

Master in Cryptography

Novosibirsk State University
Department of Mechanics and Mathematics



We welcome you to the first Master's degree programme
«**Master in Cryptography**»
in Russia!

You have the unique opportunity to study the state-of-art of
cryptography and cryptanalysis at **Novosibirsk State University**
that is located in the world-famous scientific center
in the heart of Siberia — **Akademgorodok**.

Do not miss the chance

- to get a high-level education,
- to listen to world-renowned professionals in the field of cryptography, information theory and discrete mathematics,
- to immerse yourself in the amazing atmosphere of Akademgorodok, where the real science and wonderful nature are so close to each other!

www.crypto-master.nsu.ru



Master in Cryptography

Novosibirsk State University

Department of Mechanics and Mathematics

About NSU

Novosibirsk State University was founded in 1959. It was intended to be an integral part of **Akademgorodok**, the scientific center whose history began not much earlier.

NSU provides modern, internationally competitive, classical fundamental education. We pay special attention to the comprehensive development of each student.

NSU in figures...

7000 students	85 programmes & courses	3 institutes and 6 departments
880 associate professors	570 full professors with doctorate degrees	2000 university teachers
1000 international students from 40 countries	43 international university teachers from 12 countries	73 members of the Russian Academy of Sciences
		12 English-taught programmes

«I am sure, if you enroll at Novosibirsk State University, you will never regret your choice.»



Mikhail Fedoruk

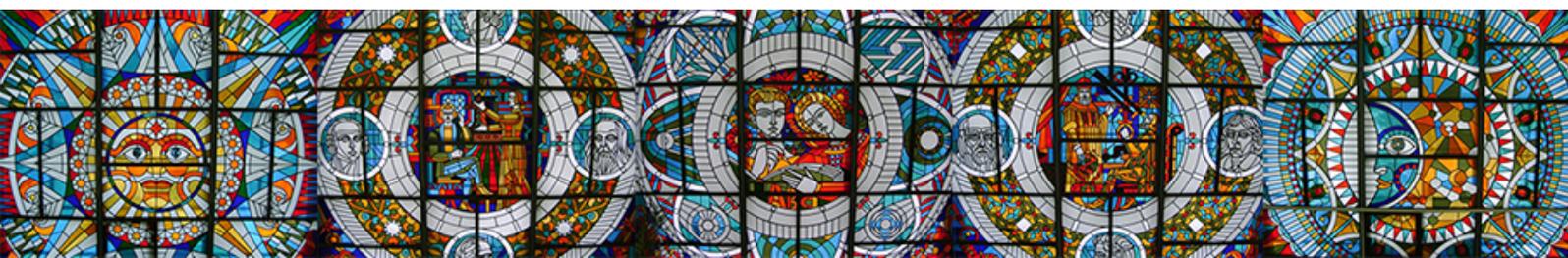
Rector of NSU.

Corresponding member of the Russian Academy of Sciences, Doctor of Sciences in Physics and Mathematics, Full Professor.

NSU Education will teach you how to think **more broadly**, to find **creative solutions** and to achieve **success in any field**.

www.nsu.ru

Read more at english.nsu.ru/about_NSU



About DMM at NSU

The Department of Mathematics and Mechanics (DMM) was founded in 1961. It is the largest department at NSU. Every year, 215 first-year students begin their study.

«We will always need people who are able to design complex mathematical models, to carefully analyze their properties and to invent algorithmic methods to work with them. Such people are called mathematicians.»

Igor Marchuk

Dean of the Department.

Doctor of Sciences in Physics and Mathematics, Full Professor.

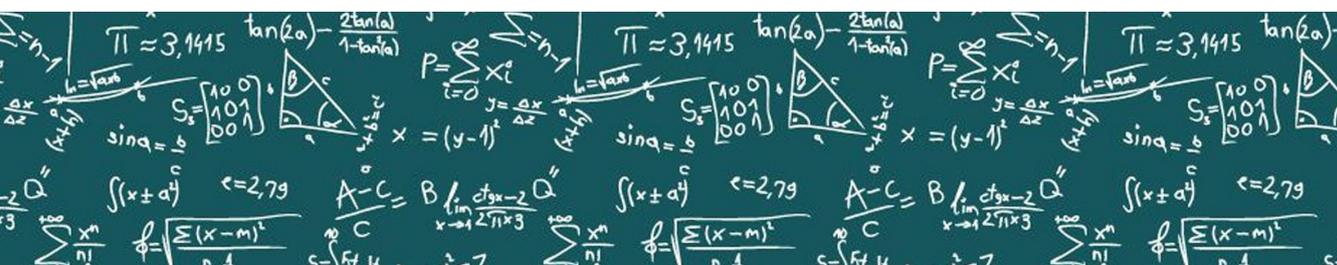


Education at NSU DMM offers a wide range of possible professional careers. A career in science is the most evident and relevant result after completing one's studies. Many graduates choose such career path and achieve considerable success occupying leading positions in research centers and universities all over the world.

There are several scientific institutes of the Siberian Branch of the Russian Academy of Sciences that actively participate in training of highly qualified scientific personnel in cooperation with NSU DMM. They are the following:

- Sobolev Institute of Mathematics of SB RAS,
- Institute of Computational Mathematics and Mathematical Geophysics of SB RAS,
- Institute of Computational Technologies of SB RAS,
- Lavrentyev Institute of Hydrodynamics of SB RAS,
- A. P. Ershov Institute of Informatics Systems of SB RAS,
- Khristianovich Institute of Theoretical and Applied Mechanics of SB RAS.

www.mmf.nsu.ru



A photograph of a winter forest. The trees are heavily covered in snow, and the ground is also blanketed in white. In the foreground, a road with a metal guardrail is visible, leading into the woods. The sky is a pale, overcast blue.

**WOH EAR ARYDE
OT MOBECE A
RESMAT NI CPOTRY ?**

Let's start!

Master in Cryptography from NSU is an innovative programme designed to involve young researchers in the field of modern cryptography and bring them onto a high professional level in this area.

The programme covers all basic aspects of cryptography and cryptanalysis and provides deep theoretical and practical background in this field.

Professionals in cryptography will be invited to deliver lectures.

PhD. Note that there is a possibility to continue your study in post-graduate course and to defend PhD thesis in mathematical problems of cryptography at NSU.

«It is my pleasure to invite you to the first in our country English-taught Master programme in Cryptography! Having no doubt it will be an important event in cryptographic life of Russia. Great specialists in cryptography and discrete mathematics from different parts of the world are ready to come to Novosibirsk and provide training for you. Studying with us you can combine lectures with scientific and practical work in cryptography even if earlier you had not such experience. Moreover, we guarantee impressive cultural and sport events, excursions and friendly atmosphere during the whole period of your studies. Join us!»

Natalia Tokareva

Chief of the Programme, PhD, senior researcher at Sobolev Institute of Mathematics, associate professor at Novosibirsk State University and of NSU Specialized Educational Scientific Center.



Research interests are: symmetric cryptography, Boolean functions and discrete mathematics. Natalia Tokareva is an author of several monographs and tutorials in cryptography, a supervisor for MS & PhD students, a general chair of the International Students' Olympiad in Cryptography NSUCRYPTO.

Master in Cryptography

Novosibirsk State University

Department of Mechanics and Mathematics

Programme itself

The educational programme is well-organized in order for students to get deep knowledge in cryptography and cryptanalysis. All courses are carefully thought out and linked with each other.

Courses included into the programme are the following:

- **Algebra and finite fields: special aspects**

This course covers some basic concepts of algebra and finite fields that have applications in cryptography. You will meet links between finite fields and vector spaces, functions and polynomials over finite fields, recurrent sequences and their characteristics, groups of automorphisms of different objects, special arithmetical algorithms and symbols, mathematical background of primality tests, etc.

- **Discrete mathematics**

The course covers such topics of discrete mathematics as enumerative combinatorics, elements of probability theory, Boolean functions, graph theory. Students will reach a certain level of mathematical maturity becoming familiar with a wide range of mathematical objects that are ubiquitous in computer science; being able to understand relations between them and proof formal statements concerning them.

- **Information theory and cryptography. Introduction**

The course contains chapters devoted to basic notions and concepts in information theory and cryptography. The following topics will be discussed: elements of signal theory, error-correcting codes, data compression, brief overview of main classical results and modern methods of cryptography, introduction into cryptanalysis.

- **Foundations of symmetric cryptography**

This course is devoted to a huge branch of cryptography and contains such chapters as evolution from one-time pad systems to modern encryption methods, general constructions of block and stream ciphers, well-known examples of ciphers, symmetric primitives implementing the principle of confusion and diffusion, key management, open problems and perspectives.

Courses included into the programme are the following:

- **Cryptographic Boolean functions**

It is well known that S-boxes form a very important nonlinear part of a modern symmetric cipher. Resistance of a cipher depends significantly on their properties. Mathematically, S-box is a vectorial Boolean function. In this course we study basic cryptographic properties of Boolean functions in detail. We deal with balanced, non-linear, resilient and algebraically immune functions, bent functions, APN functions and their generalizations. We focus on constructions, classifications, equivalence and open problems.

- **Cipher design**

The aim of the course is to describe fundamental techniques of a cipher construction as well as arising problems, to provide knowledge on performance and security of some known symmetric ciphers such as DES, MAGMA (GOST 28147-89), AES (Rijndael), Serpent, Grain, Trivium, A5, RC, lightweight ciphers Present and Clefia, etc. Some aspects related to hardware implementation of ciphers and hash function design are also observed.

- **Cryptanalysis of symmetric systems**

This course provides deep knowledge on the attacks on block and stream ciphers. Starting with basic ideas as birthday paradox, brute force and meet-in-the-middle attacks, we come to statistical and algebraic methods of cryptanalysis, distinguishing attacks. Side-channel attacks as well as other modern techniques and results in cryptanalysis will be also considered.

- **Asymmetric cryptography and cryptanalysis**

From basic principles of public-key cryptography we turn to the well-known asymmetric schemes (DH key exchange protocol, RSA, ElGamal, McEliece, etc.) and discuss their important theoretical and practical aspects. Factorization and discrete logarithm problems together with special arithmetical algorithms will be considered. Then we focus on digital signatures, elliptic curve cryptography, problems related to complexity of public-key algorithms and open questions. Various attacks on the public-key system will be also reviewed.

Master in Cryptography

Novosibirsk State University

Department of Mechanics and Mathematics

Courses included into the programme are the following:

- **Blockchain: mathematical problems and applications**

The course covers basic concepts of cryptocurrencies, mining mechanisms and Bitcoin protocol in context of anonymity, traceability and security. Blockchain technology is considered as a platform for a broad range of applications; the future of cryptocurrencies and blockchains is discussed.

- **Quantum and postquantum cryptography**

Such aspects are being observed in the course as an introduction to the quantum technologies, necessary mathematical toolbox, pure and mixed quantum states, classical quantum states, quantum key distribution protocols (BB84, B92, etc.) and attacks on them, quantum hashing, principles of postquantum cryptography.

- **Practical applications of cryptography**

The course gives a detailed overview of modern cryptography real-world applications such as secure network communications, encryption devices, authentication methods, key-exchange techniques, voting and cryptocurrencies, mobile phone security, RFID technology, smart cards and payment systems. Approaches related to biometric encryption are considered, for example, those based on iris and voice recognition.

- **Historical and legal aspects of cryptography**

The main goal of this course is to provide a broad overview of history and development of cryptology, its long (and may be infinite?) way from art to science. A number of different ciphers and techniques that were used all over the world before the World War II and after it, first methods of cryptanalysis, cipher machines and key persons in cryptography will be considered. We observe some legal aspects of cryptography, standardization process, regulation of cryptographic applications and many other important details.

Language courses (Russian or Advanced English) will also be included.

September 2018 — June 2020

Invited lecturers

Bart Preneel

Full professor in the research group COSIC of the Electrical Engineering Department of the University of Leuven (Belgium).
Director of the International Association for Cryptologic Research.



Main interests are: cryptography and information security. His research focuses on cryptographic algorithms and protocols as well as their applications to computer and network security and mobile communications.

Bart Preneel is a world-known leader in cryptography. With colleagues he created several ciphers and hash functions (MUGI, Trivium, RIPEMD-160, etc.) and contributed to the cryptanalysis of many known cryptographic systems. He is one of the leaders of COSIC, a very successful cryptographic group. Note that the cipher AES, the modern standard of symmetric encryption in the USA, was invented namely there.

Lars Knudsen

Full Professor at the Department of Applied Mathematics and Computer Science at the Technical University of Denmark.
Member of the Danish Academy of Technical Sciences.



The main interest is cryptology, in particular analysis and design of block ciphers, hash functions, and message authentication codes. He is one of the key specialists in cryptanalysis and cybersecurity in the world.

Block ciphers DEAL and Serpent designed by Lars Knudsen and his colleagues were outstanding candidates for the AES standard. The hash function Grøstl developed by the team of Lars Knudsen was in the final of the SHA-3 standard competition. Professor Knudsen introduced the technique of impossible differential cryptanalysis and so-called integral cryptanalysis.

Master in Cryptography

Novosibirsk State University

Department of Mechanics and Mathematics

Invited lecturers



Lilya Budaghyan

Dr. habil., Researcher at Reliable Communication Group at the Department of Informatics in University of Bergen (Norway).

Research interests are: symmetric cryptography, Boolean functions, discrete mathematics, algebra, finite fields, and mathematical logic.

Lilya Budaghyan is a well-known specialist in cryptographic vectorial Boolean functions over the finite fields. She obtained great results in their classification as well as studying their properties. Professor Budaghyan is an excellent supervisor for many students of hers interested in complicated algebraic problems of S-box design.



Stjepan Picek

PhD, Assistant professor at Delft University of Technology (The Netherlands), Researcher at Massachusetts Institute of Technology (USA).

Main research interests are at the intersection of cryptography, cybersecurity, evolutionary computation, and machine learning.

Evolutionary computation is a research area within computer science that draws inspiration from the process of natural evolution. These principles can be applied in obtaining cryptographic Boolean functions, S-boxes with desired properties, pseudo-random generators. Stjepan Picek is a highly-qualified young specialist in this area.

Invited lecturers

Sugata Gangopadhyay

Associate professor at the Department of Computer Science and Engineering of Indian Institute of Technology Roorkee (India).



Research interests are: algebra and information theory, mainly in cryptographic Boolean functions and stream cipher cryptanalysis.

Sugata Gangopadhyay contributed a lot to the area of cryptographic Boolean functions. He is a participant and coordinator of many successful international projects in cryptography and information security that he is combining with creative scientific work together with young researchers.

Nicky Mouha

PhD, Researcher at the Computer Security Division of the Information Technology Laboratory at NIST (USA), Associate Member at the CASCADE team of ENS (France).



Research interests are: lightweight cryptography, hash functions, automated techniques for cryptanalysis of block ciphers.

Nicky Mouha is a young but well-known specialist in cryptanalysis and design of hash functions, symmetric-key ciphers and protocols. He is a co-author of the MAC algorithm Chaskey and the family of lightweight permutation-based authenticated encryption schemes PRIMATEs. At National Institute of Standards and Technologies (NIST), he works on the standardization of lightweight cryptography.

Master in Cryptography

Novosibirsk State University

Department of Mechanics and Mathematics

Invited lecturers



Evgeny Gorkunov

PhD, Senior researcher at Sobolev Institute of Mathematics, assistant professor at NSU Department of Information Technologies.

Main scientific interests are in the field of the intersection of combinatorics, graph theory, algebra, and algorithmic information processing.

Evgeny Gorkunov has been teaching courses in discrete mathematics and coding theory for almost ten years. He is a well qualified and talented lecturer. Completing his courses, students successfully find jobs in IT, industry, engineering, education and science.



Anastasiya Gorodilova

PhD, Researcher at Sobolev Institute of Mathematics, assistant professor at Novosibirsk State University and NSU Specialized Educational Scientific Center.

Main research interests are: Boolean functions for cryptography, APN functions, cryptography, combinatorics, algebra.

Anastasiya Gorodilova is an effective supervisor for school and university students in coaching them to the cryptographic olympiads. A qualified specialist in symmetric cryptography, she is a co-author of the monograph «Cryptography and cryptanalysis: mathematical problems».

Invited lecturers

Nikolay Kolomeec

PhD, Researcher at Sobolev Institute of Mathematics, assistant at Novosibirsk State University.



Research areas are pseudorandom sequences, cryptographic Boolean functions, bent functions, and discrete mathematics.

Nikolay Kolomeec is experienced in teaching as well as in programming, especially one linked with research problems. He has completed training at the International Course on Cyber Security and Cryptography in the research group COSIC at University of Leuven.

Valeriya Idrisova

Researcher at Sobolev Institute of Mathematics, assistant at Novosibirsk State University.



Main interests are: Boolean functions for cryptography, APN functions, block ciphers, side-channel attacks.

Being a visitor to University of Leuven, Valeriya Idrisova did a joint research with COSIC in the area of countermeasures against side-channel attacks. She is a young and perspective specialist in cryptographic properties of Boolean functions.

Master in Cryptography

Novosibirsk State University

Department of Mechanics and Mathematics

Invited lecturers



Alexey Oblaukhov

Researcher at Novosibirsk State University, lecturer at Novosibirsk State University and NSU Specialized Educational Scientific Center.

Research interests are blockchain technologies, cryptography, and discrete mathematics.

Every year, being a student, Alexey Oblaukhov got prizes on international olympiads in mathematics and cryptography. Thus, in 2016 he received the First Prize at the International Mathematics Competition for University Students that is the most reputable event for this kind for young mathematicians. Now he trains school and university students for various competitions in mathematics.



Alexander Kutsenko

Researcher at Novosibirsk State University, lecturer at Novosibirsk State University.

Work interests are: in mathematical problems of quantum cryptography and cryptographic Boolean functions.

Alexander Kutsenko obtained interesting results on properties of isometric mappings of the set of bent functions. He is a perspective young teacher; at present he teaches the course on quantum cryptography at NSU Department of Mathematics and Mechanics.

How to apply

Take the following easy steps. Just start!

- 1** Prepare a short Curriculum Vitae (CV) about yourself with a photo, place you are from, information about university degree/s, work experience if you have any, your interests and personal achievements.
- 2** Send your CV to crypto-master@nsu.ru and mention that you want to apply for «Master in Cryptography».
- 3** We contact you and ask for standard entrance requirements, including:
 - Copy of the Passport (all pages);
 - Copy with apostil of education certificate;
 - Academic transcripts (transcript of record, university degree/s, diploma supplements);
 - 2 photos;
 - English language course marks sheet/TOEFL certificate or other international certificates (BEC etc.);
 - Curriculum Vitae;
 - Motivation Letter (1-2 pages);
 - Copy of medical certificate of overall health condition;
 - Copies of HIV + AIDS certificates.

Then we will work with you on going through your application process!

Deadlines:

- Till **15 June 2018** send your CV and express an intention to study.
- Till **31 July 2018** provide a full set of scanned documents.

Scholarships. Every year foreign students have an opportunity to apply for the Russian Government Scholarship programme.

Our address: 1, Pirogova str., Novosibirsk, 630090, Russia.

For all questions, please, do not hesitate to contact crypto-master@nsu.ru

For more details and actual information www.crypto-master.nsu.ru

Master in Cryptography

Novosibirsk State University
Department of Mechanics and Mathematics

Important details

Tuition fees is U.S. \$ 5 200 per year.

Students live in new comfortable dormitories located in a couple-of-minutes walk from NSU. Each single room is equipped with a desk, a bed, a wardrobe, a private bathroom. Students are given the opportunity to run at the stadium, swim in the 25-meter swimming pool, play tennis and other sports games, ski along a forest path as well as many other activities.

Tuition fees does not include cost of living which does not exceed \$ 20 per month.



Dormitory, room, hall, common kitchen.



«NSU campus is a stunning place for an active lifestyle!»

You can find a detailed map of NSU campus and its surroundings with dormitories, science, food, sport, beach, squirrels and many other things at english.nsu.ru/life/campus.



Timetable

Duration: two academic years, full-time study, **September 2018 — June 2020.**

Language of instruction: English.

Programme includes elements of a **modular system**. It means that an invited lecturer presents an intensive course for a limited period of time.

Timetable:

Semester I (September 2018 — December 2018): Lectures, exams

Semester II (March 2019 — June 2019): Lectures, exams, scientific work

Semester III (September 2019 — December 2019): Lectures, exams, scientific work

Semester IV (March 2020 — June 2020): Lectures, exams, diploma defense

Winter holidays:

January 2019 — February 2019

January 2020 — February 2020

Summer holidays:

July 2019 — August 2019

July 2020 — August 2020

During holidays there is a possibility to conduct scientific research in cryptography at Novosibirsk State University and Sobolev Institute of Mathematics.



Master in Cryptography

Novosibirsk State University

Department of Mechanics and Mathematics

Studying in NSU provides you with...



- **A high-level education.** Without any doubt NSU is one of the leading universities in Russia. See for yourself english.nsu.ru/about_NSU/rankings.

- **Opportunities for scientific research.** 80% of NSU faculty members are scientists from the Siberian Branch of the Russian Academy of Sciences. So education is carried out in close connection with the world-class scientific achievements.



- **Perspectives.** NSU history is the history of thousands of graduates who have fulfilled themselves in science, business and creative arts.

Anyone can find something to enjoy in Novosibirsk: winter snow or summer on the beach, the rhythm of the modern metropolis or the grandeur of vast forests and fields,...



Studying in NSU provides you with...

- **Modern and compact campus.** Everything is within walking distance: the dormitories, a sports center, a stadium, 35 scientific institutes, and an innovative technopark are within a 10-minute walk from campus.



- **Unique atmosphere and nature of Akademgorodok** — the world-famous scientific center located in the beautiful forest near the Ob sea.

- **Cultural benefits** such as visiting the Opera and Ballet Theatre, the largest theatre in Russia with world-famous artists.



...the permanence of traditional cultures or the best of science in Russia. And, of course, you will definitely feel real Russian hospitality.



Master in Cryptography

Novosibirsk State University

Department of Mechanics and Mathematics



You know, we organize the International Students' Olympiad in Cryptography – **NSUCRYPTO**.

Note that a successful participation in the Olympiad will be considered as a significant personal achievement for application to «Master in Cryptography». Welcome!

For more details, please, visit www.nsucrypto.nsu.ru

Useful links about NSU and Akademgorodok:

- [Why NSU?](#)
- [Interesting facts!](#)
- [Video: «Novosibirsk State University. Science. Community. Life»](#)
- [And more videos on «NSU Life» channel.](#)

*All links are available in electronic version of the booklet on the website at

www.crypto-master.nsu.ru





