MATHMATICAL SCIENCES, MASTER STUDY PROGRAMME

COURSE DESCRIPTIONS

Course name: **SELECTED TOPICS IN ANALYSIS I**

Number of ECTS credits: 9 / 6

Content:

Lectures are given on the most current research topics in the areas of analysis, among others, may include the following topics

- Fourier analysis
- Analysis on manifolds
- Vector analysis. Gauss' and Stokes' theorem.

Course name: **CODING THEORY**

Number of ECTS credits: 9 / 6

Content:

The course covers the most important topics in coding theory, that includes (among others) the topics below:

- mathematical basics (groups, rings, ideals, vector spaces, finite fields)
- basic concepts in coding theory
- algebraic methods for construction of error-correcting codes
- Hamming codes
- Linear codes
- Binary Golay codes
- Cyclic codes
- BCH codes
- Reed-Solomon codes
- Bounds (Hamming, Singleton, Johnsson bound, ...)

Course name: **HISTORY AND METHODOLOGY OF THE SUBJECT**

Number of ECTS credits: 3

Content:

1. The subject of history and methodology of mathematics and the methods used in it.

- the problem of communication of mathematical knowledge, means of communications (stone engravings, letters, books, papers, blogs, recorded lectures, etc.), problems - solutions. Open problems, conjectures, axioms, definitions, theorems, proofs.
- abstraction, logic, foundation of mathematics
- continuous vs. discrete, two paradigms that drive mathematics.

2. Mathematics in pre-Greek civilizations.

- Egypt, Mesopotamia

3. Mathematics of Ancient Greece.

- Thales, Pythagoras, Euclid’s Elements,Archimedes
- Ptolemey, Heron, Diophantus, Pappus

4. Early mathematics outside Europe

-China
-Japan
-Islam
-India

-South America
5. Mathematics in Europe in the Middle Ages and the Renaissance.
- Translations from Arabic into Latin (12h,13h century), The cubic and quartic equations
- Trigonometry, logarithms
6. Mathematics and scientific and technological revolution of the XVI-XVII centuries.
- Descartes, Bernoulli, Huygens, Fermat, Cavlieri
7. The birth of mathematical analysis.
- Newton, Leibniz
8. Development of mathematical analysis in the XVIII century.
- Euler
9. Algebra of the XVIII century.
- Lagrange, Laplace, Vandermonde
10. Mathematics of the XIX century.
- Gauss, Galois, etc.
11. Mathematics of the XIX—XX centuries.
- Lobachevsky, Chebyshev, Riemann, Hilbert, etc.
- Group theory
- Set theory
12. Mathematics in Eastern Europe, Russia and the USSR.
- Important mathematicians that are often overlooked in Western curricula: Bolyai, Lobachevsky, Chebyshev, Alexandrov, Kolmogorov, etc.
13. Mathematics of the XX century.
- Great problems and their solutions, such as four color problem, Fermat's problem, etc.
- Birth and development of selected fields of mathematics, such as topology, combinatorics, theoretical computer science, etc.
- The rise of discrete paradigm to mach the birth of computer and information science, infomation technology, coding and cryptography, understanding of human genome via DNA, computer, traffic and social networks, and logistics.

Course name: **SELECTED TOPICS IN COMPLEX ANALYSIS**

Number of ECTS credits: 9 / 6

Content:
Lectures are given on the most current research topics in the field of complex analysis, which may include the topics of

- holomorphic, harmonic, subharmonic functions.
- holomorphic functions of several variables

Course name: **THEORY OF FINITE FIELDS**

Number of ECTS credits: 9 / 6

Content:
Lectures are given on the most current research topics in the field of finite fields, which may include the topics of

- Structure of Finite Fields
- Polynomials over Finite Fields
- Polynomial Factorization
- Equations over Finite Fields
- Finite Fields and their Applications

Course name: SELECTED TOPICS IN THEORY OF FINITE GEOMETRIES

Number of ECTS credits: 9 / 6

Content:

Actual research topics are presented from the field of algebra which among others include the following areas:

- affine planes
- projectivne planes
- Desargues and Pappus theorem
- collineations and correlations
- curves of degree 2 and conics
- near linear spaces
- linear spaces
- affine and projective spaces
- generalized quadrangles

Course name: CRYPTOGRAPHIC HASH FUNCTIONS AND BLOCK CHAINS

Number of ECTS credits: 6

Cryptographic hash functions are useful cryptographic primitive which enables various cryptographic services and protocols to be efficiently implemented. In the first place, they are inevitable part for generating so-called message digest which is a compressed binary image of fixed size for any arbitrary message. A typical application that includes hash functions is generation of digital signature which relates the signed message to the signer. Quite recently, hash functions have received a lot of attention due to their use in block chain technology and in particular for implementing bitcoins.

The purpose of this course is to give rather detailed treatment of both design and security of hash functions. This naturally includes their application so-called MACs (Message authentication Codes) which are essentially keyed hash functions. The recent application of hash functions in block chain technology will be also considered on a popular level.

The content of the course can be summarized as follows:

(A) The main properties of cryptographic hash functions
(B) Generic model for iterated/tree hash functions
(C) Design methods of hash functions and implementation aspects
(D) Security analysis of hash functions and some generic cryptanalytic approaches
(E) Modern design of hash functions and standards
(F) MAC – design and security
(G) Block chain technology with focus on hash functions

(A) The main properties :
- Compression
- Preimage resistance (one-way property)
- 2nd-preimage resistance
- Collision resistance

(B) Generic models:
- Merkle-Damgord sequential approach
- Merkle tree (hash tree) and hash chains, non-sequential approach
- State-of-art approaches

(C) Design methods:
- Hash functions based on block ciphers
- Customized hash functions , MD4, MD5, SHA-XX, current standards

- Hash functions based on modular arithmetic
- Provably secure hash functions based on number theory
- Implementation aspects, speed of processing data

(D) Security analysis:
- Birthday paradox
- Yuval's birthday attack
- Differential cryptanalysis and chaining attacks on hash functions
- Practical analysis of some dedicated hash functions, BLAKE cryptanalysis

(E) Dedicated hash functions - modern design:
- SHA family of hash functions
- State-of-art proposals

(F) MAC-keyed hash functions:
- MAC-s based on block ciphers
- Customized MACs
- Existential and selective forgery
- Data integrity, authentication, different approaches

(G) Block chain technology:
- Basic concepts and functionality
- Hash functions in realm of block chains, Merkle tree as non-sequential hashing
- Security and implementation issues
- Practical examples

Course name: **THEORY OF PERMUTATION GROUPS**
Number of ECTS credits: **9 / 6**

Content:
Actual research topics are presented from the field of algebra which among others include the following areas:
- group actions;
- orbits and stabilizers;
- extensions to multiply transitive groups;
- primitivity and imprimitivity;
- permutation groups and graphs;
- automorphisms of graphs, Cayley graphs;
- graphs with a high degree of symmetry;
- permutation groups and designs.

Course name: **SELECTED TOPICS IN DISCRETE MATHEMATICS I**
Number of ECTS credits: 9 / 6

Content:
The most current research topics in discrete mathematics will be taught, which may include, among others, the following topical subsections:
- Theory of configurations,
- Graph theory,
- Algebraic methods in graph theory

Course name: **SELECTED TOPICS IN ALGEBRA I**

Number of ECTS credits: 9 / 6

Content:
Actual research topics are presented from the field of algebra which among others include the following areas:

- group theory,
- ring theory,
- field theory

Course name: **SELECTED TOPICS IN THEORY OF ASSOCIATION SCHEMES**

Number of ECTS credits: 9 / 6

Content:
The most important research topics in the field of association schemes are taught, which may among others include the following substantive subsections

- Association scheme (basic definitions, Bose-Mesner algebra, Krein's parameters and primitive and imprimitive association schemes, metric and cometric association schemes).
- Distance-regular graphs (basic definitions, distance-regular graphs as metric association schemes, the intersection numbers of, eigenvalues, primitive and imprimitive distance-regular graphs and Q-polynomial distance-regular graphs, a family of classical distance-regular graphs).

Course name: **SELECTED TOPICS IN DYNAMICAL SYSTEMS**

Number of ECTS credits: 6

Content:
Lectures are given on the most current research topics in the field of chaoticaly dynamical systems, which may include the following topics:

- One dimensional dynamical systems (basic definitions, structural stability, Šarkovsky's theorem, bifurcation theory, homocline points, the theory of kneading).
- Multi-dimensional dynamical systems (attractors, Hopf bifurcation, Henon mapping).
- Julia set, Mandelbrot set.

Course name: **SELECTED TOPICS IN TOPOLOGY**

Number of ECTS credits: 9 / 6

Content:
Lectures about the most current research topics in topology, which may include the following content subsections

- manifolds and Riemann manifolds
- Algebraic topology

Course name: **MATHEMATICAL PRACTICUM**

Number of ECTS credits: 9 / 6

Content:
1. Wolfram Mathematica
- elementary calculations, graphs.
- solving standard problems from analysis, linear algebra, differential equations, etc.

- drawing (explicit, implicit, parametric presentation of objects).
- creating interactive and dynamic drawings.
- graphical presentation of NDE and PDE solutions.
- other topics.

2. Matlab
- elementary calculations
- built-in functions
- working with matrices
- writing m functions
- drawing different objects
- solving real problems with Matlab

Course name: **SELECTED TOPICS IN NUMERICAL MATHEMATICS**
Number of ECTS credits: 9 / 6

Content:
Basic actual research topics are considered from several fields of numerical mathematics, such as:

- Approximation of functions.
- Numerical analysis of ordinary differential equations
- Numerical analysis of partial differential equations
- Bezier curves and surfaces

Course name: **SYMMETRY AND TRAVERSABILITY IN GRAPHS**
Number of ECTS credits: 9 / 6

Content:
The most important current research topics in the field of symmetries and transitions on graphs are taught. L.Lovasz (1969) has asked whether every connected vvertex transitive graph admits Hamilonian path. We will introduce this still open problem, connecting seemingly unrelated concept of symmetry and transtition of graphs. Specifically, we will touch the following topics:

- the traveling salesman problem: a historical perspective.
- Hamiltonicity of vertex transitive graphs of specific orders.
- hamiltonicity of Cayley graphs.
- hamiltonicity of cubic graphs
- Lovasz problem: attempt of looking into the future.

Course name: **SELECTED TOPICS IN CRYPTOGRAPHY**
Number of ECTS credits: 9 / 6

Content:
The modern society heavily relies on secure telecommunication and electronic commerce over the Internet. The internet also provides an easy access to various data bases. The smart cards were revolutionary cryptographic primitives with possibility of some moderate computing on a small-sized footprint. Its application area includes e.g. health care, education and is constantly expanding.
Cryptography is a science that offers us practical solutions for security and protection of the information, thus it is regarded as one of the major security mechnisms today (goals: secrecy, message integrity, electronic signatures, digital cash, and other cryptographic protocols; Field:

mathematics, computer science, electrotechnics, finance, politics, military, etc.) The course will cover the following topics:
(A) Symmetric ciphers
(B) Public key cryptography
(C) Digital signatures
(D) Cryptographic protocols
(E) Algorithmic number theory
(F) Hash functions
(G) Algebraic attacks

(A) Symmetric ciphers
- Stream ciphers
- Analysis of some particular ciphers such as RC4
- Generic attacks on block ciphers
- Cryptanalysis of specific block ciphers e.g. AES
- The use of block and stream ciphers
- Pseudo-random number generators
- Cryptanalysis of 3-DES
- Cryptanalysis of DESX-a
- Cryptanalysis of pseudo-random number generators

(B) Public key cryptography
- RSA attacks
- Attacks on ElGammal cryptosystems
- Pseudo-random number generators using discrete algorithms (analysis of linear and quadratic congruence generators and some weeknesses w.r.t to their use in DSA (Digital Signature Algorithm)
- XTR (PKC of Lenstra et al.)
- NTRU a new PKC standard
- LUC (public key cryptosystem without using operation of exponentiation)
- McEliece cryptosystem with Goppa codes

(C) Digital signatures
- Blind signatures
- Group signatures
- One-time signatures

(D) Various cryptographic protocols
- Digital cash
- Anonimity
- Shared security
- Mental poker over the phone
- Resiliant functions
- Kleptography (steling information securely)
- Key escrow (is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys)
- Visual cryptography (and Hadamard matrices)
- Identification schemes

(E) Algorithmic number theory
- Optimal computation in finite fields
- Polynomial basis
- Normal bases (e.g. optamal normal bases or Chebishev basis)
- Transformation of different basis in finite fields GF(pn)
- Integer factorization
- Pollard's rho-method for factorization
- Factorization of polynomials
- Generation of prime numbers

- Probabilistic primality tests (e.g. with elliptic curves)
- Prime factorization is in P ?
- Discrete log problem (DLP)
- Pollard's rho method for DLP
- Floyd's algorithm

(F) Hash functions

- Description and analysis of hash functions HMAC
- Description and analysis of hash functions RIPEMD

(G) Attacks

Methods using the birthday paradox (which is used in cryptanalysis of both symmetric and asymmetric cryptosystems).

Course name: **SELECTED TOPICS IN NUMBER THEORY**

Number of ECTS credits: 9 / 6

Content:

The most current research topics in the field of number theory are taught, which, among others may include the following sections:

- Diophantine equations,
- Algebraic geometry,
- Additive number theory,
- Algebraic number theory