MATHMATICAL SCIENCES, MASTER STUDY PROGRAMME, SECOND BOLOGNA CYCLE

COURSE DESCRIPTIONS

BASIC COURSES

Course name: **SELECTED TOPICS IN ALGEBRA (1)**
Number of ECTS credits: **9**

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 ANALYSIS (1)**
Number of ECTS credits: **9**

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: **SELECTED TOPICS IN DISCRETE MATHEMATICS (1)**
Number of ECTS credits: **9**

Content:
Predavajo se najpomembnejše raziskovalno aktualne teme iz področja diskretne matematike, ki med drugimi lahko vključujejo naslednja vsebinska podpodročja

- Teorija konfiguracij
- Teorija grafov
- Algebraične metode v teoriji grafov,
- Teorija velikih omrežij in analiza,
- Učenje na omrežjih,
- Slučajni sprehodi na grafih,
- Svetovni splet kot graf.

Course name: **SELECTED TOPICS IN FINANCIAL MATHEMATICS (1)**
Number of ECTS credits: **9**

Content:
Mathematics of life insurance.

- Interest, the current value.
- The principle of equivalence.

- Models of survival.
- Determination of net premiums.
- Determination of the net mathematical reserves.
- Risk management in life insurance.

Market models.
- The types of securities.
- Stochastic models of markets.
- The concept of strategy.

Asset management.
- The dimensions of risk.
- The optimal strategy for one period.
- Dynamic strategies.
- CAPM model.

Options.
- The types of options.
- The principle of arbitration.
- The protection and the basic theorem of valuating options.
- European and American options.
- Exotic options.
- Practical aspects of security.

Models of interest rates.
- The importance of stochastic modeling.
- Basic models of current interest rates.
- Options on interest rates.

Course name: **SELECTED TOPICS IN CRYPTOGRAPHY (1)**
Number of ECTS credits: **9**

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 MATHEMATICAL STATISTICS (1)**
Number of ECTS credits: **9**

Content:

The course includes most important research and actual areas in mathematical statistics, which may include the following topics:

Sufficient estimators
- Definition of sufficient estimator.
- Factorization theorem.

Optimality in estimation of parameters
- Unbiased estimators.
- The concept of optimum estimator.
- Cramér-Rao theorem.
- Optimum estimators

Course name: **MOLECULAR MODELING COURSE**
Number of ECTS credits: **9**

Content:
- Basic concepts of molecular modeling
- Introduction to Quantum Mechanics calculation
- Modern ab-initio and DFT quantum methods
- Methods of molecular mechanics
- Potential fields and molecular mechanics
- Computer simulation methods
- Methods for molecular dynamics simulation
- Methods for Monte Carlo simulations
- Using methods of molecular modeling in chemistry, pharmacy, biophysics, in the detection and design of new molecules, etc.

Course name: **SELECTED TOPICS IN FUNCTIONAL ANALYSIS**
Number of ECTS credits: **9**

Content:
Lectures are given on the most current research topics in the areas of analysis. They may include among others, the following contents
- The topological vector spaces. Generalized sequences.
- Weak * compactness.
- Operators on Banach and Hilbert space.
- Banach algebra, C * algebras and von Neumann algebras.

ELECTIVE COURSES

Course name: **ALGEBRAIC COMBINATORICS**
Number of ECTS credits: **9**

Content:
Current research topics are presented from the field of algebra which among others maz include the following areas:
- spectral graph theory;
- automorphism groups of graphs;
- symmetries of graphs;
- graphs with transitive automorphism groups (vertex-transitive, edge-transitive, arc-transitive and distance-transitive graphs).
- strongly regular graphs via algebraic methods.

Course name: **ELLIPTIC CURVES IN CRYPTOGRAPHY**
Number of ECTS credits: **9**

Content:
The aim of this course is to introduce the theory of elliptic curves for practical applications in public key cryptosystems. Firstly, the standard discrete log problem is discussed and other discrete structures for implementing public key cryptography are elaborated. We will consider elliptic curves over the prime fields of characteristic 2 (binary prime fields), which gives a rise to an efficient hardware implementation; but also elliptic curves over the prime fields of odd characteristic will be considered. The following topics will be covered in details.

- Practical cryptography
- The use of finite fields
- Polynomial factorization over finite fields
- Recursive and efficient constructions of irreducible polynomials
- Irreducibility of compositional polynomials
- Normal basis and distribution of normal elements
- Algortihms for the construction of normal elements
- Optimal normal basis, introduction to construction
- Discrete log problem
- Elliptic curves over finite fields
- Cryptosystems using elliptic curves
- Discrete log problem on elliptic curves and supersingular curves
- Number of points on elliptic curves

Course name: **HEALTHCARE FINANCING**
Number of ECTS credits: **9**

Content:
Health.

- definition of the term;
- indicators of the health of the population.

Public and private.

- sources of financing health care;
- role of the coexistence of public and private health care funding.

Health care systems.

- Bismarck's system of compulsory health insurance;
- Beveridge's national health care system;
- commercial health insurance system;
- Classification of health insurances.

Public compulsory health insurance.

- historical data on development;
- Nature of the compulsory health insurance;
- Issues and trends.

Private health insurance.

- insurance activity;
- Risk factors and determination of the premium;
- Issues and trends.

Case studies.

- increase expenditure on health care and control of growth;
- private health insurance offer;
- absence from work due to illness or injury;
- financing of health insurance and longevity;
- other actual themes.

Course name: **GROUPS, COVERS AND MAPS**
Number of ECTS credits: **9**

Content:

- Group action (homomorphisms and auto- morphisms of actions, invariant groups of an action).
- Covers, lift of automorphisms and group extension (covering projection, reconstruction via voltage group, regular covering projection, lift and projection of automorphisms, necessary and sufficient conditions for lifting with the help of the voltage group, lift of automorphisms in regular abelian covers, examples for cyclic and $(\ZZ_p \times \ZZ_p)$-covers, group extension and the structure of the lifted group, geo-metrical split extensions.
- Action graphs (homomorphism of actions and covering projections of action graphs).
- Maps (concept of a map on a compact surface, algebraic maps, triangular groups and cristallo-graphic groups of orientable algebraic maps, representation with the action graph and Schre-ier representation, homomorphisms and auto-morphisms of oriantable algebraic maps, topo-logical interpretation, regular homomorphisms, Riemann-Hurwitz formula and its applications, lift and projection of automorphisms).
- Maps with a high degree of symmetry (regular orientable maps, constructions, classification problem, orientable Cayley maps, necessary and sufficient conditions for regularity, group of automorphisms as rotation product, genus of a group, Hurwitz theorem, groups of small genus).

Course name: **SELECTED TOPICS IN ALGEBRA (2)**
Number of ECTS credits: **9**

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

- Representations
- Non-associative algebras
- Group action
- Group rings
- Schur rings

Course name: **SELECTED TOPICS IN DIFERENTIAL EQUATIONS**
Number of ECTS credits: **9**

Content:
Lectures are given on the most current research topics in the areas of analysis. They may include among others, the following contents

- Differential equations.
- Partial differential equations
- Distributions
- Calculus of variations.

Course name: **SELECTED TOPICS IN THEORY OF ASSOCIATION SCHEMES**
Number of ECTS credits: **9**

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 DISCRETE MATHEMATICS (2)**
Number of ECTS credits: **9**

Content:
The most current research topics in discrete mathematics will be taught, which may include, among others, the following topical subsections:
- Design theory
- Discrete methods in geometry
- Algebraic methods in discrete mathematics

Course name: **SELECTED TOPICS IN COMPLEX ANALYSIS**
Number of ECTS credits: **9**

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: **SELECTED TOPICS IN MATHEMATICAL STATISTICS (2)**
Number of ECTS credits: **9**

Content:
At the lectures the students will learn the most current research topics in the field of mathematical statistics, which may the following subfields:

Optimality theory in testing hypotheses
- Neyman-Person's lemma.
- Uniformly most powerful tests.

Asymptotic properties of estimators
- Consistent estimators.
- Asymptotic normality of the MLE estimators.

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

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
- Numerical methods for large linear systems and
  Numerical methods for large eigenvalue problems.

- Large scale numerical optimization
- Bezier curves and surfaces

Course name: **SELECTED TOPICS IN THEORY OF FINITE GEOMETRIES**
Number of ECTS credits: **9**

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: **SELECTED TOPICS IN NUMBER THEORY**
Number of ECTS credits: **9**

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

Course name: **SELECTED TOPICS IN TOPOLOGY**
Number of ECTS credits: **9**

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: **SELECTED TOPICS IN COMPUTING METHODS AND APPLICATIONS**
Number of ECTS credits: **9**

Content:

- Hamiltonian Systems
- Numerical Integration Methods and Algorithms
- Lie Formalism
- Symplectic Integration Methods
- Numerical Experiments

Course name: **CHAOTIC DYNAMICAL SYSTEMS**
Number of ECTS credits: **9**

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: **CHARACTERS OF FINITE GROUPS**
Number of ECTS credits: **9**

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

- algebras, modules and representations;
- group characters;
- tensor product;
- induced characters;
- Frobenius and Burnside theorem.

Course name: **COMBINED QUANTUM AND CLASSICAL METHODS FOR MOLECULAR SIMULATIONS**
Number of ECTS credits: **9**

Content:

- Basics of quantum mechanics
- Ab-initio quantum-chemical methods
- Density Functional Theory
- Kohn-Sham theory
- atoms and molecules
- Basics of Classical Mechanics
- The theory of the potential fields
- Methods for the QM / MM simulations
- Application of methods for the combined quantum-classical simulations

Course name: **MATHEMATICAL MODELLING**
Number of ECTS credits: **9**

Content:
Lectures are given on the most current research topics in the field of mathematical modeling, which may include the following topics:

- Optimization (Minimum, Maximum and Saddle Points. Taylor Formula for Scalar Fields. Types of Stationary Points. Constrained Extrema. Discrete Catenary. Newton's Method. Method of Continuous Variations. Truss Balance.)
- Calculus of Variations (Standard Variation. Isoperimetric Problem. Truss Oscillation. Rotation of Axes. Shape of Rotating Rope.)
- Torsion (Navier's Equation. Tension Load.)
- Statistics ($\chi 2$ test. Impartial Evaluation. Statistical Simulations.)
- Combinatorial Optimization (Optimization Problems. Transportation Problem. Shortest Path in a Graph. Maximum Flow Problem. Travelling Salesman Problem. Combinatorial Optimization.)

- Linear programming (Linear Programm. Artificial Rudders. Log Sawing. Nonstandard Linear Programming. Terminology. Combinatorial Nature of Linear programming. Simplex Method.)
- Sawing (Formulation of the Problem. Algorithm. Backpack Problem.)
- Duality Problem (Definition of Duality. Duality Theorem. Optimality of The Simplex Method.)
- Algebraic Graph Theory (Concept of the Graph. Network. Subspaces Theorem. Cycles and Co-cycles. Dimensions of Subspaces C and K. Basis in K. Solving Equations Ax=χ. Basis in C.)
- Out of Kilter (Problem. Reduction to Circular Flows. Duality. Minty's Theorem.)

Course name: **MATHEMATICAL FINANCES IN REAL TIME**
Number of ECTS credits: **9**

Content:
Stochastic integrals.
- Brownian motion.
- Martingales in continuous time.
- Stochastic integrals, Itôv isometry.
- Itôv formula.
- Girsanova Theorem.
- Stochastic differential equations.

Evaluation with the arbitration
- Models for the price movements of securities.
- Implemented claims.
- Options and Black-Sholes formula.
- Inconstancy.
- American options.

Completeness of markets.
- Completeness of markets.
- Completeness of the Black-Sholes model.

Incomplete markets.
- Definitions and examples.
- The concept of availability.
- Evaluation with the domination.

Models of interest rates.
- The importance of stochastic modeling.
- Basic models for current interest rates.
- Options on interest rates.

Course name: **MATHEMATICAL TOPICS IN FOREIGN LANGUAGE**
Number of ECTS credits: **9**

Content:
Actual research topics are presented from the field of algebra which among others include the following areas:
- algebra,
- analysis,
- discrete mathematics,
- financial mathematics,
- cryptography,
- extensive computational methods and applications,
- statistics.

Course name: **MOLECULAR DYNAMICS SIMULATION METHODS**
Number of ECTS credits: **9**

Content:
- Models for molecular simulation
- Newtonian dynamics
- Hamiltonian dynamics
- Classification of dynamical systems
- Numerical integration methods and algorithms
- Lie formalism
- Symplectic methods for molecular dynamics
- Molecular dynamics simulations of temperature and pressure konstatni
- Deals with static properties of molecular systems
- Consideration of the dynamic properties of molecular systems
- Using simulation methods for molecular dynamics

Course name: **MOLECULAR GRAPHICS**
Number of ECTS credits: **9**

Content:
- Overview of computer systems for molecular modelling
- Overview of Computer Graphics
- Molecular visualization
- Geometric optimization
- Modern computer programs for molecular graphics
- Graphical manipulation of molecules and molecular systems

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

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: **STOCHASTIC PROCESSES**
Number of ECTS credits: **9**

Content:
- Markov chains in discrete time, classification of states, strong Markov property, the hit probability, ergodic properties.
- Markov chains in continuous time: definitions, strong Markov property, left and right equations, birth and death processes, processes of diversification, ergodic properties, use.
- Brownian motion: construction of Brownian motion, properties of trajectories, Markov property, the principle of mirroring, martingales related to Brownian motion.

- Poisson processes: abstract definitions, the transformation of Poisson processes, the theory of excursions.

Course name: **GAME THEORY**
Number of ECTS credits: **9**

Content:

- The problems of decision making in strategic situations.
- Basic concepts of game theory: players, moves, income, matrix game with two players.
- Games in normal form: dominating moves, the best answer, Nash balance, mixed moves, the Nash balance existence, important examples.
- Games in normal form in practice: modeling, human decision making.
- Dynamic games, games in the branched form: strategies, Nash balance, reversible induction, undergames, perfect balance of undergames.
- Repeated games: endless recurrence, final recurrence, the People's theorem.
- Dynamic games in practice: differences between theory and human decision making.
- Deciding without common knowledge: dynamic games with incomplete information, sequential balance.
- Evolution game theory.

Course name: **CODING THEORY**
Number of ECTS credits: **9**

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: **THEORY OF FINITE FIELDS**
Number of ECTS credits: **9**

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: **MEASURE THEORY**
Number of ECTS credits: **9**

Content:
The course consists of most relevant subjects in measure theory, which may include:

- The concept of measureability. σ-algebra of measurable sets. Measurable functions. Borel sets and Borel measurable functions. Measureability of limit functions. Simple functions.
- Integral of nonnegative measurable functions and complex measurable functions. Fatou's lemma. Lebesgue's monotone convergence theorem and Lebesgue's dominated convergence theorem. Sets with measure zero and the concept of equality almost everywhere. Lp spaces.
- Positive Borel measures. Support of a function. Riesz's representation theorem for positive linear functional on algebra of continuous functions with compact support. Regularity of Borelovih measures. Lebesgu's measure.
- Approximation of a measurable function with continuous function. Lusin's theorem.
- Complex measures. Total variation. Absolute continuity. Lebesgue-Radon-Nikodym's theorem. Lp spaces as reflexive Banach spaces.
- Measure differentiability, symmetrical derivative of a measure. Absolute continuous functions and fundamental theorem of calculus. Theorem on new variables in integration.
- Product measure and Fubini's theorem. Completion of product Lebesgue measures.

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

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: **INTRODUCTION TO PUBLIC-KEY CRYPTOGRAPHY**
Number of ECTS credits: **9**

Content:
In 1976 Diffie and Hellman invented the concept of public key cryptography which is an essential cryptographic primitive for key exchange and secure (encrypted) communication. The emergance of public key cryptography affected positively the overall use of cryptography due to the simplicity of key exchange using it.
Public key cryptography is used today in electronic mail services, fax, in virus protection, in electronic money, Internet protocols, wireless telecommunication, cable TV, to name a few. In all tellecommunication areas different standards have been adopted such as IEEE, ANSI, ISO, IETF and ATM Forum.
Most of the public key encryption schemes is based on number theory, so that some new algorithms were discovered for some well known old problems. In this course we will study these new algorithms for some number theoretic problems. In the security analysis of the weaknesses of certain cryptographic protocols we also rely on stathistical methods. The objective of this course is to give some general overview of the public key cryptography and the most important public key algorithms that has been used for last 35 years. The following topics will be covered:

- basic concepts in public key cryptography
- finite fields and extended Euclidean algorithm
- public cryptosystems, one-way functions and related problems in number theory (integer factorization, discrete algorithm)
- digital signature
- hash functions and message integrity and authenticity
- key exchange protocols and identification protocols

Course name: **INTRODUCTION TO SYMMETRIC-CIPHER CRYPTOGRAPHY**
Number of ECTS credits: **9**

Content:
Cryptography has a long and fascinating history. The first known use of cryptography goeas back to ancient Egypt, some 4000 years ago.
Since then cryptography has become a modern science that relies on some other mathematical disciplines such as information theory, computer science, number theory, discrete math etc. In modern society exchange and storing of the information in an efficient and secure way of central importance.
Cryptology consists of two areas, namely cryptography (designing secure algorithms) and cryptanalysis which attempts to find security weaknesses. Cryptographic ciphers are used to protect the information of being readable to unauthorized people, modified, or being manipulated in any other way. On the other hand, the cryptanalysis aims in breaking ciphers so that unauthorized access to the information becomes possible. A secure transmission of data is of great importance for Internet and mobile communication, since the range of applications that need secrecy is enormous, e.g.
Payment systems, e-commerce, health and educational systems, military communication, etc. Thus, cryptology becomes important for the security of the society at large.
Stream ciphers is one family of symmetric ciphers along with the so called block ciphers. The major difference between the two is that stream ciphers usually operate on a single bit of information whereas the block ciphers process larger blocks of data at the time.
A widely known symmetric key cipher is AES (Advanced Encryption Standard), which has become a standard cipher adopted by the american government in 2002 as a replacement of the old standard DES.
AES has developed through an initiative of NIST (National Institute of Standards and Technology), which announced an open call for proposals in 1997. Similar initiative was taken later by ECRYPT Stream Cipher Project, which was an attempt to identify and recommend a stream cipher suitable for applications that requires high level of security.
This course gives a solid knowledge about cryptography of synmmetric key ciphers. The following topics will be covered:

- hystory of the classical symmetric key encryption schemes
- fundamental concepts in the design of block and stream ciphers,
- modes of operation of symmetric key ciphers,
- cryptographic criteria for encryption schemes,
- security evaluation and generic attacks,
- basic building blocks of symmetric key encryption schemes,
- State-of-art ciphers and their security

Course name: **PROBABILITY**
Number of ECTS credits: **9**

Content:

- Outcomes, events, σ-algebras (Sample spaces. σ-algebras of events, probability measures. Systems of events, Dynkin's lema. Independence of evens and systems of events.)

- Distributions as measures (Distribution as push-forward of measure. Discretness, density of distributions. Functions of random variables. Multivariate distributions, marginal distributions, independence.)
- Expected value (Expected value as an abstract integral. Expectation as an integral with respect to distribution. Variances and covariances.).
- Conditional expectation (Conditioning with respect to events and discrete random variables. Conditioning with respect to general random variables and σ-fields, existence. Properties of conditional expectation. Conditional distribution. Conditional monotone and dominated convergence theorems.)
- Transformation of random variables (Generating functions. Characteristic functions, uniqueness theorem.)
- Convergence of random variables (Types of convergence, relationships between types of convergence. Borel-Cantelli lemmas. Laws of large numbers. Convergence in distribution. Approximation of distributions.)
- Martingales (Definitions and properties. Optional sampling theorem. Convergence of martingales. Maximal inequalities.)

Course name: **PROBABILITY WITH MEASURE (1)**
Number of ECTS credits: **9**

Content:
Basics of measure theory
- Motivation of the term measure, σ-algebras, construction of measures.
- Measureable functions, Lebesque intergral, convergence theorems.
- L^p - spaces.
- Product measures, Fubini's theorem.
- Radón-Nikodým theorem.

Probability spaces and random variables
- Axiomatic definition of the probability.
- Random variables and their distributions.
- Independence of random variables.

Mathematical mean
- Abstract definition of mathematical mean.
- Variance, covariance.

Course name: **PROBABILITY WITH MEASURE (2)**
Number of ECTS credits: **9**

Content:
Conditional mathematical mean and conditional distributions
- An abstract definition of the conditional mean and basic characteristics.
- The existence of the conditional mathematical mean in general.
- Examples for the calculation of the conditional mathematical mean.
- Conditional distributions.

Transformations of distributions
- Generating functions.
- The process of diversification.
- The characteristic functions.

Approximation of distributions
- Types of convergence of random variables.
- Weak Theorems of large numbers.
- Strong theorems of large numbers.

- Convergence in distribution.
- Normal approximation.
- Poisson approximation.