конференция
РусКрипто

Ежегодная международная научно-практическая конференция
«РусКрипто'2023»

Криптография: вовлечение в профессию. Опыт Новосибирска

Наталья Токарева,
к.ф.-м.н., руководитель Криптографического центра (Новосибирск)
зав. лабораторией криптографии Новосибирского государственного университета

Криптографический центр (Новосибирск)

- Создан в 2011 году. Состав: более 20 преподавателей, аспирантов и студентов.
- Вовлечение в профессию: с 1-3 курса НГУ. Более 50 защит ВКР.
- Подключение к преподаванию, поступление в аспирантуру, защита.
- Направления деятельности:
  - Научные исследования в области криптографии
  - Преподавание и разработка программ
  - Организация масштабных мероприятий:

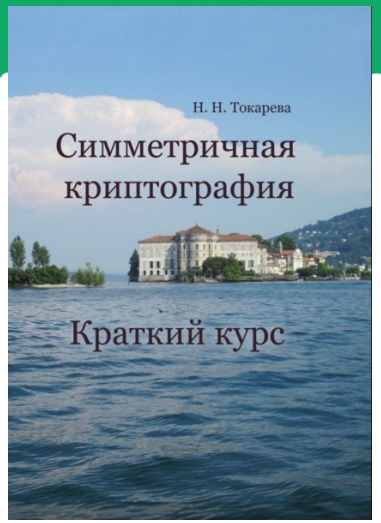
  Международная олимпиада по криптографии NSUCRYPTO

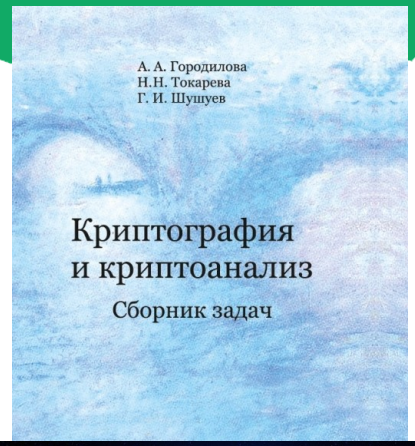
  Летняя школа по криптографии и информационной безопасности

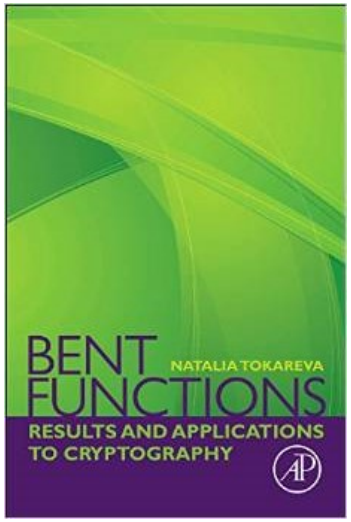
  Международная конференция SIBECRYPT «Компьютерная безопасность и криптография»
- Научные направления: симметричная криптография и криптоанализ; криптографические булевы функции; блочные шифры и S-блоки; постквантовая криптография.
- Научные контакты: Томск, Калининград, Москва, Таганрог, Минск (Беларусь), COSIC (Бельгия), Selmer Center (Норвегия) и др.

Преподавание

- Формирование группы Крипто-центра
- С 2011 года – научный семинар «Криптография и криптоанализ»
- 2018-2020 Первая в России англоязычная магистратура по криптографии.
- С 2022 года – новая англоязычная магистратура «Quantum technologies and cryptography».
- Наши курсы в настоящее время: «Криптография и криптоанализ», «Математические основы и приложения квантовой информатики: криптография и вычисления», «Основы теории информации и криптографии», «Криптография в задачах», «Криптография и криптоанализ. Современные методы», «Булевы функции в криптографии», «Введение в распределенные реестры и технологию блокчейн», «Криптографические проекты», «Современные вычислительные системы для решения задач криптографии и информационной безопасности» и др.







Летняя школа по криптографии

- Ежегодно: около 50 участников – преподавателей и студентов. Практика приглашённых преподавателей. Публикация сборника трудов.
- На школе совмещаются лекции и научно-практическая работа в проектах. После школы исследования продолжаются, публикуются научные статьи.
- География: Новосибирск, Москва, Томск, Калининград, Таганрог, Ростов-на-Дону, др. Сайт: www.crypto.nsu.ru

Летняя школа

КРИПТОГРАФИЯ

и информационная безопасность

7 августа - 17 августа 2023, Калининград

Новосибирский государственный университет
Международный математический центр в Академгородке
Северо-Западный центр математических исследований имени
Софьи Ковалевской (БФУ им. И.Канта)

объявляют о наборе студентов и учеников старших классов учебных заведений России на Летнюю школу "Криптография и информационная безопасность", которая пройдёт на базе БФУ им. Канта с 7 по 17 августа 2023 года.

На Летней школе с лекциями выступят российские специалисты по криптографии, ведущие разработчики постквантовых криптосистем, участвующих в конкурсе на новый государственный стандарт РФ.

Вас ждёт командная и индивидуальная работа над проектами по актуальным темам криптографии, спортивные занятия и круглый стол по современным проблемам криптографии.

Участие в Летней школе бесплатное, возможна частичная материальная поддержка проезда и проживания участников.
Количество мест ограничено.
Заявки принимаются до 17 мая 2023 года.
По всем вопросам обращайтесь на cryptography.nsu@gmail.com

Сайт Летней школы: https://crypto.nsu.ru/ru/letnyaya-shkola

Международная конференция SIBECRYPT

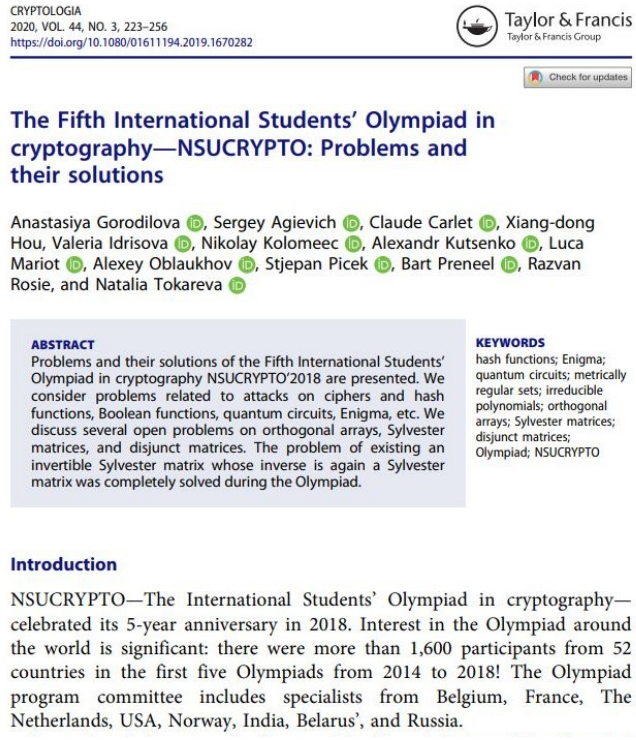
- Международная конференция «Сибирская научная школа-семинар «Компьютерная безопасность и криптография»» им. Г.П.Агибалова.
- www.sibecrypt.ru
- Проходит с 2001 года. В этом году – в 22-й раз.
- Одна из ведущих конференций по криптографии и компьютерной безопасности в России, ежегодно проходящая в разных городах Сибири. Её цель — обсуждение фундаментальных математических проблем криптографии и защиты информации в компьютерных системах и сетях, обмен научными результатами.
- География участников: Москва, Томск, Новосибирск, Красноярск, Калининград, Иркутск, Тюмень, Саратов, Ярославль и др.
- Организаторы:
  - Новосибирский государственный университет,
  - Международный математический центр в Академгородке
  - Томский государственный университет
  - Институт криптографии, связи и информатики Академии ФСБ
  - Академия криптографии Российской Федерации
  - Московский государственный университет им. М.В. Ломоносов
  - Северо-Западный центр математических исследований им. Софьи Ковалевской

Международная олимпиада NSUCRYPTO

- www.nsucrypto.nsu.ru
- Проходит с 2014 года. В этом году – десятая, юбилейная.
- Крупное международное мероприятие, цель которого привлечь молодых исследователей к решению вопросов современной криптографии, в том числе – к открытым научным проблемам. Мероприятие проводится дистанционно на английском языке.
- **Ежегодно в олимпиаде принимают участие около 800-1000 участников из 40-50 стран мира.** Общая география участников: более 68 стран.
- В настоящее время организаторами олимпиады выступают Криптографический Центр (Новосибирск), Международный Математический Центр в Академгородке, Новосибирский государственный университет, Университет г. Лёвена (Бельгия), Томский государственный университет, Белорусский государственный университет, Северо-Западный центр математических исследований имени Софьи Ковалевской и компания «Криптонит». В программный комитет олимпиады входят специалисты из России, Европы и США.
- По итогам каждой олимпиады публикуются научные статьи с разбором проблем, предложенных участникам, в том числе – нерешенных, требующих отдельного научного исследования. Победители и призеры олимпиады награждаются ценными призами, организуется доставка призов и дипломов иностранным участникам.

Международная олимпиада NSUCRYPTO

- www.nsucrypto.nsu.ru
- Каждый год мы рассылаем более 10 000 писем молодым специалистам в ИТ и криптографии по всему миру с приглашениями участвовать в Олимпиаде. Наша база постоянно обновляется. Около 200-400 дипломов и писем благодарностей отправляются по итогам олимпиады.
- **Приглашаем вас стать со-организатором или спонсором олимпиады!**



CRYPTOLOGIA
2020, VOL. 44, NO. 3, 223–256
https://doi.org/10.1080/01611194.2019.1670282

Taylor & Francis
Taylor & Francis Group

Check for updates

The Fifth International Students' Olympiad in cryptography—NSUCRYPTO: Problems and their solutions

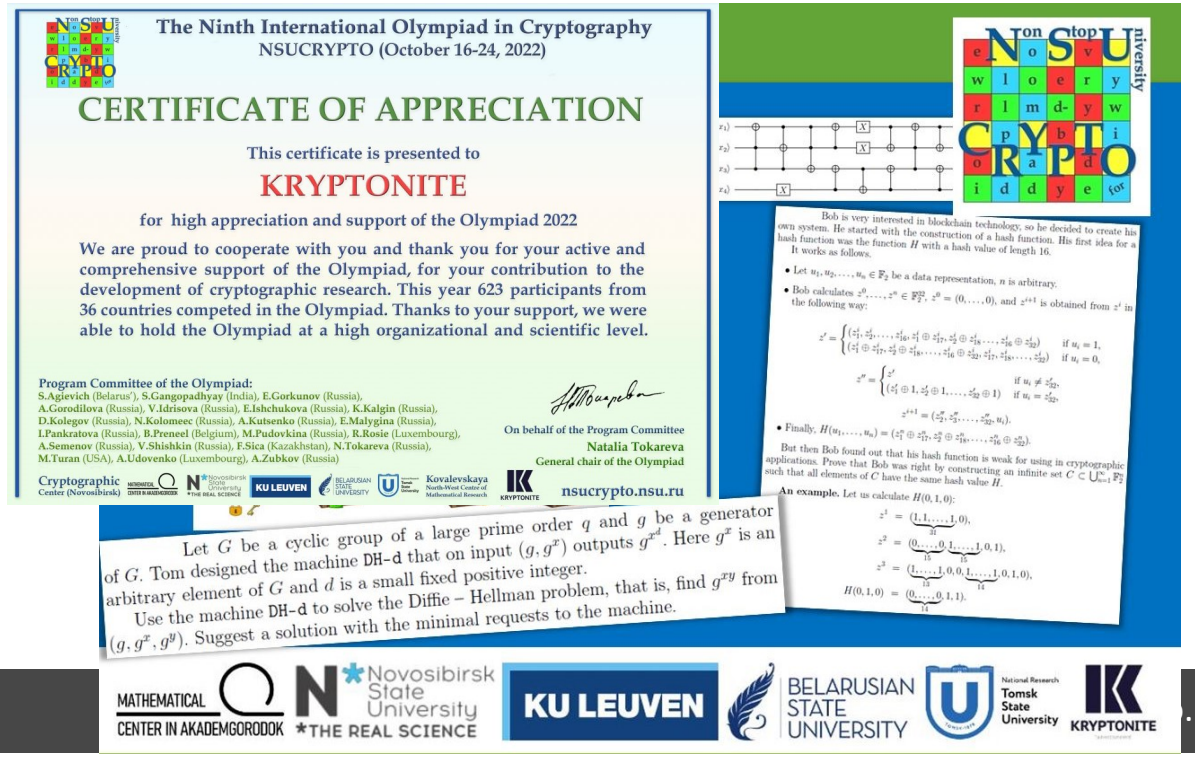
Anastasiya Gorodilova, Sergey Agievich, Claude Carlet, Xiang-dong Hou, Valeria Idrisova, Nikolay Kolomeec, Alexandr Kutsenko, Luca Mariot, Alexey Oblaukhov, Stjepan Picek, Bart Preneel, Razvan Rosie, and Natalia Tokareva

ABSTRACT
Problems and their solutions of the Fifth International Students' Olympiad in cryptography NSUCRYPTO'2018 are presented. We consider problems related to attacks on ciphers and hash functions, Boolean functions, quantum circuits, Enigma, etc. We discuss several open problems on orthogonal arrays, Sylvester matrices, and disjunct matrices. The problem of existing an invertible Sylvester matrix whose inverse is again a Sylvester matrix was completely solved during the Olympiad.

KEYWORDS
hash functions; Enigma; quantum circuits; metrically regular sets; irreducible polynomials; orthogonal arrays; Sylvester matrices; disjunct matrices; Olympiad; NSUCRYPTO

Introduction

NSUCRYPTO—The International Students' Olympiad in cryptography—celebrated its 5-year anniversary in 2018. Interest in the Olympiad around the world is significant: there were more than 1,600 participants from 52 countries in the first five Olympiads from 2014 to 2018! The Olympiad program committee includes specialists from Belgium, France, The Netherlands, USA, Norway, India, Belarus', and Russia.



The Ninth International Olympiad in Cryptography
NSUCRYPTO (October 16-24, 2022)

CERTIFICATE OF APPRECIATION

This certificate is presented to

KRYPTONITE

for high appreciation and support of the Olympiad 2022

We are proud to cooperate with you and thank you for your active and comprehensive support of the Olympiad, for your contribution to the development of cryptographic research. This year 623 participants from 36 countries competed in the Olympiad. Thanks to your support, we were able to hold the Olympiad at a high organizational and scientific level.

Program Committee of the Olympiad:
S.Agievich (Belarus'), S.Gangopadhyay (India), E.Gorkunov (Russia), A.Gorodilova (Russia), V.Idrisova (Russia), E.Ishchukova (Russia), K.Kalgin (Russia), D.Kolegov (Russia), N.Kolomeec (Russia), A.Kutsenko (Russia), E.Malygina (Russia), I.Pankratova (Russia), B.Preneel (Belgium), M.Pudovkina (Russia), R.Rosie (Luxembourg), A.Semenov (Russia), V.Shishkin (Russia), F.Sica (Kazakhstan), N.Tokareva (Russia), M.Turan (USA), A.Udovenko (Luxembourg), A.Zubkov (Russia)

On behalf of the Program Committee
Natalia Tokareva
General chair of the Olympiad

Cryptographic Center (Novosibirsk) · Kovalevskaya North-West Centre of Mathematical Research · KU LEUVEN · BELARUSIAN STATE UNIVERSITY · KRYPTONITE

nsucrypto.nsu.ru

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^{xd}. 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, that is, find g^{xy} from (g, g^x, g^y). Suggest a solution with the minimal requests to the machine.

Bob is very interested in blockchain technology, so he decided to create his own system. He started with the construction of a hash function. His first idea for a hash function was the function H with a hash value of length 16. It works as follows.

- Let $u_1, u_2, \ldots, u_n \in \mathbb{F}_2$ be a data representation, n is arbitrary.
- Bob calculates $z^0, \ldots, z^n \in \mathbb{F}_2^{32}$, $z^0 = (0, \ldots, 0)$, and z^{i+1} is obtained from z^i in the following way:

$$z' = \begin{cases} (z_1^i, z_2^i, \ldots, z_{16}^i, z_{17}^i \oplus z_1^i, z_2^i \oplus z_{18}^i, \ldots, z_{16}^i \oplus z_{32}^i) & \text{if } u_i = 1, \\ (z_1^i \oplus z_{17}^i, z_2^i \oplus z_{18}^i, \ldots, z_{16}^i \oplus z_{32}^i, z_{17}^i, z_{18}^i, \ldots, z_{32}^i) & \text{if } u_i = 0, \end{cases}$$

$$z'' = \begin{cases} z' & \text{if } u_i \neq z'_{32}, \\ (z_1' \oplus 1, z_2' \oplus 1, \ldots, z_{32}' \oplus 1) & \text{if } u_i = z'_{32}, \end{cases}$$

$$z^{i+1} = (z''_2, z''_3, \ldots, z''_{32}, u_i).$$

- Finally, $H(u_1, \ldots, u_n) = (z_1^n \oplus z_{17}^n, z_2^n \oplus z_{18}^n, \ldots, z_{16}^n \oplus z_{32}^n)$.

But then Bob found out that his hash function is weak for using in cryptographic applications. Prove that Bob was right by constructing an infinite set $C \subset \bigcup_{i=1}^{\infty} \mathbb{F}_2^i$ such that all elements of C have the same hash value H.

An example. Let us calculate $H(0,1,0)$:

$$z^1 = (\underbrace{1,1,\ldots,1}_{31},0),$$
$$z^2 = (\underbrace{0,\ldots,0}_{15},1,\underbrace{\ldots,1}_{15},0,1),$$
$$z^3 = (\underbrace{1,\ldots,1}_{14},0,0,1,\underbrace{\ldots,1}_{14},0,1,0),$$
$$H(0,1,0) = (\underbrace{0,\ldots,0}_{14},1,1).$$

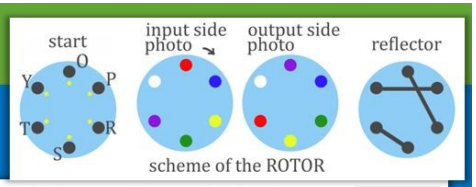
MATHEMATICAL CENTER IN AKADEMGORODOK · Novosibirsk State University *THE REAL SCIENCE · KU LEUVEN · BELARUSIAN STATE UNIVERSITY · National Research Tomsk State University · KRYPTONITE

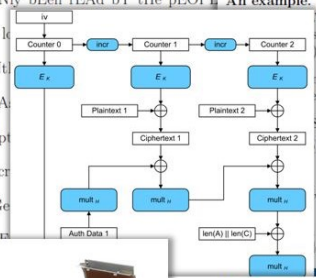
.ru

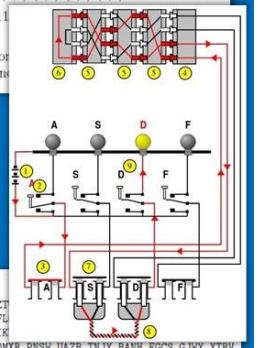
Международная олимпиада NSUCRYPTO

- Разнообразные задачи

“Fun tasks”: Historical ciphers



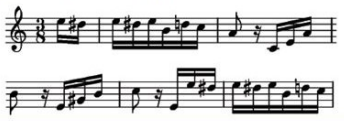




Decrypt the following ciphertext sent to Bob by Alice:

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.



Ciphertext:

RHSM ZHXX AOWW ZT
YLGE VGZG KULJ FL
BGSW OARG EYSP IK
BBRT ROZD XJCC OMXR PNSW UAZB TNJY BANH FGCS GJWY YTBV
VGLX KUZW PARO NMXP LDLZ ICBK XVSJ NXCF SOTA AQYS YZFX
MZDH MSZI ABAH RFXT FTPU VWMC PEXQ NZVA LMFX BHKG QGYS
BIYE MEUE PJNR AVTL JSUZ PLHQ MOUI IQFD HVXI NOOJ YJAF
WAVU PVQA FMKP AHLK XJYD GITB QSPK CUZU XPRK MUJJ YRJ

Link to “Moby Dick” text file: click here.

Programming tasks

The company *Palindrome* had been using the block cipher DES to encrypt its documents for 12 years since the foundation until its engineers took a decision to use the block cipher Blowfish in addition to DES. It was in 2005 year. So, up to now all its documents are encrypted by DES and then the result is also encrypted by Blowfish. The ciphering is conducted in EBC mode. Both ciphers DES and Blowfish have the same key and block lengths equal to 64 bits. The descriptions of these ciphers can be found here: DES and Blowfish.

As a result of infor
company, the text of a

Dear colleagues
of success and we

And the ciphertex

$C =$ 83c100497
23034db7b4408629 4df36ca87ad39f4a 99277e6f1e217dfd
f2eab13d1161e849 0fe72e9b98fc1e8a 0aa5680e3b4022cb
4e44c8745afae37f bd5d6d49292bd1b2 9386f2f383061bfd
ae8fca32e6745687 565d353f3bbb1204 aa79742f7ab55fb1
123e6cf37fbad6fe

$n =$ 40763613025504836845249840044831561583564626405535158138667037
18791672670905308860844304055285019651507728831663677166092475
16155419756121537288444995708421977847213953345126368990185271
10259760189356588305406519080647582874212687596214191915933827
67252094717222418132289251314647500491996323400002019,

Could you decrypt the following ciphertext that was intercepted in the company network 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 key is changed dynamically every day according to certain rules and it is always a sequence of 128 bits where each of 16 bytes is given by ASCII codes of figures from 0 to 9. The first 64 bits form a DES key and the other 64 bits form a Blowfish key.

The FNV2 hash function is derived from the function FNV-1a. FNV2 processes a message x composed of bytes $x_1, x_2, \ldots, x_n \in \{0, 1, \ldots, 255\}$ in the following way:

1) $h \leftarrow h_0$;

2) for $i = 1, 2, \ldots, n$: $h \leftarrow (h + x_i)g \bmod 2^{128}$;

3) return h.

$\ldots 62632977698155964956296670623676 29, \; g = 2^{88} + 315.$

… that is, two different messages x and x' such that FNV2(x) = … on short messages and collisions that are obtained without intensive … comed. Supply your answer as a pair of two hexadecimal strings … of colliding messages.

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

1. it generates the binary sequence $u_0, u_1, u_2, \ldots$, where $u_i \in \mathbb{F}_2 = \{0, 1\}$, such that for some secret $c_0, \ldots, c_{15} \in \mathbb{F}_2$ it holds

$$u_{i+16} = c_{15}u_{i+15} \oplus c_{14}u_{i+14} \oplus \ldots \oplus c_0 u_i \text{ for all integer } i \geqslant 0;$$

2. i-th random number r_i, $i \geqslant 1$, is calculated as

$$r_i = u_{16i} + u_{16i+1}2 + u_{16i+2}2^2 + \ldots + u_{16i+15}2^{15};$$

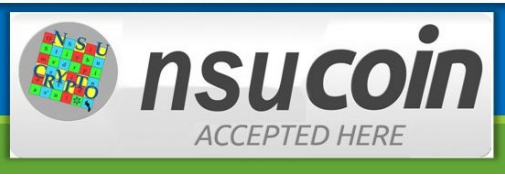
3. Bob initializes $u_0, u_1, \ldots, u_{15}$ using some integer number IV (initial value), where $0 < IV < 2^{16}$, by the same way, i. e.

$$IV = u_0 + u_1 2 + u_2 2^2 + \ldots + u_{15}2^{15};$$

4. it is known that as IV Bob uses the number of seconds from January 1, 1970, 00:00 (in his time zone) to his current time (in his time zone too) modulo 2^{16}.

Eva has intercepted the third and the fourth random numbers ($r_3 = 9\,731$ and $r_4 = 57\,586$). She lives in Novosibirsk and knows that Bob has initialized the generator at 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 Eva to detect Bob's time zone.



nsucrypto.nsu.ru

Международная олимпиада NSUCRYPTO

- Разнообразные задачи

Mathematical tasks

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

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

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

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

- How many solutions may the equation

$$F(x + a) = F(x) + b \quad (1)$$

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

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

Please, help to Alice!

Bob is very interested in blockchain technology, so he decided to create his own system. He started with the construction of a hash function. His first idea for a hash function was the function H with a hash value of length 16.

It works as follows.

- Let $u_1, u_2, \ldots, u_n \in \mathbb{F}_2$ be a data representation, n is arbitrary.
- Bob calculates $z^0, \ldots, z^n \in \mathbb{F}_2^{32}$, $z^0 = (0, \ldots, 0)$, and z^{i+1} is obtained from z^i in the following way:

$$z' = \begin{cases} (z^i_1, z^i_2, \ldots, z^i_{16}, z^i_1 \oplus z^i_{17}, z^i_2 \oplus z^i_{18}, \ldots, z^i_{16} \oplus z^i_{32}) & \text{if } u_i = 1, \\ (z^i_1 \oplus z^i_{17}, z^i_2 \oplus z^i_{18}, \ldots, z^i_{16} \oplus z^i_{32}, z^i_{17}, z^i_{18}, \ldots, z^i_{32}) & \text{if } u_i = 0. \end{cases}$$

$$z'' = \begin{cases} z' & \text{if } u_i \neq z'_{32}, \\ (z'_1 \oplus 1, z'_2 \oplus 1, \ldots, z'_{32} \oplus 1) & \text{if } u_i = z'_{32}, \end{cases}$$

$$z^{i+1} = (z''_2, z''_3, \ldots, z''_{32}, u_i).$$

- Finally, $H(u_1, \ldots, u_n) = (z^n_1 \oplus z^n_{17}, z^n_2 \oplus z^n_{18}, \ldots, z^n_{16} \oplus z^n_{32})$.

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

Q1 Let

$$\Lambda(g) = \{\alpha_i \oplus \alpha'_i :\ i = 1, \ldots, d\}, \qquad \widehat{\Lambda}(g) = [\alpha_i \oplus \alpha'_i :\ i = 1, \ldots, d],$$
$$\mathrm{B}(g) = \{x \oplus y :\ \{x, y\} \subseteq \mathrm{FixP}(g),\ x \neq y\}, \quad \widehat{\mathrm{B}}(g) = [x \oplus y :\ \{x, y\} \subseteq \mathrm{FixP}(g),\ x \neq y],$$

where $\mathrm{FixP}(g)$ is the set of all **fixed points** of g, i.e. $\mathrm{FixP}(g) = \{x \in \mathbb{F}_2^n :\ g(x) = x\}$.

Suppose that g is an APN permutation. Get necessary conditions for multisets $\widehat{\Lambda}(g)$, $\widehat{\mathrm{B}}(g)$ and sets $\Lambda(g)$, $\mathrm{B}(g)$. Prove that if your conditions are not satisfied, then g is not an APN permutation.

Q2 Let

$$\mathrm{d}_{a,b}(g) = |\{x \in \mathbb{F}_2^n :\ g(x \oplus a) \oplus g(x) = b\}|, \quad a, b \in \mathbb{F}_2^n.$$

Let g be an involution and APN. Find $\mathrm{d}_{a,a}(g)$ for each nonzero $a \in \mathbb{F}_2^n$.

Q3 Can you get the nontrivial upper bound on $|\mathrm{FixP}(g)|$?

Bob decided to improve the famous Miller — Rabin primality test. The odd number n being tested is represented in the form $n - 1 = 2^k 3^\ell m$, where m is not divisible by 2 or 3.

The modified primality test is the following:

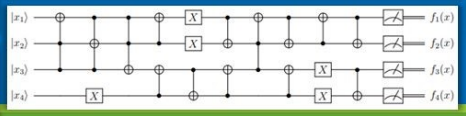
1. Take a random $a \in \{2, \ldots, n-2\}$.
2. Put $a \leftarrow a^m \bmod n$. If $a = 1$, return "`PROBABLY PRIME`".
3. For $i = 0, 1, \ldots, \ell - 1$ do the following steps:
   (a) $b \leftarrow a^2 \bmod n$;
   (b) if $a + b + 1$ is divisible by n, return "`PROBABLY PRIME`";
   (c) $a \leftarrow ab \bmod n$.
4. For $i = 0, 1, \ldots, k - 1$ repeat:
   (a) if $a + 1$ is divisible by n, return "`PROBABLY PRIME`";
   (b) $a \leftarrow a^2 \bmod n$.
5. Return "`COMPOSITE`".

Q1 Prove that this algorithm does not fail, that is, not return "`COMPOSITE`", for a prime n.

```
c = 0000 aaaa 0000 bbbb
    0000 cccc 0000 dddd
bX = dbb1 f04f 2d5a 42e1
     a554 4916 51af a669
bY = 13ae d689 294a a168
     bbf3 57a2 522b 3be9
```

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, that is, find g^{xy} from (g, g^x, g^y). Suggest a solution with the minimal requests to the machine.



nsucrypto.nsu.ru

Unsolved problems

Year	Problem title	Status	Year	Problem title	Status
2014	Watermarking cipher	Unsolved	2019	Sharing	Unsolved
2014	APN permutation	Unsolved	2019	Curl27	Partially SOLVED during the Olympiad
2014	Super S-box	Unsolved	2019	8-bit S-box	Unsolved
2015	A secret sharing	Partially SOLVED in [1,2]	2019	APN + Involutions	Unsolved
2015	Hypothesis	Unsolved	2019	Conjecture	Unsolved
2016	Algebraic immunity	SOLVED during the Olympiad	2020	JPEG Encoding	Unsolved
2016	Big Fermat numbers	Unsolved	2020	Miller — Rabin revisited	SOLVED during the Olympiad
2017	The image set	Unsolved	2020	Bases	Partially SOLVED during the Olympiad
2017	Boolean hidden shift problem	Unsolved	2020	AES-GCM	Unsolved
2017	Useful Proof-of-work for blockchains	Unsolved	2021	Let's find permutations!	Unsolved
2018	Orthogonal arrays	SOLVED in [3]	2021	s-Boolean sharing	Partially SOLVED during the Olympiad
2018	Sylvester matrices	SOLVED during the Olympiad	2021	Quantum error correction	Partially SOLVED during the Olympiad
2018	Disjunct Matrices	Unsolved	2021	Distance to affine functions	Unsolved

1) Geut K., Kirienko K., Sadkov P., Taskin R., Titov S. On explicit constructions for solving the problem 'A secret sharing'. ПДМ, 2017, 10, 68–70.
2) S.M. Ayat, M. Ghahramani, A recursive algorithm for solving «A secret sharing» problem, Cryptologia, 43:6 (2019), 497–503.
3) Kiss R., Nagy G. P. On the nonexistence of certain orthogonal arrays of strength four. ПДМ, 2021, 52, 65–68.

nsucrypto.nsu.ru/unsolved-problems/

Трудности, мысли, шаги

- **Академическая наука.** Непонимание актуальности криптографических результатов, в связи с чем есть трудности с проведением фундаментальных исследований. Отсутствие представителей «от криптографии» в научных комиссиях, советах, экспертных группах. Математики отсылают к ИТ-отрасли. Специалисты от ИТ результатов не понимают.
- **Криптографическое сообщество мало скоординировано**. Нет общего новостного портала, где могла бы свободно появляться информация о событиях в криптографии в России. Конференции, школы, магистерские программы, программы повышения квалификации, конкурсы, олимпиады, книги, журналы, популярные статьи. Имеет смысл перенять опыт IACR – международной ассоциации криптографических исследований.
- **Криптография в Сибири.** Наблюдается интерес к получению кадров из Сибири, к их переезду в Москву, Санкт-Петербург. В меньшей степени – к развитию направления на нашей территории. Мы пытаемся это делать.

Благодарю за внимание!

Наталья Токарева
Криптографический центр (Новосибирск)
Лаборатория криптографии НГУ
www.crypto.nsu.ru
crypto1127@mail.ru