RUSSIAN - ARMENIAN UNIVERSITY

Master Program

jointly with Kaspersky Laboratories
"Mathematical and Software for Information Security"

MODULE DESCRIPTION

Professional Cycle (64 ECTS credit points)

Continuous Mathematical Models

Lecturer: Prof. Dr. Garnik Karapetyan
Labor intensity: 3 ECTS, 108 academic hours
Form of final control: exam (graded)
Standard Studies Period: 2 years

Course description: A course aimed at the construction, simplification, analysis, interpretation and evaluation of mathematical models that shed light on problems arising in the physical and social sciences. Derivation and methods for solution of model equations, heat conduction problems, simple random walk processes, simplification of model equations, dimensional analysis and scaling, perturbation theory, and a discussion of self-contained modular units that illustrate the principal modeling ideas. Students will normally be expected to develop a modeling project as part of the course requirements.

Recommended literature:

1. G.I. Marchuk. Mathematical modeling in the environmental problem .- M., Nauka, 1982
2. G.I. Marchuk. Methods of computational mathematics .- M., Nauka, 1989
3. V. Volterra. Mathematical theory of the struggle for existence .- M., Nauka, 1976
4. Yu.M. Svirizhev, D.O. Logofet. Stability of biological communities .- M., Nauka, 1978
5. L.A. Petrosyan, V.V. Zakharov. Introduction to mathematical ecology .- M., Nauka, 1986
6. O.V. Besov, V.P. Ilyin, S.M. Nikolsky. Integral representations of functions and embedding theorems.-M., Nauka, 1975
7. V.S. Of the world. Equations of mathematical physics.-M., Nauka, 1971.
8. L. HERMANDER. Linear differential operators with partial derivatives. - M., Mir, 1965.
9. L. HERMANDER. Analysis of linear partial differential operators, vol.1 (Theory of distributions and Fourier analysis) .- M., Mir, 1986.
10. V.S. Vladimirov. Generalized functions in mathematical physics.-M., Nauka, 1979.

History and Methodology of Applied Mathematics and Informatics

Lecturer: Prof. Dr. Parkev Avetisyan
Labor intensity: 2 ECTS, 72 academic hours
Form of final control: exam (pass/fail)

Standard Studies Period: 2 years

Course description: The course is designed for the future specialists in applied mathematics. It aims to show students the historical roots of their specializations and to unfold some methodological problems that anyone working in the field most frequently encounters. This is the major rationale for the course.

Foreign language

Labor intensity: 5 ECTS, 180 academic hours
Form of final control: exam (pass/fail)
Standard Studies Period: 2 years

Course description: This course will provide instruction in academic and professional language skills for non-native speakers of English. Emphasis is placed on development of integrated language skills for use in studying a particular content area. Upon completion, students should be able to demonstrate improved language skills for participation and success within the particular topic area.

Modern problems of applied mathematics and computer science

Lecturer: Prof. Dr. Parkev Avetisyan
Labor intensity: 2 ECTS, 72 academic hours
Form of final control: exam (pass/fail)
Standard Studies Period: 2 years

Course description: The course is designed for the future specialists in applied mathematics. It aims to show students the modern problems of their specializations and to unfold some methodological problems that anyone working in the field most frequently encounters. This is the major rationale for the course.

Information theory

Lecturer: G. Mkrtchyan, Phd, Japan
Labor intensity: 3 ECTS, 108 academic hours
Form of final control: exam (pass/fail)

Course description: The target of information theory course is to teach fundamental bases of the mathematical theory of information generation, conversion and transmission.

The course consists of four parts.

We start from the definition of entropy as a fundamental measure of mutual information of random data grounded on its random probabilistic nature, then generalize to joint entropy and conditional entropy for combination of multiple dependent random data ensembles.

For effective and reliable transmission of information, it should be converted to the form most suitable for communication channel, and as a result arises the requirement of data encoding (data conversion before transmission through the channel) and decoding (data conversion after transmission through the channel). This part of the course is dedicated to the source coding theorem, and introduction to the fixed and variable length codes, including discussion of variable length codes for compression, fixed length linear block codes and convolution codes for error detection and correction.

Communication channels are mediums for transmission of data, and their characteristics limit the form and amount of data which can be transmitted through them. In channels related part of the course are discussed discrete (binary and multi-state) and continuous (AWGN and multi-path propagation) communication channels and their characteristics: noise, bandwidth, channel response function. Then is defined channel capacity as the maximum of its mutual information over all possible input distributions, and calculated the Shannon rate limit and efficiency for noisy continuous channels.

The final part of the course is related to the Kolmogorov complexity, with the definition of the algorithmic complexity of a data sequence, its relation to the entropy of the distribution from which the data was generated, minimal description length and comparability of complexity based on it.

Recommended literature:

1. "Elements of Information Theory", 2nd Edition, by Thomas M. Cover and Joy A. Thomas, 2006.
2. "Information Theory and Statistics", by Solomon Kullback, 1997.

Discrete stochastic models

Lecturer: L. Kachaturyan, Phd.
Labor intensity: 3 ECTS, 108 academic hours
Form of final description: exam (graded)

Course content: The main purpose of this course for muster students is to demonstrate on various examples the power and generous possibilities of probabilistic methods applied to problems from different areas of mathematics.
The course consists of three main parts. The first part contains preliminary facts from probability theory including general discrete probability model, model of sequence of independent trials and Markov scheme (Markov chains). All these material is accompanied by practical examples.
The second part is dedicated to application of probabilistic methods in graph theory, combinatorics, Ramsey theory and extreme theory of sets. We demonstrate on various examples how to use probabilistic methods to obtain deterministic assertions. Generally such statements are existence theorems, but we also demonstrate how probabilistic approach gives an opportunity to create (deterministic) algorithms of finding objects which existence are proved.
In the third part of this course the mathematical theory of communication (Shannon's information theory) is expound. The notion of entropy and its properties are considered. The source coding theorems are discussed both for uniform and variable-length coding. The Shannon's theorems of optimal information transmission in discrete channels without memory are proved.

Recommended literature:

1. Parzen, E. (1962) Stochastic Processes, Holden-Day.
2. Dodge, Y. (2006) The Oxford Dictionary of Statistical Terms, OUP.

Modern Operating Systems

Lecturer: Prof. Rouben Topchyan
Labor intensity: 4 ECTS, 144 academic hours
Form of final control: exam (graded)
Standard Studies Period: 2 years

Course description: The foundations of the organization of modern multiprocessor operating systems are studied in the course. The concepts of the organization of interactions between parallel processes and questions connected with deadlocks, the issues of planning of the computer system processors loading, as well as memory management, the organization of file

systems, and information security issues are examined. The course contains both a thorough familiarization with system calls that control flows, processes, objects of inter process communication, and existing utilities that facilitate the process of developing software in the environment of operating systems of various types. The principles of the organization of operating systems for computer networks in multiprocessor systems are being studied. A comparative analysis of the performance of different operating systems is carried out. Methods and features of programming in Windows, Linux and Unix-like operating systems are being studied.

Topics cover the following themes:

- interfacing synchronous and asynchronous processes
- input/output system, buffering
- interrupts
- general parallel processes using fork and join
- critical sections, mutual exclusion
- other coordination primitives
- segmentation and paging
- virtual memory
- storage allocation and sharing

Recommended literature:

1. TanenbaumA., WoodhallA. .OperatingSystems: Design and Development. (3rded.) 2005
2. Stollins W. OperatingSystems: InternalsandDesignPrinciples. — Addison Wesley,2003.
3. TanenbaumA. ModernOperating Systems (6th ed.), Prentice-Hall, 2010.

Numerical methods and optimization

Lecturer: Prof. Dr. Yuri Hakobyan
Labor intensity: 4 ECTS, 144 academic hours
Form of final control: exam (graded)
Standard Studies Period: 2 years

Course description: Numerical methods are an important branch in Applied Mathematics. It aims at numerically solving all kinds of mathematical problems which arise from practical applications and can be modelled by different mathematical equations or inequalities, for example, linear or nonlinear differential equations and integral equations.
Course prerequisite:
Most fundamental: advanced calculus and linear algebra.
The course is focused on both numerical methods and numerical analysis. And mathematical analysis is needed for nearly every numerical method to be introduced. So students should be

very solid in analysis, and have a very good feeling and understanding of numerical methods and rigorous mathematical reasoning.

Recommended literature:

1. V.M. Verzhbitsky. Fundamentals of numerical methods.-M .: Higher School, 2002.
2. D. Watkins. Fundamentals of matrix calculations. - Moscow: BINOM. Laboratory of Knowledge, 2006.
3. D.V. Beklemishev. Additional chapters of linear algebra. - Moscow: Nauka, 1983.
4. D. Kincaid and W. Cheney. Numerical Analysis: Mathematics of Scientific Computing.- Brooks / Cole Publishing Company, 1991.

Architecture of Modern Computer Systems

Lecturer: Prof. Gagik Sardaryan
Labor intensity: 4 ECTS, 144 academic hours
Form of final control: exam (graded)
Standard Studies Period: 2 years

Course description: In the course the various fundamental components of computer systems are explored. The operation of the computer CPU in detail is explained and some of the many variations on the basic CPU design in different systems are introduced. The fundamental group of instructions that make up the repertoire of the computer and a fetch-execute cycle are learned. The variations in instruction sets and memory addressing techniques that differentiate computers from one another and extend the flexibility of the basic architecture are considered. In the course various CPU architectures, memory enhancements, and CPU organizations that expand the processing power of the CPU are explored. Various techniques used to perform I/O operations are considered as well. The advantages of adding additional CPUs in the form of multiprocessing and of off-loading operations into additional processors built into I/O modules are explored. The workings of various peripheral devices and some of the interactions between the various components in the computer system are presented.

Topics cover the following themes:

- Performance Measurement
- Instruction Set Architecture
- Arithmetic and ALU Design
- CPU Design and Execution
- Pipelining for Increased Performance
- Memory: Cache, Main, Virtual
- I/O Devices and Protocols

Recommended literature:

1. Patterson, D.A. and J.L. Hennesey. Computer Organization and Design: The Hardware/Software Interface, Second Edition, San Francisco, CA: Morgan Kaufman, 1998.
2. Tanenbaum, A. S. Structured Computer Organization. Englewood Cliffs, New Jersey: Prentice-Hall,1979.
3. John L. Hennessy and David A. Patterson. Computer Architecture: A Quantitative Approach (3rd ed.). Morgan Kaufmann Publishers.2001.
4. Joseph D. Dumas II. Computer Architecture: Fundamentals and Principles of Computer Design. CRC Press, 2005.
5. Tanenbaum A., Austin T. Computer Architecture. (6th ed.), Prentice-Hall, 2014.

Principles of Database Systems

Lecturer: Prof. Manuk Manukyan
Labor intensity: 4 ECTS, 144 academic hours
Form of final control: exam (graded)
Standard Studies Period: 2 years

Course description: The theoretical and practical aspects of the implementation of the concept of databases are being considered within the course. Entity-relationship and object definition models are used as formalism for database modeling. Problems of relational database scheme design are emphasized. Issues for object, object-relational, deductive and semi structured data models are considered as well. SQL and OQL (Object Query Language) are examined. The algebraic and logical approaches of the query language construction, active, semi-structured and deductive databases are examined in detail. The problems of database integrity constraints are considered in the context of the relational model. Theoretical considerations are accompanied by development of corresponding projects in well-known database systems which help to acquire the knowledge. A comparative analysis of different approaches in database systems is provided.

Topics cover the following themes:

- an introduction to the implementation of database systems;
- data storing essentials;
- system and index structures:
- query development;
- parallel management;
- transaction development;
- security and information integration;
- semi-structured and deductive databases;
- distributed databases.

Prerequisites: Data Structures and Fundamental Algorithms, Discrete Mathematics, Programming languages, Basics of Database Systems.

Recommended literature:

1. Ricardo C.M. Database Systems: Principles, Design and Implementation. Prentice Hall PTR Upper Saddle River,1990
2. C. J. Date, An Introduction to Database Systems, Addison-Wesley, 2004.
3. H. Garcia-Molina, J. D. Ullman, J. Widom, Database System: The Complete Book, Printice Hall, 2002.
4. L. A. Kalinichenko, Data model transformation method based on axiomatic data model extension, 4th International Conference on VLDB, pp. 549-555, Germany, September, 1978.

Stochastic processes

Lecturer: N. Babayan, Phd.
Labor intensity: 2 ECTS, 72 academic hours
Form of final control: exam (pass/fail)
Standard Studies Period: 2 years

Course description:

1. The contents of the discipline:

- the bases of the theory of stochastic processes, including:
- basic concepts and provisions of the theory of stochastic processes;
- classes of stochastic processes and their examples: Markov, Gaussian, stationary in the narrow and broad sense, homogeneous processes with independent increments, processes with uncorrelated increments;
- methods for the study of stochastic processes: combinatorial, differential, spectral;
- applications of the theory of stochasticprocesses.

2. Objectives of the discipline:

- acquisition of knowledge, skills and abilities in volume of the contents of the discipline;
- development of students skills of application of the course provisions in the chosen specialty;
- development of professional mobility of students, formation of their abilities for self-improvement of knowledge in the theory of stochastic processes and their applications;
- raising the general mathematical culture of students, improving their probabilistic and analytical thinking, as well as common professional and cultural competences.

Recommended literature:

1. Joseph L. Doob. Stochastic processes. Wiley. 1990.

Coding theory

Lecturer: G. Mkrtchyan, Phd, Japan
Labor intensity: 3 ECTS, 108 academic hours
Form of final control: exam (pass/fail)
Standard Studies Period: 2 years

Course description: The aims of coding theory course is to provide knowledge of the mathematical theory of information (data) conversion targeted to the error detection and correction in stored and transmitted data.

The course consists of five parts.

We start from overview of algebraic field theory with definition of groups, rings and fields based on composition laws. Then discuss homomorphism, isomorphism and automorphism mapping of the rings and fields, polynomial representation of rings, polynomials factoring and irreducible polynomials, and finalize overview with discussion of Galois fields theory and vector spaces representation based on it.

After algebraic math overview we continue with discussion of general codes characteristics, defining the distance between codes as Hamming distance and prove that it is a metric. Then we provide the maximum likelihood decoding principle applied to codes and show its relation to Hamming distance.

In next part are discussed linear block codes. We define generation and parity-check matrices, with their implementation in creation of codes and detection of errors, then provide usage of coset and its leader calculation for correction of linear codes. After discussion of general characteristics of linear codes we continue with examples of perfect codes and proving the bounding theorems for linear codes performance. Since cyclic codes are linear block codes with very fast and easy generation, detection and correction and are widely used because of that capabilities, we thoroughly discuss their Galois field polynomial representation and employ polynomials factoring for their generation, detection and correction. Next we present the most popular examples of cyclic codes: BCH and Reed-Solomon Codes and discuss their generation, detection and correction both direct and alternative algorithms.

After linear block codes we discuss convolutional codes, their polynomial and rational encoders and hard and soft decoding based on quantization and Viterbi algorithm. We perform error analysis for convolutional codes based on node error probability and the bit error rate.

The final part of the course is dedicated to the currently most actual coding theory topics: turbo codes, low density parity check codes (LDPC) and space-time coding since they can provide very high performance. We discuss their encoding based on parallel concatenation, finite geometries and maximal-ratio combining and iterative, graph and trellis based soft decoding.

Recommended literature:

1. "Error Correction Coding: Mathematical Methods and Algorithms", by Todd K. Moon, 2005
2. "Introduction to Coding Theory (Graduate Texts in Mathematics)", by J.H. van Lint, 1998

Asymmetric cryptography algorithms

Lecturer: G. Mkrtchyan, Phd, Japan
Labor intensity: 2 ECTS, 72 academic hours
Form of final control: exam (pass/fail)
Standard Studies Period: 2 years

Course description: The purpose of asymmetric cryptography algorithms course is to introduce to the algebraic number theory and its application to the asymmetric public/private key based cryptography.

The course consists of four parts.

We start from introduction of number theory basics: prime numbers, divisibility, Euclid's theorem, unique factorization theorem, primality testing and factorization methods: sieve of Eratosthenes; Euler's, Fermat's, Pollard's and Dixon's factorization methods, quadratic and rational sieves, algebraic-group factorization algorithm, Shanks' square forms factorization and Shor's quantum algorithm, then discuss modular arithmetic and Fermat's little, Euler's and Wilson's theorems. Next we discuss general Diophantine equations and their special case Weierstrass equation as an elliptic curves generation function, and we finalize introduction with elliptic curves discussion: j-invariancy, endomorphisms, singularity, elliptic curves modular arithmetic, elliptic curves over finite fields, elliptic curves in primality testing and factoring.

After number theory introduction we start discussion of asymmetric cryptography algorithms based on usage of integer numbers modular arithmetic under assumption of high complexity of discrete logarithm computation for big integers: Diffie–Hellman key exchange algorithm and ElGamal encryption. Next we discuss an asymmetric cryptography algorithm based on integer numbers modular arithmetic but under assumption of high complexity of big integers factorization: RSA public key cryptosystem. At the of this part are discussed possible

vulnerabilities in Diffie–Hellman, ElGamal and RSA algorithms in cases of certain integers usages.

Third part of the course is dedicated to the asymmetric cryptography algorithms based on usage of elliptic curves modular arithmetic with assumption of complexity of solving Weierstrass equation for integer numbers under big modulo n. We again discus Diffie–Hellman key exchange, ElGamal encryption and RSA public key cryptosystem but now based on elliptic curves modular arithmetic operations.

The final part of the course is related to the introduction of extension of elliptic curves based asymmetric cryptography algorithms to the hyperelliptic curves with usage of Diophantine equations of more complex forms and higher degrees of polynomials instead of Weierstrass equation. We discuss implementation of divisor classes and pseudo discrete logarithm in hyperelliptic based curve cryptosystems.

Recommended literature:

1. "An Introduction to Number Theory with Cryptography", by J. S. Kraft and L. C. Washington, 2013.
2. "Elliptic Curves: Number Theory and Cryptography", Second Edition, by L. C. Washington, 2008.

Special chapters of graph theory

Lecturer: P. Petrosyan, Phd
Labor intensity: 2 ECTS, 72 academic hours
Form of final control: exam (pass/fail)
Standard Studies Period: 2 years

Course description:

1. Main results of Extremal graph theory (theorems of Mantel, Reiman, Turan and Erdős-Stone).

2. Factors, independent sets, matchings and covers. Matchings in bipartite graphs and min-max theorems. Maximum matchings and alternating paths. The characterization of maximum matching in terms of alternating paths. Matchings that saturates X in a bipartite graph with bipartition (X,Y). System of distinct representatives and Hall's theorem. Tutte's **f**-factor theorem. Independent sets and Caro-Wei's theorem.

3. Eulerian and Hamiltonian graphs. Euler's theorem and Fleury's algorithm. Necessary, sufficient conditions for hamiltonicity. Theorems of Dirac, Ore, Goodman-Hedetniemi, Chvatal-Erdős and Bondy-Chvatal. Hamiltonian cycles and Travelling salesman problem.
4. Degree sequences. Graphic sequences. Degree sequences of pseudographs, multigraphs and hypergraphs (theorems of Hakimi, Erdős-Gallai and Havel-Hakimi).
5. Vertex colorings of graphs. General bounds of chromatic number. Brooks' theorem. Edge-colorings of graphs. König's and Vizing's theorems. Interval edge-colorings of graphs and scheduling problems.

Recommended literature:

1. B. Bollobas, Modern Graph Theory, Springer, 1998.
2. J. Akiyama, M. Kano, Factors and Factorizations of Graphs, (Proof Techniques in Factor Theory), Springer-Verlag Berlin Heidelbelg, 2011.
3. G. Chartrand, P. Zhang, Chromatic Graph Theory, Discrete Mathematics and Its Applications, CRC Press, 2009.

Protecting Information from Malicious Software

Lecturer: S. Abrahamyan, Phd
Labor intensity: 3 ECTS, 108 academic hours
Form of final control: exam (pass/fail)
Standard Studies Period: 2 years

Course description: 1**.** Classification. DdOS attacks. Spam. Online banking. 2. Winbase. Windows architecture. Service. Drivers (Practice: dynamic analysis, ProcMon practice). 3. Assembler. Disassembling. (Practice: antistatic, simple ddos-trojan, downloader). 4. PE-format. Loader work. (Practice: file infectors in NOTEPAD.exe, a real infector). 5.Static code analysis. Dynamic code analysis. (Practice: sample using ProcMon, a sample for Ida Pro, krekmi Narvahi). 6.Software packers. (Practice: manual unpacking). 7. Methods of protecting software from dynamic analysis. SHE (Practice: Crackme with antidynamics + WinSpy). 8. Web-based vulnerabilities.(Practice: vulnerable site). 9. Vulnerability of software. Exploits. Silk codes. (Practice: Metasploit.). 10. Intel Architecture. Operating modes of the processor. (Practice: getting to know WinDbgRootkits (Butkits)).11. Optional: parse stuxnet. 12. Types of attacks.(Practice: WireShark). 13. IDS / IPS attack detection systems. (Practice: Snort).

The Basics of Information Security

Lecturer: S. Tairyan Phd
Labor intensity: 2 ECTS, 72 academic hours
Form of final control: exam (pass/fail)
Standard Studies Period: 2 years

Course description: "The Basics of Information Security*"* provides fundamental knowledge of information security in both theoretical and practical aspects. This course provides a one-semester overview of information security. It is designed to help students with basic computer knowledge understand this important priority in society today. This course is packed with key concepts of information security, such as confidentiality, integrity, and availability, as well as tips and additional resources for further advanced study. The technical content of the course gives a broad overview of essential concepts and methods for providing and evaluating security in information systems . This course includes practical applications in the areas of physical, network, operating system, cryptography, steganography, IT audit and ethical hacking. In addition to its technical content, the course touches on the importance of management and administration, the place information security holds in overall business risk, social issues such as individual privacy, and the role of public policy.

Computational Geometry

Lecturer: Prof. Dr. R. Aramyan
Labor intensity: 2 ECTS, 36 academic hours
Form of final control: exam (pass/fail)
Standard Studies Period: 2 years

Course description: The aim of the course is the design and analysis of algorithms for solving geometric problems. Also the course consider integral and stochastic geometry methods for solving problems.
Summary.
Representation of geometric objects (points, segments, polygons).
The problem of "intersection of segments". Method of sweeping the plane.
Polygons, types of polygons. Area of the polygon. The task "point in a polygon". Triangulation: the existence and complexity of construction. Delaunay triangulation. The task of Art-Gallery.
The problem of "construction of a convex hull of a set of points", an estimate of the lower bound of complexity. Algorithms: Jarvis, Graham, "divide and conquer", Krikpatrika-Seidel, Chan.

The Voronoi diagram. Algorithms of construction. Steiner tree. Extreme geometric problems. Consider basic models of stochastic geometry -- random sets, point processes of geometric objects (particles, flats), and random mosaics.

Recommended literature:

1. D.M. Vasilkov. Geometric Modeling and Computer Graphics. Computational and Algorithmic Fundamentals. Minsk. BSU.
2. T. Corman, C. Leyzerson, R.Rivest, K.Stait. Algorithms. Construction and Analysis. M. Williams 2005.
3. M. Laslo. Computational Geometry and Computer Graphics in C ++. M.Binom.1997.
4. R. Schneider, W, Weil, Wolfgang Stochastic and Integral Geometry, Springer, 2004.

Cryptography

Lecturer: S. Abrahamyan, Phd
Labor intensity: 1 ECTS, 36 academic hours
Form of final control: exam (pass/fail)
Standard Studies Period: 2 years

Course description: The course covers core the following topics.

1. Introduction. 2. Mathematical Background. 3Block ciphers. 4. AES (Encryption of AES, Decryption of AES, Cryptanalysis of block-ciphers). 5. Public key cryptography. 6.Encryption of RSA. 7. Decryption of RSA. 8. Encryption of El-Gamal. 9.Decryption of El-Gamal. 10. Digital Signature algorithms. 11. DSA based on RSA. 12. DSA based on El-Gamal.13. Stream-Ciphers, pseudo-random number generators. 14. RC-4. 15. Searchable encryption. 16. Homomorphic encryption open problems.

Theory and methods of statistical data analysis

Lecturer: V. Bardakchyan, Phd
Labor intensity: 2 ECTS, 72 academic hours
Form of final control: exam (pass/fail)
Standard Studies Period: 2 years

Course description: The course is intended to introduce the use of several statistical packages (Eviews, Stata and partially R) to students. The main goal is achieving practice in the use of mentioned computer programmes for statistical purposes and in data analysis.

These programmes (Eviews and Stata) are designedmainly for econometrics and hypothesis testing. So during the course students will learn to perform several types of regressions, and make inferences based on results presented.

Also at the end of the course students should be able to introduce and make manipulations (summing, combining, making lagged variants of etc.) with statistical data, work with time series (extract trends, detect seasonality find the type of process (AR, ARIMA, GARCH) etc.) and panel data, and to analyze data (check normality, stationarity etc.). Also students should be able to visualize the results by plotting, or drawing several types of charts.

Recommended literature:

1. Devore JL, Kenneth N. Modern mathematical statistics with applications, 2nd edn. Springer, New York, 2012.

Complexity of algorithms and Computations

Lecturer: R. Tonoyan, Prof.
Labor intensity: 3 ECTS, 108 academic hours
Form of final control: exam (graded)
Standard Studies Period: 2 years

Course description: The course is intended to introduce the use of Fourier transforms, Euclid algorithms, some fast number multiplication algorithms and polynomials evaluation method.

We start from introduction of number theory basics: prime numbers, divisibility, Euclid's theorem, unique factorization theorem, primality testing and factorization methods: Euler's, Fermat's and Dixon's factorization methods, quadratic and rational sieves, algebraic-group factorization algorithm, Shanks' square forms factorization and Shor's quantum algorithm, then discuss modular arithmetic and Fermat's little and theorems.
After number theory introduction we start discussion of Fourier transforms(Fast and Fourier transforms). During this part the many FFT algorithms is considered.

Third part of the course is dedicated to the number multiplication algorithms. During this part we consider Karatsuba's algorithm, some methods from Fourier transforms, polynomial evaluation and multiplication methods.

At the end of the course students should be able to introduce the aim of Fourier transform, do some computations via Fourier transform, implement number multiplication algorithms, gives a complexity of multiplication algorithms.

Recommended literature:

1. Stein, Elias; Shakarchi, Rami (2003*),* Fourier Analysis: An introduction, Princeton University Press, ISBN 0-691-11384-X.

2. David C. Lay. Linear Algebra and Its Applications, 3rd ed. Addison Wesley, Boston, 2003.

Advanced Probability Theory

Lecturer: Prof. Dr. R. Aramyan
Labor intensity: 3 ECTS, 108 academic hours
Form of final control: exam (pass/fail)
Standard Studies Period: 2 years

Course description: The course covers core topics in measure theoretic probability and modern stochastic calculus, thus laying a rigorous foundation for studies in statistics and other areas where uncertainty is essential and needs to be described with advanced probability models. Emphasis is on probability theory as such rather than on special models occurring in its applications. Brief review of basic probability concepts in a measure theoretic setting: probability spaces, random variables, expected value, conditional probability and expectation, independence, Borel-Cantelli lemmas Construction of probability spaces with emphasis on stochastic processes. Operator methods in probability: generating functions, moment generating functions, Laplace transforms, and characteristic functions. Notions of convergence: convergence in probability and weak laws of large numbers, convergence almost surely and strong laws of large numbers, convergence of probability measures and central limit theorems. If time permits and depending on the interest of the students topics from stochastic calculus might be covered as well.

Algorithms and information security

Lecturer: Prof. Dr. R. Tonoyan
Labor intensity: 4 ECTS, 144 academic hours
Form of final control: exam (graded)
Standard Studies Period: 2 years

Course description: 1. Recursive algorithms. 2. Computable functions. Solvable and enumerable sets. 3. Algorithmically insoluble problems. 4. The 10th problem of Hilbert. 5. Probabilistic algorithms. 6. Hashing. 7. Introduction to the theory of algorithms and examples. 8. Complexity of algorithms. 9. Linear Programming.

Recommended literature:

1. William Stallings. Cryptography and Network Security, 7th edition, Pearson, 2016.

Economy and policy of transition

Lecturer: Prof. Dr. Armen Darbinyan
Labor intensity: 1 ECTS, 36 academic hours
Form of final control: exam (pass/fail)
Standard Studies Period: 2 years

Course description: This course studies the economics of public policy towards the environment. We begin by examining the problem of market failure in the presence of externalities and public goods. Then, we consider the public policy responses to these market failures, including command-and-control regulations, tax and subsidy incentives, marketable pollution permits, voluntary programs, and information as regulation. We consider these policies in contexts such as local pollution, climate change, threats to biodiversity, environmental justice, international trade, and development. In addition, we learn how to measure the costs and benefits of pollution control. By the end of the semester, you will learn how economists think about environmental problems, understand the advantages and disadvantages of a range of environmental policies, be able to conduct a cost-benefit analysis, and have a complete economic analysis of an environmental problem.