message CRYPTO TEXT can be transformed by Eve in the following way:

$$\texttt{CRYPTO TEXT} \to (\texttt{CR})(\underline{\texttt{YP}})(\texttt{TO})(\texttt{TE})(\underline{\texttt{XT}}) \to (\underline{\texttt{OE}})(\underline{\texttt{CR}})(\texttt{TO})(\texttt{TE}) \to (\texttt{FE})(\texttt{TO})(\texttt{TE})$$

The question is the following. You know that Alice has sent the following message to Bob

THE MEETING WILL TAKE PLACE AT THREE IN EEYORE – EAGLE – BEE CREEK INN

The message has been intercepted by Eve. She has repeated iterations of destruction until only one bigram remained. Could it be a bigram consisting of one vowel and one consonant?

4.4. Problem "An encryption table"

Mary read a book about the history of cryptography and found an interesting cipher. It encrypts messages consisting of letters from the English alphabet (26 letters from "A" to "Z"). For encryption, one must choose a codeword of length n in the English alphabet and construct an encryption table T of size $n \times n$ in the following way. The first column is filled by the letters of the chosen codeword. Then, each row is filled by letters in alphabetical order starting with the letter in the first cell.

The message is encrypted letter by letter. The ciphertext for a message of length t consists of t ordered pairs of integers (i, j), where i is the row number and j is the column number in the table T of a current letter.

An example. Let the codeword be MARY. Then the ciphertext for the message CRYPTO is (2,3) (3,1) (4,1) (1,4) (3,3) (1,3).

For the message R S A, the ciphertext could be (3,1) (3,2) (2,1) or (3,1) (3,2) (4,3).

Mary has encrypted a sentence using this cipher. As a result, she got the following ciphertext, where all spaces in the text are preserved unchanged:

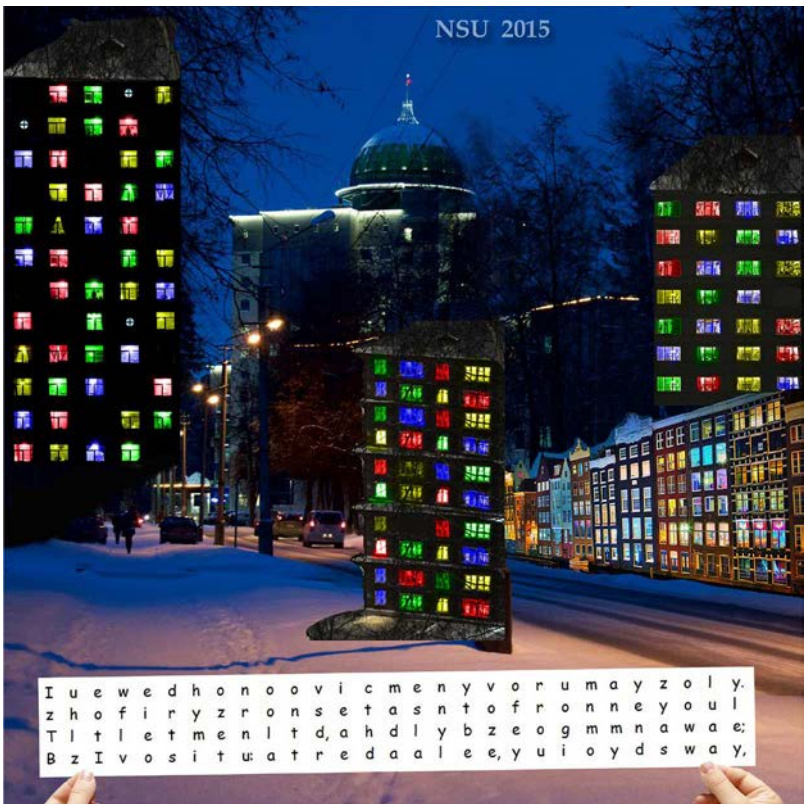
(8, 1) (7, 8) (1, 1) (2, 6) (5, 5) (7, 5) (11, 7) (7, 8) (5, 7) (8, 11) (9, 1) (3, 1)
(6, 1) (7, 5) (7, 6) (7, 5) (1, 10) (2, 5) (7, 5) (7, 4) (2, 7) (11, 2) (3, 9) (1, 11)
(6, 3) (7, 8) (7, 5) (11, 6) (7, 9) (1, 5) (9, 8) (1, 4) (7, 5)
(3, 1) (5, 9) (6, 4) (8, 8) (5, 10) (7, 5) (3, 11) (9, 1) (1, 8) (7, 8) (7, 5) (9, 10)

Try to read it given that the codeword was 11 letters in length, the encryption table contained all English letters, and its fragment was the following:

M	N	O
S	T	U
R	S	T

4.5. Problem "Crypto street"

You are walking near Novosibirsk State University and its new hostels with a secret message in hand. Can you read it? (Note that a *colored* picture is available at www.nsucrypto.nsu.ru.)



4.6. Problem "Give an answer"

Two young friends Roman and Stephan use a method to communicate with each other without exchanging common secret keys. Their messages consist of letters from the following extended English alphabet: ≪A≫, ≪B≫, … , ≪Z≫, ≪0≫, ≪1≫, …, ≪9≫, ≪≫, ≪?≫, ≪.≫.

Here is a fragment of their recent dialog:

Stephan to Roman : `Q2A?4FV4GOCX4IASOXF?K4AJSKN?CXK4NOSK6T`

Roman to Stephan : `AXOLNJ42?K4QOXUJ4IN4804JA7S`

They supposed that nobody could understand their dialog, but surprisingly Stephan recieved the message

`2?K4AJVKN2LXKS4OF42OM4SAQ7KX`

from their classmate Anton, and Stephan easily understood it!

Try to read the chat!

And what would be your answer?

4.7. Problem "Covering radius"

In order to protect a new block cipher against some attacks based on S-box approximations, Alice must solve the following problem.

Let $\mathbb{F}_2^n$ be an n-dimensional vector space over the field $\mathbb{F}_2 = \{0, 1\}$. Let $n = 2k$, where k is a positive integer. Evaluate the covering radius, and describe the metric complement of the linear subspace spanned by the rows of the following $k \times n$ matrix:

$$M = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 & 1 \\ 0 & 1 & \dots & 0 & 0 & \dots & 1 & 0 \\ \dots & \dots & \ddots & \dots & \dots & \ddots & \dots & \dots \\ 0 & \dots & 1 & 0 & 0 & 1 & \dots & 0 \\ 0 & \dots & 0 & 1 & 1 & 0 & \dots & 0 \end{pmatrix} = (I_k / I_k'),$$

where I_k is the identity $k \times k$ matrix and I_k' is its copy flipped horizontally.

Remark I. Recall several definitions and notions. A set $L \subseteq \mathbb{F}_2^n$ is called a *linear subspace* if for every $x, y \in L$ the sum $x \oplus y$ is also in L. The *Hamming distance* $d(x, y)$ between vectors $x, y \in \mathbb{F}_2^n$ is defined as the number of positions where they differ, that is, $d(x, y) = |\{i \mid x_i \neq y_i\}|$. The Hamming distance from a vector y to a subset $X \subseteq \mathbb{F}_2^n$ is defined as $d(y, X) = \min_{x \in X} d(y, X)$. Since the distance between any two vectors is bound by n, for an arbitrary subset X there is the number $d(X)$ such that

– For every $y \in \mathbb{F}_2^n$, it holds that $d(y, X) \le d(X)$;
– There is a vector $z \in \mathbb{F}_2^n$ with $d(z, X) = d(X)$.

This number is called the *covering radius* of X. The set $\hat{X} = \{z \in \mathbb{F}_2^n \mid d(z, X) = d(X)\}$ is called the *metric complement* of X.

Remark II. Let us consider several examples:
– Let X consist of a single vector $x \in \mathbb{F}_2^n$. It is easy to see that $d(X) = n$ and $\hat{X} = \{x \oplus \mathbf{1}\}$, where $\mathbf{1}$ is the all-ones vector;
– Let Y be a ball of radius r centered at x: $Y = \{y \in \mathbb{F}_2^n \mid d(x, y) \le r\}$. One can verify that $d(Y) = n - r$ and $\hat{Y} = \{x \oplus \mathbf{1}\}$.

4.8. Problem "Guess the cipher"

There was a cipher, NSUCRYPTO'2015, that encrypted messages written in the 26-letter English alphabet from A to Z. A message length did not exceed 50 letters. Participants had access to the page www.nsucrypto.nsu.ru/archive/2015r2/task4 where the encryption algorithm was implemented, and they could get the ciphertext for any of their correct input messages. The task was to describe this cipher.

4.9. Problem "A binary tape"

A cipher machine works with a binary infinite tape that starts with an input word of length n, and all its other elements are zero. The machine encrypts an input word and writes the result instead of it.

The cipher machine can perform two operations:
1. Copy any symbol on the tape to another position;
2. Apply a fixed one-to-one function $S : \mathbb{F}_2^m \to \mathbb{F}_2^m$ to the first m symbols, where $\mathbb{F}_2 = \{0, 1\}$.

The same sequence of operations (the encryption program) is applied to all input words of length n. Find the conditions for S so that the machine can perform any bijective mapping of words of length n.

Examples of operations.
1. For instance, the machine can copy the third symbol to the fifth place:

1	1	**1**	0	**0**	0	1	1	1	…

The result will be

1	1	1	0	**1**	0	1	1	1	…

2. Let m be 3 and $S(x, y, z) = (x, y, x \oplus z)$; applying S to the first three symbols:

1	**1**	**1**	0	0	0	1	1	1	…

The result will be

1	**1**	**0**	0	0	0	1	1	1	…

4.10. Problem "A modification of PRESENT"

Peter decided to modify the well-known cipher PRESENT.

At first, we give a description of PRESENT according to the article "PRESENT: An Ultra-Lightweight Block Cipher" by A. Bogdanov and colleagues (2007).

It is a classical substitution-permutation network (SP-network) that consists of 31 rounds with the block size equal to 64 bits and the key size equal to 80 bits. Each of the 31 rounds consists of an XOR operation to introduce a round key K_i for $1 \le i \le 32$, where K_{32} is used for post-whitening, a non-linear substitution layer, and a linear bitwise permutation P. The non-linear layer uses a single 4-bit S-box S which is applied 16 times in parallel in each round.

addRoundKey. Given the current state $b_{63} \dots b_0$ and round key $K_i = k^i_{63}k^i_{62} \cdots k^i_0$ for $1 \le i \le 32$, addRoundKey consists of the operation $b_j \to b_j \oplus k^i_j$ for $0 \le j \le 63$.

sBoxlayer. The S-box is a permutation from $\mathbb{F}_2^4$ to $\mathbb{F}_2^4$. For sBoxLayer the current state $b_{63} \dots b_0$ is considered as sixteen 4-bit words $w_{15} \dots w_0$ where $w_i = b_{4\cdot i+3}||b_{4\cdot i+2}||\ b_{4\cdot i+1}||b_{4\cdot i}$ for $0 \le i \le 15$ and the output nibble $S[w_i]$ provides the updated state values in the obvious way. The action of this box in hexadecimal notation is defined by the following table.

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

pLayer. The bit permutation is defined by the table. Bit i of state is moved to bit position $P(i)$.

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

The key schedule. The user-supplied key is stored in a key register K and represented as $k_{79}k_{78} \dots k_0$. At round i, the 64-bit round key $K_i = k_{63}k_{62} \dots k_0$ consists of the 64 leftmost bits of the current contents of register K. Thus, at round i, we have $K_i = k_{63}k_{62} \dots k_0 = k_{79}k_{78} \dots k_{16}$. After extracting the round key K_i, the key register $K = k_{79}k_{78} \dots k_0$ is updated as follows. The key register is rotated by 61 bit positions to the left, then the left-most four bits $k_{79}k_{78}k_{77}k_{76}$ are passed through the PRESENT S-box, and finally the round-counter value i is XORed with bits $k_{19}k_{18}k_{17}k_{16}k_{15}$ of K with the least significant bit of round-counter on the right.

What Peter has modified:

- In **sBoxlayer**, he changed S-box to the following

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

- In **pLayer**, he applied permutation P^3 instead of P.
- In **the key schedule**, he rotated the key register by 16 bit positions to the left instead of 61. He used his new S-box from **sBoxlayer** here.
- Finally, he reduced the number of rounds to 15.

As a result, Peter got the new cipher Peter-PRESENT. Below, you can find examples of test vectors for Peter-PRESENT that are given as integers in hexadecimal notation.

plaintext	key	ciphertext
0000000000000000	00000000000000000000	f778777b0774f772
ffffffffffffffff	00000000000000000000	8887088478838888d
0000000000000000	ffffffffffffffffffff	7ff8fffb0ffc7ffa
ffffffffffffffff	ffffffffffffffffffff	00078004700b0005

Peter states that his modification is rather good, but his friend Mark does not think so. He claims that it is enough to get only two pairs ≪plaintext–ciphertext ≫ (P_1, C_1), (P_2, C_2), where $C_i = \text{Peter-PRESENT}(P_i, K)$, $i = 1, 2$, and K is the unknown key, for reading any message C encrypted with this key K in the ECB mode.

Peter decides to argue with Mark and presents the following pairs, where P_1 and P_2 form the message !NSUCRYPTO-2015! (ASCII codes of letters and little-endian order of bytes are used to form 64-bit integers as the inputs $b_{63}b_{62} \ldots b_0$):

$$\texttt{!NSUCRYP} \rightarrow P_1 = \texttt{5059524355534e21} \rightarrow C_1 = \texttt{2ddbf038b201448f}$$
$$\texttt{TO} - \texttt{2015!} \rightarrow P_2 = \texttt{21353130322d4f54} \rightarrow C_2 = \texttt{d4bf134bd57f4df2}$$

He asks Mark to read the secret message whose ciphertext C is

$$C = \begin{matrix} \texttt{37aa471c953defe1} & \texttt{91aa595c0236edc9} & \texttt{80f10a020c33e5cb} \\ \texttt{ddf14e15923df8dc} & \texttt{8cf8470d027af1db} & \texttt{9caa061e9537ead1} \\ \texttt{92e10a1e072ea2c0} & \texttt{d1f1501e9b27f2c3} & \texttt{94e750140134e386} \\ \texttt{92f6595b093de3d2} & \texttt{99ec435b0235ebdc} & \texttt{83ef4b099b37f886} \\ \texttt{9eef461e4f76eecf} & \texttt{9eaa4912093df8d2} & \texttt{ddf15e129231f8c7} \\ \texttt{89ec45184f3ee4cf} & \texttt{94e25e5b9c36eddc} & \texttt{87e55a0b9221a2d2} \\ \texttt{ddae471d0e36a2d2} & \texttt{9aec4b159533efca} & \texttt{98e5495b0b34eb86} \\ \texttt{9cf643180e34ffc3} & \texttt{89aa4c124f21e4c9} & \texttt{ddf6594ad57aefce} \\ \texttt{dbfb500e9b34efc5} & & \end{matrix}$$

Can Mark win the argument?

4.11. Problem "Highly nonlinear functions"

One of the interesting classes of one-to-one vectorial Boolean functions of the form $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, where n is even, is the set of functions such that $F^{-1} = F$. Does this class contain a function with nonlinearity not less than $2^{n-1} - 2^{n/2}$?

Remark. Recall several definitions.

- A vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be represented as the set of its n coordinate Boolean functions: $F = (f_1, f_2, \ldots, f_n)$, where $f_1, \cdots, f_n : \mathbb{F}_2^n \to \mathbb{F}_2$;
- The Hamming distance $dist(f,g)$ between two Boolean function $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ is equal to the number of vectors $x \in \mathbb{F}_2^n$ such that $f(x) \neq g(x)$;
- Nonlinearity nl_F of F is equal to

$$\min_{b \in \mathbb{F}_2^n, b \neq 0} \min_{a \in \mathbb{F}_2^n, c \in \mathbb{F}_2} dist(b \cdot F, \ell_{a,c})$$

where $b \cdot F = b_1 f_1 \oplus b_2 f_2 \oplus \ldots \oplus b_n f_n$ and $\ell_{a,c}(x) = a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_n x_n \oplus c$.

4.12. Problem "Covering radius — 2"

In order to protect a new block cipher against some attacks based on S-box approximations, Alice must solve the following problem.

Let $\mathbb{F}_2^n$ be an n-dimensional vector space over the field $\mathbb{F}_2 = \{0, 1\}$. Let $n = 2k$, where k is a positive integer. Evaluate the covering radius and describe the metric complement of the linear subspace spanned by the rows of the following $k \times n$ matrix:

$$M = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ & & & & & \ddots & \ddots & \ddots & & & & \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Remark I. Recall several definitions and notions. A set $L \subseteq \mathbb{F}_2^n$ is called a *linear subspace* if for every $x, y \in L$, the sum $x \oplus y$ is also in L. The *Hamming distance* $d(x, y)$ between vectors $x, y \in \mathbb{F}_2^n$ is defined as the number of positions where they differ, that is, $d(x, y) = |\{i \mid x_i \neq y_i\}|$. The Hamming distance from a vector y to a subset $X \subseteq \mathbb{F}_2^n$ is defined as $d(y, X) = \min_{x \in X} d(y, x)$. Since the distance between any two vectors is bounded by n, for an arbitrary subset X there is the number $d(X)$ such that

- For every $y \in \mathbb{F}_2^n$, it holds $d(y, X) \leq d(X)$;
- There is a vector $z \in \mathbb{F}_2^n$ with $d(z, X) = d(X)$.

This number is called the *covering radius* of X. The set $\hat{X} = \{z \in \mathbb{F}_2^n \mid d(z, X) = d(X)\}$ is called the *metric complement* of X.

Remark II. Let us consider several examples:

– Let X consist of a single vector $x \in \mathbb{F}_2^n$. It is easy to see that $d(X) = n$ and $\hat{X} = \{x \oplus \mathbf{1}\}$, where $\mathbf{1}$ is the all-ones vector;

– Let Y be a ball of radius r centered at x: $Y = \{y \in \mathbb{F}_2^n \mid d(x, y) \leq r\}$. One can verify that $d(Y) = n - r$ and $\hat{Y} = \{x \oplus \mathbf{1}\}$.

4.13. Problem "An elliptic curve"

Bob develops a new cryptosystem based on elliptic curves. An elliptic curve determines the set of points (x, y), satisfying the equation $y^2 = x^3 + ax + b$ for some fixed real numbers a, b. For the system, Bob chooses the curve $y^2 = x^3 + 56x + 6$ and must find all integer points on this curve, that is points (x, y), where x and y are both integer numbers. Help Bob do this!

4.14. Problem "The machine DH-d"

Let G be a cyclic group of a large prime order q and g be a generator of G. Tom designed the machine DH-d that on input (g, g^x) outputs g^{x^d}. Here, g^x is an arbitrary element of G, and d is a small fixed positive integer.

Use the machine DH-d to solve the Diffie-Hellman problem (Diffie and Hellman, 1976), that is, find g^{xy} from (g, g^x, g^y). Suggest a solution with the minimal number of requests to the machine.

4.15. Problem "Palindrome cipher"

The company *Palindrome* had been using the block cipher DES (National Bureau of Standards, 1977) to encrypt its documents for the 12 years since its foundation until its engineers made the decision to use the block cipher Blowfish (Schneier, 1994) in addition to DES. It was in 2005. Up to now, all its documents are encrypted by DES, and then the result is also encrypted by Blowfish. The encryption is conducted in ECB mode.

Both ciphers DES and Blowfish have the same key and block lengths equal to 64 bits (the descriptions of these ciphers can be easily found).

As a result of information leakage, which occurred during the celebration of the anniversary of the company, the text of a greeting card leaked to the Internet. The text of the greeting card was

Dear colleagues! Congratulations for our wonderful journey of 20 years of success and we hope the same for the future also!

The ciphertext for that greeting card was

$C =$ 83c100497b13525e fc8d3201d58ab9ed f6820425912ce184
23034db7b4408629 4df36ca87ad39f4a 99277e6f1e217dfd
f2eab13d1161e849 0fe72e9b98fc1e8a 0aa5680e3b4022cb
4e44c8745afae37f bd5d6d49292bd1b2 9386f2f383061bfd
ae8fca32e6745687 565d353f3bbb1204 aa79742f7ab55fb1
123e6cf37fbad6fe

Could you decrypt the following ciphertext that was intercepted in the company network a few weeks ago?

$C =$ cf414505b7d3aee3 36f48ae753ec799c fb49aaea17fa2a38
2992ed164e9622aa 0b64549dad59a803 0b93be9baf9339e6
fe9780d39168bdff 10d77405d1b51a6a 5475ddf991ef3ad9
85a6c0c451b75da5 aa4c59ec0c40af09 852b70cebeb127b9
43c362dccbebf21e dbb2b086aba67212 1c92e2f327a03b05
b1affd236d8e0f9c 62386237b27597b4 cbe8ec78b07f4ce6

It is known that an encryption 128-bit encryption key is changed dynamically every day according to certain rules, and it is always a sequence of 128 bits where each of the 16 bytes is given by ASCII codes for the figures from `0` to `9`. The first 64 bits form a `DES` key, and the other 64 bits form a `Blowfish` key. The parity bits of the DES key are to be ignored.

Here, we present some technical information of the company encryption. Below, you can find examples of test vectors for combination of both ciphers `DES` and `Blowfish`. They are given as 64-bit integers $b_{63}b_{62}\ldots b_0$ in hexadecimal notation.

plaintext	DES key	Blowfish key	ciphertext
0000000000000000	0000000000000000	0000000000000000	561543527d054ad0
0000000000000000	0000000000000000	ffffffffffffffff	df27adaec8337f57
0000000000000000	ffffffffffffffff	0000000000000000	11148646af0d82e9
ffffffffffffffff	0000000000000000	ffffffffffffffff	18708bdc3837046f
6c6f632072616544	3837363534333231	3132333435363738	72e66b26309de78c

To form a 64-bit integer $b_{63}b_{62}\ldots b_0$, each consecutive eight symbols of an original text (or key) are transformed into their ASCII codes and little-endian order of bytes is used.

For example, let us encrypt the message `Dear colleagues!` using the keys `12345678` and `87654321` for `DES` and `Blowfish`, respectively. We divide it into two blocks of eight symbols `Dear col` and `leagues!`, and encrypt them separately:

$$\texttt{Dear col} \to P_1 = \texttt{6c6f632072616544} \to \texttt{DES} \to T_1 = \texttt{cb32b921efe674e5} \to$$
$$\to \texttt{Blowfish} \to C_1 = \texttt{72e66b26309de78c}$$
$$\texttt{leagues!} \to P_2 = \texttt{217365756761656c} \to \texttt{DES} \to T_2 = \texttt{f3d9c5f0cf2e9e8f} \to$$
$$\to \texttt{Blowfish} \to C_2 = \texttt{2d9f9fd83b15ae75}$$

Thus, the ciphertext is `72e66b26309de78c 2d9f9fd83b15ae75`.

4.16. Problem "Hypothesis" (Unsolved)

Prove the following hypothesis, or find a counterexample to it.

Hypothesis. For all $n \geq 2$, there exists a Boolean function $g : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ in the disjunctive normal form, *where every variable appears not more than one time*, so that a binary sequence $\{u_1, u_2,\ldots\}$ produced for all $t \geq 1$ from the initial state $u_1,\ldots, u_n$ according to the following rule

$$u_{t+n} = u_t \oplus g(u_{t+1}, u_{t+2}, \cdots, u_{t+n-1})$$

has the maximal possible period equal to 2^n.

Remark I. A Boolean function g in m variables is given in a disjunctive normal form if $g(x_1,\ldots, x_m) = A_1 \vee \ldots \vee A_k$, where A_i is a conjunction of variables or their negations, $i = 1,\ldots, k$.

Remark II. In the table, the functions g that confirm the hypothesis for small n are presented.

n	the examples of $g(x_1, \ldots, x_{n-1})$
2	1
3	$x_1 \vee \overline{x}_2$
4	$x_1 \vee \overline{x}_2\overline{x}_3, x_1 \vee x_2 \vee \overline{x}_3$
5	$x_2 \vee \overline{x}_1\overline{x}_3\overline{x}_4, x_1 \vee x_2x_3 \vee \overline{x}_4$

4.17. Problem "A secret sharing" (Unsolved)

Alice, Bob, and Caroline are going to create a secret sharing system. They choose a subset $M \subseteq \mathbb{F}_2^n$ and want to share a secret element u from M in the following way: The secret is represented as $x \oplus y \oplus z$ where x, y, z are different elements of $\overline{M} = \mathbb{F}_2^n \backslash M$; Alice, Bob, and Caroline will store x, y, and z, respectively. Here, $\mathbb{F}_2^n$ is the set of all binary vectors of length n.

To use the system, the sets M and $\overline{M}$ should satisfy the following conditions:

1. Each element $u \in M$ can be represented as $u = x \oplus y \oplus z$, where x, y, z are different elements of $\overline{M}$;
2. For all different $x, y, z \in \overline{M}$, it is right that $x \oplus y \oplus z \in M$.

Help them to implement the system suggesting an explicit construction of the set M for an arbitrary n.

5. Solutions of the problems

Here, we discuss the solutions of the problems. Special attention is paid to the solutions of the participants (right/wrong and beautiful).

5.1. Problem "Key sharing"

Solution. Consider remainders modulo 3 of all sets. There are all possible remainders (1, 2, and 0) in the set of each person. Hence, it does not matter who exactly forgot the rule, they are still able to open the safe in the following way: If the remainders of the two inserted keys are {0,1}, then the necessary sequence of keys (in terms of remainders) is {0,1,2,0,1,2,0,1,2}. It is obvious that such a sum is divisible by 3. The same can be done with all possible pairs of remainders.

This task was completely solved by 15 senior pupils, and they all used the fact that each person possesses the entire set of possible remainders. Another five participants offered partial solutions.

5.2. Problem "RSA numbers"

Solution. This problem can be solved in various ways. One interesting and nontrivial solution was sent by participant Alexandr Evpak (SESC NSU, Novosibirsk). Let us consider it.

Since p and q are prime numbers, and it holds

$$\begin{aligned} &p^{4x} + 4 \cdot 2015 = q^{4y};\\ &q^{4y} - p^{4x} = (q^{2y} - p^{2x})(q^{2y} + p^{2x}) = 8060;\\ &(q^{y} - p^{x})(q^{y} + p^{x})(q^{2y} + p^{2x}) \quad = 4 \cdot 5 \cdot 13 \cdot 31; \end{aligned}$$

we get that p and q are odd numbers. The following relations hold: $2 \mid (q^y - p^x)$, $2 \mid (q^y + p^x)$ and $2 \mid (q^{2y} + p^{2x})$, then their product is divisible by 8, but 8060 is not divisible by 8, so the answer should be negative.

The most widespread idea from the sent solutions was to consider the residue modulo 3 of both equation's sides. Let us provide a beautiful solution by Vladimir Schavelev (Gymnasium 6, Novosibirsk):

Let $A = p^{4x}$ and $B = q^{4y}$. Look at both sides of the equation modulo 3: $A + 2 = B$. It is known that a perfect square and 2 can not be congruent modulo 3. If $A \equiv 0 \bmod 3$, then $B \equiv 2 \bmod 3$, that is not the case. If $A \equiv 1 \bmod 3$, then $B \equiv 0 \bmod 3$, hence 3 divides B and $q = 3$, since q is a prime number. We can note that $B \equiv 1 \bmod 8$, hence $A = B - 4 \cdot 2015 \equiv 1 - 4 \equiv 5 \bmod 8$. But the number in degree $4y$ and 5 can not be congruent modulo 8, so we should not buy these numbers from Eve.

This task was solved by 18 senior pupils, but unfortunately, a few participants did not check all possible variants of the primes because they did not consider small numbers.

5.3. Problem "Bigrams"

Solution. We split this sentence into bigrams:

THE MEETING WILL TAKE PLACE AT THREE IN EEYORE-EAGLE-BEE CREEK INN →(TH)(EM)(EE)(TI)(NG)(WI)(LL)(TA)(KE)(PL)(AC)(EA)(TT) (HR)(EE)(IN)(EE)(YO)(RE)(EA)(GL)(EB)(EE)(CR)(EE)(KI)(NN)

We have the following number of bigrams of each type:

Bigrams I: 8 (EE, EA, EE, EE, YO, EA, EE, EE)
Bigrams II: 9 (TH, NG, LL, PL, TT, HR, GL, CR, NN)
Bigrams III: 10 (EM, TI, WI, TA, KE, AC, IN, RE, EB, KI)

The parity of the sum Bigrams I and Bigrams III is invariant, because if $B_1 =$ Bigram I, $B_2 =$ Bigram III, their sum is reduced by 2 and the parity is not changed, if B_1 or $B_2 =$ Bigram II, the sum is not changed. In the beginning, this sum is even, so if the number of Bigrams III is equal to 1, then the number of Bigrams I is not equal to 0, so the answer is negative.

Nineteen participants completely coped with this problem, and some of them wrote the code, which allows one to obtain the final state (one vowel and one consonant) from the initial state.

5.4. Problem "An encryption table"

Solution. Since we are provided with a fragment of the encryption table, we could try to find a part of the codeword by filling each row with letters to the left (MSR are hardly the part of a word).

E	F	G	H	I	J	K	L	M	N	O
K	L	M	N	O	P	Q	R	S	T	U
J	K	L	M	N	O	P	Q	R	S	T

The only suitable part seems to be ION, and it is likely to be the end of the codeword. Thus, we know rows 9 to 11 of the encryption table. If we suppose that letter T is before ION, then the first word of the ciphertext could be TH.. that corresponds to the codeword ..... ATION. It allows us to recover the eighth ciphertext word SI.P.E to SIMPLE and get the first letter I of the codeword. Step by step, we easily decrypt the whole ciphertext THIS METHOD

IS REFERRED TO AS THE SIMPLE SQUARE CIPHER and the codeword INSPIRATION.

This problem was completely solved by almost all participants (by 107 out of 117 students, by 8 out of 12 professionals, and by 16 out of 30 senior pupils). Note that many participants started to solve this problem applying another approach. They noticed that (7,5) is the most frequent letter in the ciphertext and supposed it to be E. This observation (being Mary's mistake in choosing the codeword) helped them to find other letters of the codeword by analyzing the fourth and seventh words .EFE..ED and .HE. As a result, they decrypted the whole ciphertext.

5.5. Problem "Crypto street"

Solution. Notice that the total number of floors is equal to the number of columns in the given text. We have four types of rectangular windows: red, green, blue, and yellow. Dark and circle-shaped windows are to be considered as spaces. Hence, starting from the bottom-left corner of the text (letter B), we write all the letters in a few rows depending on colors. In such way, we obtain the row with red windows, the row with blue windows, and so one. The answer is:

Yellow: I LOVED YOU: AND, IT MAY BE, FROM MY SOUL
Green: THE FORMER LOVE HAS NEVER GONE AWAY,
Red: BUT LET IT NOT RECALL TO YOU MY DOLE;
Blue: I WISH NOT SADDEN YOU IN ANY WAY.

This is a part of a famous poem written by Alexander Pushkin and translated by Yevgeny Bonver.

This problem was solved by 37 students, three professionals, and six senior pupils. They all used this basic approach to cope with the task. A few participants read only rows, tinted in particular color, so their solutions were not finalized.

5.6. Problem "Give an answer"

Solution. We can obtain the following information from the problem condition: The friends have used an asymmetric cryptosystem, and the length of their alphabet is $39 = 3 \cdot 13$. This brings to mind the idea that the RSA algorithm has been used, which is also supported by the names of the friends: **R**oman, **S**tephan, **A**nton. Thus, if the RSA modulus $n = 39$, then $\varphi(n) = 24$, where φ is Euler's totient function, and the only encryption/deciphering exponents that could be correct are 1, 5, 7, 11, 13, 17, 19, 23. Simple analysis shows that there are four pairs of equivalent exponents: 1 and 13, 5 and 17, 7 and 19, 11 and 23. Moreover, the encryption and deciphering exponents

coincide with each other. So, we must consider only three nontrivial exponents. As a result, we get that Roman's public key is 11, and Stephan's public key is 5. The chat was the following:

Stephan to Roman: WHAT IS YOUR FAVORITE ADVENTURE NOVEL?
Roman to Stephan: AROUND THE WORLD IN 80 DAYS.
Anton to Stephan: THE ADVENTURES OF TOM SAWYER

The problem was solved by eight students, but none of them used the solution described above; they found the answer by applying frequency analysis only. They said that different substitution ciphers were used without explaining why there were no secret keys exchanges. The most detailed solution was provided by Evgeniy Strepetov (Saratov State University). It is interesting to mention the favorite books of the participants: *Treasure Island, The Mysterious Island, The Children of Captain Grant, The Inhabited Island,* and *The Adventures of Tintin*.

5.7. Problem "Covering radius"

Solution. Divide all coordinates into pairs like this: $(1, n)$, $(2, n-1)$, …, $(k, k+1)$.

We can say that each pair of coordinates does not depend on the other in relation to the distance between a vector and the set L, so for arbitrary $y \in \mathbb{F}_2^n$, there is vector x from L such that there is not more than one nonzero element in each pair of coordinates of $y \oplus x$, therefore $d(X) \leq k$. In fact, $d(X)$ is equal to k and the metric complement consists of vectors that have only one 1 for each pair of coordinates.

This problem was solved by nine participants, and they all used a similar approach. Other solutions of participants were not complete.

5.8. Problem "Guess the cipher"

Solution. The encryption algorithm for NSUCRYPTO'2015 is the following.

1. The plaintext/ciphertext is a word in the alphabet "A", "B", ..., "Z".
2. The length of the ciphertext is twice the length of the plaintext.
3. A random symbol from "A" to "Y" is prepended to each plaintext symbol. The obtained pair is transformed into integers $p_0 \in \{0, 1, \ldots, 25\}$, $p_1 \in \{0, 1, \ldots, 24\}$. Then, the integer $p = 26p_1 + p_0$ is encrypted in the manner of RSA: $c = p^3 \bmod 667$, where the modulus is $667 = 23 \cdot 29$.

   The ciphertext c is presented as $c = 26c_1 + c_0$, both $c_1, c_2 \in \{0, 1, \ldots, 25\}$, and c_1, c_2 are converted into symbols.
4. The pair of ciphertext symbols is transformed into an integer c. This integer is decrypted in the following way: $p = c^{103} \bmod 667$.

   The plaintext symbol can be recovered using the residue of p mod 26.

This problem was solved by many participants, and most of them solved the problem by obtaining the list of all possible bigrams for each letter (19 teams proposed the full description).

5.9. Problem "A binary tape"

Solution. Here, we provide the best solution for the problem. It was proposed by the participant Alexey Udovenko (University of Luxembourg).

Let $M(S, x)$ be the result of running some machine with function S and input x.

The function is one-to-one, and the domain is equal to the codomain, therefore the function is a bijection.

1. The first necessary condition is that for the all-zero input, there should be at least one non-zero output bit of S. Otherwise, the machine will not be able to compute a single 1-bit (the whole infinite tape is filled with zeros).

   This condition allows the machine to get a constant 1-bit.
2. Let us assume that S is an affine function, that is, that it can be represented as $S(x) = Ax + b$, where A is a $m \times m$ matrix over $\mathbb{F}_2$, b is a binary vector of length m. At each step of the machine, each bit is an affine combination of some input bits. Therefore, for example, $M(S, 00) \oplus M(S, 10) = M(S, 01) \oplus M(S, 11)$. It is impossible to compute a mapping such that $M(S, 11) \neq M(S, 00) \oplus M(S, 10) \oplus M(S, 01)$. Hence, S is not affine.

We now prove that these two conditions are sufficient. We will use the fact that any function $\mathbb{F}_2^m \to \mathbb{F}_2$ can be uniquely represented as an ANF, that is, as a multivariate polynomial with variables from $\mathbb{F}_2$.

1. Consider some input $c_0 \in \mathbb{F}_2^m$ with a zero bit in some position. Let c_1 be equal to c_0 with that bit set to 1. For some c_0, some output bit of $S(c_0)$ is equal to 1, and the same output bit of $S(c_1)$ is equal to 0. Indeed, we start with $x = 0^m$. We know that $S(0^m) \neq 0^m$. We will set bits to 1 one-by-one to make x equal to $S^{-1}(0^m)$. Then, assign $c_1 = x = S^{-1}(0^m)$, and let c_0 be equal to x without the last setting of 1-bit. Therefore, flipping this bit from 0 to 1 flipped some output bit from 1 to 0.

   This means that we can fix c_0 except that zero bit and compute a Boolean NOT function.
2. Since S is not affine, some of the output bits contain a term of degree $d \geq 2$ in its ANF. We let $d - 2$ variables be equal to 1, and then we will have a function $\mathbb{F}_2^2 \to \mathbb{F}_2$ with a term of degree 2 in its ANF. This ANF may contain other terms. Up to renaming the input variables and then up to applying the NOT function, the possible ANFs are ab and $ab + a$. Note that the second one is equal to $a(b + 1)$, therefore we can apply NOT to the variable b and get the function with the ANF ab, that is, the Boolean function AND.

Since the machine now has two primitive functions NOT and AND, every Boolean function can be computed and any vectorial Boolean function as well. Therefore, the necessary and sufficient conditions are (1) $S(0^m) \neq 0^m$; (2) S is not affine.

Other full solutions were proposed by Alexey Miloserdov, Nikita Odinokih, Saveliy Skresanov (Novosibirsk State University), and Samir Godzhaev, Ravil Khisamov (Lomonosov Moscow State University).

5.10. Problem "A modification of PRESENT"

Solution. There are several ways to solve this problem. We describe one method that does not include recovery of the unknown secret key. At first, from Peter's modifications we get the following facts:

1. The permutation P^3 is the identity, so there is no permutation layer in Peter-PRESENT.
2. The new S-box has the representation $S(x, y, z, t) = (1 \oplus x \oplus y{\cdot}z \oplus y{\cdot}t, 1 \oplus t, y, z)$. Thus, its last three coordinate functions are affine and independent from the input variable x.

Let $P = p_{63}p_{62} \ldots p_0$, $C = c_{63}c_{62} \ldots c_0$ and $P' = p'_{63}p'_{62} \ldots p'_0$, $C' = c'_{63}c'_{62} \ldots c'_0$ be two pairs of plaintext and ciphertext obtained with the same unknown key K. The two facts above easily imply that we have the equality $p_{4\cdot i+j} \oplus c_{4\cdot i+j} = p'_{4\cdot i+j} \oplus c'_{4\cdot i+j}$ for all $i = 0, \ldots, 15$ and $j = 0, 1, 2$. Thus, given only one pair of known plaintext and ciphertext, that is (P, C), and another ciphertext C', we can obtain 75% of the bits of the corresponding plaintext P'. Additionally, since ASCII code is used, we can suppose that bits $p'_{8\cdot i+7}$ are equal to 0 for all $i = 0, \ldots, 7$.

To decrypt the ciphertext from the problem condition, we must vary eight unknown bits in each block and analyze the combinations of letters obtained. It can be easily done by applying a computer program, and the only readable text is the following:

> George Boole's legacy surrounds us everywhere, in the computers, information storage and retrieval, electronic circuits and controls that support life, learning and communications in the 21st century.

Using different methods, 11 teams were able to decrypt the secret message that was devoted to the 200th anniversary of George Boole's birth on 2 November 2015.

Solutions similar to the one described above were put forth by the teams from Minsk (Anna Gusakova, Dzmitry Emelyanov, Vadzim Marchuk) and Prague (Jakub Klemsa, Tomas Jeziorsky, Andrew Kozlik). Note that many other teams applied another approach and also found the secret key.

Their method was based on the fact that Peter's modification of the key schedule is weak. Namely, we can form four groups of 20 secret key bits that are independently used to encrypt/decipher four groups of corresponding 16 bits of plaintext/ciphertext. Thus, given a pair of plaintext and ciphertext, we can separately solve four tasks with complexity 2^{20} to recover all bits of the unknown secret key instead of the complexity 2^{80} of brute force.

5.11. Problem "Highly nonlinear functions"

Solution. We provide here the only full solution, proposed by the team consisting of Alexey Miloserdov, Nikita Odinokih, Saveliy Skresanov (Novosibirsk State University).

Let F be the function $F(x) = x^{2^n-2}$. It is obvious that F is an inverse function, since for the given element it puts into correspondence the multiplicative inverse element in $GF(2^n)$. The classic result related to our problem can be found in Nyberg (1994). It is proven there that the nonlinearity of this function has the following lower bound: $nl_F \geq 2^{n-1} - 2^{n/2}$. The answer is positive since all of the conditions are fulfilled.

5.12. Problem "Covering radius — 2"

Solution. Denote by L the linear subspace spanned by the given vectors. First, we notice that permutation of coordinates in $\mathbb{F}_2^n$ is an isometry and therefore does not change the maximum distance and metric complement in any irreversible way. A permutation of coordinates corresponds to a permutation of columns in the given matrix. We permute the columns of the matrix so that we get

$$M = \left(\begin{array}{cccccc|cccccc} 1 & 0 & 0 & \cdots & 0 & 0 & 1 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 & 1 & 1 & \cdots & 0 \\ & & \ddots & & & & & & \ddots & \ddots & & \\ 0 & \cdots & \cdots & \cdots & 1 & 0 & 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & \cdots & \cdots & \cdots & 0 & 1 & 1 & 0 & 0 & \cdots & 0 & 1 \end{array}\right)$$

which is easier to work with. Both halves have k columns.

Then, note that if $d(y, L) = k$, then for any $x \in L$ the distance from $y \oplus x$ to L is also k because

$$d(y \oplus x, L) = \min_{z \in X} d(y \oplus x, z) = \min_{z \in X} d(y, x \oplus z) = \min_{z \in X} d(y, z) = d(y, L).$$

Thus, the metric complement of L is the union of sets of the form $y \oplus L = \{y \oplus x\colon x \in L\}$, and we only need to find one vector from each set to describe the complement.

From an arbitrary $y \oplus L$, we can take (uniquely) the vector z such that it has zeros in the first k coordinates, because the first k columns of the matrix M' form a nonsingular square matrix. Moreover, the arbitrary vector z with zeros in the first k coordinates lies in $z \oplus L$. We can limit our search from $\mathbb{F}_2^n$ to $L^* = \{z \in \mathbb{F}_2^n : z_1 = z_2 = \cdots = z_k = 0\}$.

Let y be a vector from $\mathbb{F}_2^n$. We can express it as $y = (y_1|y_2)$, where $y_1, y_2 \in \mathbb{F}_2^k$. Then, all vectors from L^* are of the form $z = (0|z_2)$. Consider the following procedure (P*)

1. $s := 1$, $K = \theta$;
2. If the s-th and $(s+1)$-th coordinates of z_2 are both 1, then $z := z \oplus e_s$, add s and $s+1$ to K (if $s = k$ then $(s+1) \to 1$);
3. $s := s + 1$;
4. If s is greater than k, then STOP; otherwise, go to step 2.

Applying this to any vector $z \in L^*$ we get some vector $a = z \oplus x$, $x \in L$. Obviously, a_2 has no consecutive 1s, because what the algorithm does is eliminate them (here a_2 is viewed as a cyclic vector). Assume that l basis vectors were added to z during the procedure. Then, $wt(a_1) = l$.

Consider the vector a_2^* of length $k - 2l$ obtained from a_2 by deleting coordinates that are in the set K (a_2 has zeros in these coordinates). If there are two consecutive 1s in the vector a_2^*, (here a_2^* is **not** viewed as a cyclic vector), then they were either consecutive in vector a_2, or they were not. The first is impossible, as has already been mentioned earlier. The second means that in the vector a_2 there is 1 in position s that precedes position $(s+1)$ from the set K. This is also impossible, because in this case the algorithm would have eliminated the 1 in position s first. There are no consecutive 1s in the vector a_2^*, and therefore not more than $\lceil \frac{k-2l}{2} \rceil$ ones in the vector a_2^* (and also in a_2). Therefore, the weight of a is not greater than $\lceil \frac{k-2l}{2} \rceil + l = \lceil \frac{k}{2} \rceil$. In other words,

$$d(L) \le d(z, L) \le d(z, x) = wt(a) \le \left\lceil \frac{k}{2} \right\rceil$$

Now let us show that this is the exact value. Let $z^* = (0|1)$. Addition of any basis vector adds one 1 to the first half of z^* and removes not more than two from the second. Therefore, for any x from L we have $d(x, z^*) = wt(x \oplus z^*) \ge wt(z^*) + l - 2l = k - l$, where l is the number of basis vectors in the decomposition of x. If l is not greater than $\lfloor \frac{k}{2} \rfloor$, then through the obtained inequality we get that $d(x, z^*) \ge \lceil \frac{k}{2} \rceil$. If l is not less than $\lceil \frac{k}{2} \rceil$, then the weight of the first half of $x \oplus z^*$ alone is not less than $\lceil \frac{k}{2} \rceil$, and $d(x, z^*)$ is also not less than that. For any $x \in L$, we have $d(x, z^*) \ge \lceil \frac{k}{2} \rceil$, which proves that $d(L)$ is equal to $\lceil \frac{k}{2} \rceil$.

If k is odd, then this is the only vector from L^* that is in the metric complement. Let z be any other vector from L^*. Permute the last k coordinates cyclically so that the last coordinate of z is zero (the second half of the matrix

stays the same until the permutation of the rows). After applying (P*), we get the vector a such that $wt(a_1) = l$ and $wt(a_2) \leq \lfloor \frac{k-2l}{2} \rfloor$, because a_2^* is of odd length, has zero at the end, and has no two consecutive 1s. So $d(z, L) \leq wt(a) \leq \lfloor \frac{k}{2} \rfloor$.

Let k be even, $z \in L^*$, $z \neq z^*$. Let z_2 (as a cyclic vector) have a group of consecutive 1s of even size $2j$. We can add j basis vectors to z so that this group is eliminated, getting the vector a. Now we have a group of at least $2j + 2$ zeros in a_2 (to the left and right from that group of 1s, there were zeros, too). Excluding this group from a_2 and applying (P*) to the resulting (this time **not** cyclic) vector a_2' of length $k - 2j - 2$, we add l basis vectors, and the resulting b_2 has not more than $\frac{k-2j-2-2l}{2} = \frac{k}{2} - j - l - 1$ ones, because b_2^* cannot have more than two consecutive 1s (it can have two because of that removed coordinates breaking cyclicity). If we put everything together, the resulting vector has weight not greater than $j + l + \frac{k}{2} - j - l - 1 = \frac{k}{2} - 1$. So, z can not be in the metric complement.

This argument can be applied to vectors z so that z_2 has two consecutive zeros by assuming there is a group of 0 ones between those two zeros.

Now let us assume that the second half of $z \in L^*$ does not have two consecutive zeros and all groups of consecutive ones are of odd size. Let $x \in L$ be the closest vector to z. If the decomposition of x has two consecutive basis vectors, then they add 2 to the weight of $(z \oplus x)_1$ and subtract no more than 2 from the weight of $(z \oplus x)_2$, so we can remove them. So without loss of generality the decomposition of x does not have two consecutive basis vectors. Due to this, if the s-th and $(s + 1)$-th coordinates of z_2 are (01), (00), or (10), then e_s is also not in x, because it would only add to the distance. With that in mind, every group of ones (of odd size) is independent from others in the sense that if e_s is in x, then all two 1s of the second half of e_s are in the same group. Every group of size $2j - 1$ contributes exactly j to the distance (as proved for z^*), and has one zero after it, so the vector z_2 can be split in groups of even size $2j$ of the form (111…0), each adding j to the distance. Thus, the distance from x to z is equal to $\frac{k}{2}$.

All in all, $d(X)$ is equal to $\lceil \frac{k}{2} \rceil$, the metric complement consists of

- $z^* \oplus L$, where $z^* = (0|1)$, if k is odd;
- $z^* \oplus L$ and $\bigcup_{z \in L_{odd}} z \oplus L$, where L_{odd} is the set of vectors from L^* such that their second half does not have two consecutive zeros, and all groups of consecutive ones are of odd size, if k is even.

5.13. Problem "An elliptic curve"

Solution. The best solution was sent by participant Renzhang Liu (Beijing, Academy of Mathematics and Systems Science).

If (a, b) is an integer point on the curve $y^2 = x^3 + 56x = 6$, and p is a prime factor of b, then $(x - a)^2$ is a factor of $x^3 + 56x + 6 = 0$ over $\mathbb{F}_p$. Then, $g(x)$

and $g'(x)$ has a common factor $x - a$ over $\mathbb{F}_p$, where $g(x) = x^3 + 56x + 6$ and $g'(x) = 3x^2 + 56$. Since $3g(x) - xg'(x) = 2(56x + 9)$, we know that $x - a$ is also a factor of $2(56x + 9)$.

Note that p must be odd, since for any $b \in 2\mathbb{Z}$, $b^2 \bmod 4 = 0$, and $a^3 + 56a + 6 \bmod 4 = a^3 + 2 \bmod 4$ will never be 0. Then, $a^3 + 56a + 6 = 1 \bmod 8$, which gives $a \bmod 8 = 3$. Similarly, we know that $p \neq 3; 7$. Polynomials $x - a$ and $2(56x + 9)$ are of the same degree, we know $a = -9 \cdot (56)^{-1} \bmod p$. Note that $g'(a) = 0$. Then we have $3 \cdot 81 + 56^3 = 0 \bmod p$, which is $175859 = 0 \bmod p$. Since 175859 is a prime, we know that $p = 175859$. However, $x^3 + 56x + 6 = 0 \bmod p$ has no solution over $\mathbb{F}_p$, which means that there are no integer points on the curve $y^2 = x^3 + 56x + 6$.

Many participants obtained partial results. The majority of them used modular arithmetic and tried to find restrictions on possible values of variables.

5.14. Problem "The machine DHd"

Solution. The following solution was proposed by Anna Gusakova, Dzmitry Emelyanov, and Vadzim Marchuk (Belarusian State University). It is very short, but it requires quite a big number of queries to DHd.

Let us define the polynomial $f_{d-1}(x) = (x + 1)^d - (x - 1)^d$ over $\mathbb{Z}_q$, then

$$g^{f_{d-1}(x)} = g^{(x+1)^d}\left(g^{(x-1)^d}\right)^{-1} = \mathtt{DHd}(g, gg^x)\left(\mathtt{DHd}(g, g^{-1}g^x)\right)^{-1}.$$

Denote by DH_{d-1} the machine that calculates $g^{f_{d-1}(x)}$ by g and g^x.

Next, we can define $f_{d-2}(x) = f_{d-1}(x + 1) - f_{d-1}(x - 1)$ and the machine DH_{d-2}, that calculates

$$g^{f_{d-2}(x)} = g^{f_{d-1}(x+1)}\left(g^{f_{d-1}(x-1)}\right)^{-1} = DH_{d-1}(g, gg^x)DH_{d-1}(g, g^{-1}g^x))^{-1}$$

and so on.

The degree of the polynomial $f_k(x)$ is equal to k. In fact, the eldest coefficient e is equal to $2d \cdot 2(d-1) \cdot \ldots \cdot 2(k+1)$, as long as d is small and q is a large prime number. It holds that $(e, q) = 1$.

Therefore, we have constructed the machine DH_2, which calculates g^{ax^2+bx+c}, $a, b, c \in \mathbb{Z}_q$, $a \neq 0$. Let us construct DH2 in the following way:

$$g^{x^2} = \left(g^{ax^2+bx+c}\right)^{a^{-1}} \cdot \left(g^x\right)^{-ba^{-1}} \cdot g^{-ca^{-1}}.$$

Next, we can get

$$g^{xy} = \left(\mathtt{DH2}(g, g^x g^y) \cdot \left(\mathtt{DH2}(g, g^x(g^y)^{-1})\right)^{-1}\right)^{4^{-1}}.$$

Thus, the total number of queries to DHd is equal to 2^{d-1}.

The solution with the minimal query number was proposed by Alexey Udovenko (University of Luxembourg). Other complete solutions were

proposed by Alexey Miloserdov, Nikita Odinokih, Saveliy Skresanov (Novosibirsk State University); Roman Ginyatullin, Victoriya Vlasova, Igor Motroni (Moscow Engineering Physics Institute); Konstantin Kogos, Sergey Kyazhin, Anna Epishkina (Moscow Engineering Physics Institute).

5.15. Problem "Palindrome *cipher*"

Solution. First, we find the key used to encrypt the congratulation.

Because the bits of the key are ASCII codes of digits, we may suppose that the key is a 16-digit number. We have 10^{16} variants of the keys, and this number is too large to implement an exhaustive search. Using a meet-in-the-middle attack, we can reduce the complexity of the exhaustive search to 10^9 operations. This can be implemented quickly on a PC:

1. Encrypt the plaintext with the DES cipher using each variant of the DES-key one by one to get all 10^8 possible intermediate ciphertexts.
2. Decrypt each ciphertext by the Blowfish algorithm using each possible Blowfish-key one by one to get all 10^8 possible intermediate ciphertexts.
3. The intermediate ciphertexts are the original plaintexts after applying DES to them, but before applying Blowfish. Consider the intersection of these two sets of intermediate ciphertexts and mark out all the variants of used DES and Blowfish keys.
4. Steps 1 to 3 can be applied to each block (8 bytes) independently, because the ECB format of encryption was used. Apply these steps to each block to ensure that the obtained keys do encrypt each block correctly.

Using the program, we can find all possible variants of the key, encrypting the given congratulation into a fixed ciphertext. Note that 256 variants of the DES-key and one variant of the Blowfish-key are obtained.

One possible variant of the key is `06062002 22935162`.

DES uses only 7 bits of each byte of the key (the eighth was considered as being the parity check bit and is not used in this case). It explains all 256 variants of the DES-key. They all differ only in the least significant bits of each byte.

We can derive from the statement of the problem that in 2005, the company was 12 years old, so it was founded in 1993. Hence, the twentieth anniversary of the company was in 2013. It is likely that the first part of the key is the date in `DDMMYYYY` format. Then, the date of the twentieth anniversary is one of 06, 07, 16, 17 days in June (06) or July (07) (it is uncertain because of the parity check bits of the DES key).

Remember that company is named Palindrome. Consider the variant of the key `06062013 22935162`. It is not a palindrome, but is very close to one. In a random date $D_0D_1M_0M_1Y_0Y_1Y_2Y_3$, there was a key $D_0D_1M_0M_1Y_0Y_1Y_2Y_3abcdefgh$, where $a = Y_3 - 1$, $b = Y_2 + 1$, $c = Y_1 - 1$, $d = Y_0 + 1$, $e = M_1 - 1$, $f = M_0 + 1$, $g = D_1 - 1$, $h = D_0 + 1$ modulo 10. We can decrypt the main

ciphertext by trying out the dates in inverse order from the date of the Olympiad start 16.11.2015.

The key `01112015 42930201` decrypts the ciphertext as:

```
Quote of the day: ≪Most people say that it is the
intellect which makes a great scientist. They are
wrong: it is character. Albert Einstein≫
```

5.16. Problem "Hypothesis" (unsolved. special prize)

Solution. This problem is based on the hypothesis (1966) of G. P. Agibalov. The statement of this conjecture is the following:

Hypothesis. For all $n \geq 2$, there exists a Boolean function $g : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ in the disjunctive normal form, *where every variable appears not more than one time*, so that a binary sequence $\{u_1, u_2, \ldots\}$ produced for all $t \geq 1$ from the initial state $u_1,\ldots, u_n$ according to the following rule

$$u_{t+n} = u_t \oplus g(u_{t+1}, u_{t+2}, \cdots, u_{t+n-1})$$

has the maximal possible period equal to 2^n.

This hypothesis had been partially proved for every $n \leq 22$ in Agibalov (2007).

There was no complete solution of the problem. The best attempt was proposed by Mikhail Borodin, Katerina Karelina, and Lyudmila Kushchinskaya (Lomonosov Moscow State University). Their solution was based on linear recurrent sequences, but contained an unremovable mistake.

5.17. Problem "A secret sharing" (unsolved. special prize)

Solution. There was no complete solution of this problem, either. The most popular ideas of the participants were implemented in the algorithm to generate the set M and in the analysis of small dimensions. Interesting attempts were proposed by the teams of George Beloshapko, Anna Taranenko, and Evarist Fomenko (Novosibirsk State University, Sobolev Institute of Mathematics); Roman Ginyatullin, Victoriya Vlasova, and Igor Motroni (Moscow Engineering Physics Institute); Ivan Emeliyanenkov (Novosibirsk State University); Sergei Titov, Roman Taskin, Prokhor Sadkov, and Konstantin Kirienko (Ural State University of Railway Transport).

6. Winners of the Olympiad

In this section, we provide information about the winners of NSUCRYPTO'2015.

Winners of the first round in the school section A ("senior pupils")

Place	Name	Country, City	School	Grade	Score
1	Vladimir Schavelev	Russia, Novosibirsk	Gymnasium 6	9	20
2	Ekaterina Bestsennaya	Russia, Novosibirsk	SESC NSU	11	19
2	Alexey Solovev	Russia, Moscow	AESC MSU	10	19
3	Alexander Dorokhin	Russia, Novosibirsk	MOU 159	9	18
3	Arkadij Pokazan'ev	Russia, Novosibirsk	Gymnasium 6	8	17
3	Ivan Lozinskiy	Russia, Moscow	AESC MSU	11	17
3	Ivan Sutormin	Russia, Novosibirsk	SESC NSU	11	17
3	Alexandr Evpak	Russia, Novosibirsk	SESC NSU	11	16
Diploma	Nikita Mingaleev	Russia, Novosibirsk	SESC NSU	11	15
Diploma	Ivan Baksheev	Russia, Novosibirsk	Gymnasium 6	8	15

Winners of the first round in student section B (in the category "students")

Place	Name	Country, City	University	Department	Year	Score
1	Peter Razumovsky	Russia, Saratov	Saratov State University	Computer Science and Information Technology	5	14
2	Evgeniy Strepetov	Russia, Saratov	Saratov State University	Computer Science and Information Technology	5	13
2	Nikita Odinokih	Russia, Novosibirsk	Novosibirsk State University	Mathematics and Mechanics	4	13
2	Sergey Zhdanov	Russia, Saratov	Saratov State University	Computer Science and Information Technology	4	13
3	Alexey Miloserdov	Russia, Novosibirsk	Novosibirsk State University	Mathematics and Mechanics	3	12
3	Aliaksei Ivanin	Belarus, Minsk	Belarusian State University	Faculty of Applied Mathematics and Computer Science	5	12
3	Pavel Hvoryh	Russia, Omsk	Omsk State Technical University	Information Technologies and Computer Systems	4	12
3	Elena Khabarova	Russia, Novosibirsk	Novosibirsk State University	Economics	2	12
3	Mikhail Kotov	Russia, Tomsk	Tomsk State University	Applied Mathematics and Cybernetics	3	12
3	Vitaliy Cherkashin	Russia, Novosibirsk	Novosibirsk State University	Mathematics and Mechanics	2	12

Place	Name	Country, City	University	Department	Year	Score
Diploma	Vladimir Laptev	Russia, Omsk	Omsk State Technical University	Radio Engineering Faculty	3	12
Diploma	Anastasiya Yarunina	Russia, Engels	Saratov State University	Computer Science and Information Technology	3	12
Diploma	Charles de Mauroy	Russia, Novosibirsk	Novosibirsk State University	Mathematics and Mechanics	5	10
Diploma	Jakub Klemsa	Czech Republic, Prague	Czech Technical University in Prague	Mathematics	5	10
Diploma	Alexey Ripinen	Russia, Saratov	Saratov State University	Computer Science and Information Technology	4	10
Diploma	Anastasia Kislyakova	Russia, Moscow	Lomonosov Moscow State University	Computational Mathematics and Cybernetics	4	10
Diploma	Roman Lebedev	Russia, Novosibirsk	Novosibirsk State University	Physics	3	10
Diploma	Oleg Smirnov	Russia, Saratov	Saratov State University	Computer Science and Information Technology	5	10
Diploma	Konstantin Pavlov	Belarus, Minsk	Belarusian State University	Applied Mathematics and Computer Science	5	9

Winners of the first round in the student section B (in the category "professionals")

Place	Name	Country, City	Organization	Score
1	Renzhang Liu	China, Beijing	Academy of Mathematics and Systems Science	27
2	Vadzim Marchuk	Belarus, Minsk	Belarusian State University, Research Institute for Applied Problems of Mathematics and Informatics	25
3	Alexey Udovenko	Luxembourg, Luxembourg	University of Luxembourg	17
Diploma	George Beloshapko	Russia, Novosibirsk	Novosibirsk State University	14
Diploma	Andrew Kozlik	Czech Republic, Prague	SII	12

Winners of the second round (in the category "senior pupils")

Place	Name	Country, City	School	Grade	Score
Diploma	Ivan Lozinskiy, Bogdan Sinitsyn, Maxim Plushkin	Russia, Moscow	AESC MSU	11	11
Diploma	Andrei Igo	Russia, Novosibirsk	Gymnasium 6	10	6

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

Place	Name	Country, City	University	Department	Year	Score
1	Alexey Miloserdov, Nikita Odinokih, Saveliy Skresanov	Russia, Novosibirsk	Novosibirsk State University	Mechanics and Mathematics	3	41
2	Alexey Ripinen, Oleg Smirnov, Peter Razumovsky	Russia, Saratov	Saratov State University	Computer Science and Information Technology	5	34
3	Roman Ginyatullin, Victoriya Vlasova, Igor Motroni	Russia, Moscow	Moscow Engineering Physics Institute	IB, Cybernetics and Information Security, Information Security of Automated Systems	4	31
Diploma	Irina Slonkina	Russia, Novosibirsk	Novosibirsk State University of Economics and Management	Information and Technologies	3	18
Diploma	Samir Godzhaev, Ravil Khisamov	Russia, Moscow	Lomonosov Moscow State University	Mechanics and Mathematics	2	17
Diploma	Roman Rezvukhin, Vladimir Martyshin, Mikhail Zaytsev	Russia, Moscow	Moscow Engineering Physics Institute	Cybernetics and Information Security	4	16
Diploma	Roman Taskin, Prokhor Sadkov	Russia, Yekaterinburg	Ural State University of Railway Transport	Information security	3	14

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

Place	Name	Country, City	Organization	Score
1	Alexey Udovenko	Luxembourg, Luxembourg	University of Luxembourg	48
2	George Beloshapko, Anna Taranenko, Evarist Fomenko	Russia, Novosibirsk	Novosibirsk State University, Institute of Mathematics	42
3	Anna Gusakova, Dzmitry Emelyanov, Vadzim Marchuk	Belarus, Minsk	Belarusian State University, Research Institute for Applied problems of Mathematics and Informatics	30
Diploma	Mikhail Borodin, Katerina Karelina, Lyudmila Kushchinskaya	Russia, Moscow	Lomonosov Moscow State University	28
Diploma	Konstantin Kogos, Sergey Kyazhin, Anna Epishkina	Russia, Moscow	Moscow Engineering Physics Institute	27
Diploma	Evgeniya Ishchukova, Ekaterina Maro	Russia, Taganrog	Southern Federal University	26
Diploma	Sergey Belov, Grigory Sedov	Russia, Obninsk, Moscow	Lomonosov Moscow State University	23
Diploma	Jakub Klemsa, Tomas Jeziorsky, Andrew Kozlik	Czech Republic, Prague	Czech Technical University in Prague	22

About the authors

S. Agievich is the head of the IT Security Research Laboratory of the Research Institute for Applied Problems of Mathematics and Informatics (Belarusian State University). He teaches the "Cryptographic methods" course in the Faculty of Applied Mathematics and Informatics. His research interests: Boolean functions in cryptography, cryptographic algorithms and protocols, enumerative and asymptotic combinatorics, exponential sums and systems of polynomial equaitions.

A. Gorodilova is a researcher at the Laboratory of Discrete Analysis in the Sobolev Institute of Mathematics; she teaches courses in Boolean functions and cryptology at Novosibirsk State University and Specialized Educational Scientific Center of Novosibirsk State University. She is interested in cryptographic Boolean functions, APN functions, bent functions, symmetric cryptography, combinatorics, and algebra.

V. Idrisova is a PhD student in the Sobolev Institute of Mathematics. Also, she teaches a course in cryptology and information theory for master students at Novosibirsk State University. Her research interests includes vectorial Boolean functions, block ciphers, and side-channel attacks.

N. Kolomeec is a researcher at the Laboratory of Discrete Analysis in the Sobolev Institute of Mathematics. He teaches courses in cryptology in the Department of Mathematics and Mechanics at Novosibirsk State University. His research interests are Boolean functions in cryptography and pseudorandom sequences.

G. Shushuev is a PhD student at the Laboratory of Discrete Analysis in the Sobolev Institute of Mathematics; he teaches special course in cryptology in the Department of Mathematics and Mechanics at Novosibirsk State University. His research interests include block and stream ciphers, cryptanalysis, and cryptographic protocols.

N. Tokareva is a senior researcher at the Laboratory of Discrete Analysis in the Sobolev Institute of Mathematics; she teaches courses in cryptology in the Department of Mathematics

and Mechanics at Novosibirsk State University. Her research interests include Boolean functions in cryptography, bent functions, block and stream ciphers, cryptanalysis, coding theory, combinatorics, and algebra.

Acknowledgments

We are very grateful to Gennadiy Agibalov, Svetla Nikova, Irina Pankratova, Bart Preneel, and Vincent Rijmen for their valuable contribution to this article: ideas for the problems and all-out support. We thank Alexey Oblaukhov for his kind help during the Olympiad and in the process of writing this article. We thank Novosibirsk State University for the financial support of the Olympiad and invite you to take part in NSUCRYPTO-2017 that starts on 22 October 2017. Your ideas on the unsolved problems are also very welcome and can be sent to olymp@nsucrypto.ru.

Funding

The article was financially supported by RFBR (grants 15-07-01328, 15-31-20635), by the Ministry of Education and Science of the Russian Federation and grant N 0314-2015-0011.

References

Agibalov, G. 2007. *Normal reccurent sequences*, Bulletin of Tomsk State University. Supplement. 23:4–11 (in Russian).

Agievich, S., Gorodilova, A., Kolomeec, N., Nikova, S., Preneel, B., Rijmen, V., Shushuev, G., Tokareva, N., Vitkup, V. 2015. *Problems, solutions and experience of the First International Students' Olympiad in Cryptography*. Applied Discrete Mathematics (Prikl. Diskret. Matemat.). 3:41–62.

Bell, C. 2013. *The internet mystery that has the world baffled*. The Telegraph, 25 November, www.telegraph.co.uk/technology/internet/10468112/The-internet-mystery-that-has-the-world-baffled.html.

Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y., Vikkelsoe, C. 2007. PRESENT: An ultra-lightweight block cipher. In *Cryptographic Hardware and Embedded Systems — CHES. LNCS* 4727:450–466. Berlin: Springer.

Burton, B. A. 2008. *Breaking the routine: Events to complement Informatics Olympiad training*. Olympiads in Informatics. 2:5–15.

Diffie, W., Hellman, M. E. 1976. *New Directions in Cryptography*. IEEE Transactions on Information Theory, IT-22(6):644–654.

National Bureau of Standards. 1977. *Data Encryption Standard*. FIPS publication, N. 46, U. S. Department of Commerce.

Nyberg, K. 1994. Differentially uniform mappings for cryptography. In *Advances in Cryptology – EUROCRYPT'93 LNCS* 765:55–64. Berlin: Springer.

Schneier, B. 1994. Description of a new variable-length key, 64-bit block cipher (Blowfish). *Fast Software Encryption, LNCS* 809:191–204. Berlin: Springer.