Universitatea Națională de Știință și Tehnologie Politehnica București
Facultatea de Electronică, Telecomunicații și
Tehnologia Informației

COURSE DESCRIPTION

1. Program identification information

1.1 Higher education institution	**National University of Science and Technology Politehnica Bucharest**
1.2 Faculty	**Electronics, Telecommunications and Information Technology**
1.3 Department	**Electronic Technology and Reliability**
1.4 Domain of studies	Electronic Engineering, Telecommunications and Information Technology
1.5 Cycle of studies	Masters
1.6 Programme of studies	Quality and Safety Engineering in Electronics and Telecommunications

2. Date despre disciplină

2.1 Course name (ro) (en)				Modelarea stochastică şi statistică aplicată Stochastic modeling and applied statistics			
2.2 Course Lecturer				Conf. Dr. Emil SIMION			
2.3 Instructor for practical activities				Conf. Dr. Emil SIMION			
2.4 Year of studies	1	2.5 Semester	I	2.6. Evaluation type	E	2.7 Course regime	Ob
2.8 Course type		DS	2.9 Course code	UPB.04.M1.O.14-01		2.10 Tipul de notare	Nota

3. Total estimated time (hours per semester for academic activities)

3.1 Number of hours per week	2	Out of which: 3.2 course	1.00	3.3 seminary/laboratory	1
3.4 Total hours in the curricula	28.00	Out of which: 3.5 course	14	3.6 seminary/laboratory	14
Distribution of time:					hours
Study according to the manual, course support, bibliography and hand notes Supplemental documentation (library, electronic access resources, in the field, etc) Preparation for practical activities, homework, essays, portfolios, etc.					40
Tutoring					4
Examinations					3
Other activities (if any):					0

3.7 Total hours of individual study	47.00
3.8 Total hours per semester	75
3.9 Number of ECTS credit points	3

4. Prerequisites (if applicable) (where applicable)

4.1 Curriculum	Is not mandatory.
4.2 Results of learning	Accumulation of basic knowledge in the fields: statistics, cryptography.

5. Necessary conditions for the optimal development of teaching activities (where applicable)

5.1 Course	The course will take place in a room equipped with video projector and computer.
5.2 Seminary/ Laboratory/Project	The seminar will take place in a room equipped with video projector and computer.

6. General objective *(Reffering to the teachers' intentions for students and to what the students will be thought during the course. It offers an idea on the position of course in the scientific domain, as well as the role it has for the study programme. The course topics, the justification of including the course in the currcula of the study programme, etc. will be described in a general manner)*

The application of probabilistic and statistical techniques and methods in the virtual environment. The application, in typical situations, of the methods of designing cryptographic algorithms and protocols (cryptography), as well as of their evaluation methods (cryptanalysis).

7. Competences *(Proven capacity to use knowledge, aptitudes and personal, social and/or methodological abilities in work or study situations and for personal and proffesional growth. They refflect the empolyers requirements.)*

Specific Competences	Demonstrates basic/advanced knowledge in applied statistics and cryptography. Correlate knowledge. Apply knowledge in practice. It applies standardized methods and tools, specific to the field, to carry out the evaluation and diagnosis process of a situation, depending on the identified/reported problems, and identifies solutions. It argues and analyzes coherently and correctly the context of application of the basic knowledge of the field, using key concepts of the discipline and the specific methodology. Oral and written communication in Romanian: uses the scientific vocabulary specific to the field, in order to communicate effectively, in writing and orally.
Transversal (General) Competences	Autonomy and critical thinking: the ability to think in scientific terms, search and analyze data independently, and draw and present conclusions / identify solutions. Ability to analyze and synthesize: presents the acquired knowledge in a synthetic way, as a result of a process of systematic analysis. Respect the principles of academic ethics: correctly cite the bibliographic sources used in the documentation activity. Puts elements of emotional intelligence into practice in the appropriate social-emotional management of real-life/academic/professional situations, demonstrating self-control and objectivity in decision-making or stressful situations.

8. Learning outcomes *(Synthetic descriptions for what a student will be capable of doing or showing at the completion of a course. The learning outcomes reflect the student's acomplishments and to a lesser extent the teachers' intentions. The learning outcomes inform the students of what is expected from them with respect to performance and to obtain the desired grades and ECTS points. They are defined in concise terms, using verbs similar to the examples below and indicate what will be required for evaluation. The learning outcomes will be formulated so that the correlation with the competences defined in section 7 is highlighted.)*

Knowledge	*The result of knowledge aquisition through learning. The knowledge represents the totality of facts, priciples, theories and practices for a given work or study field. They can be theoretical and/or factual.* Defines domain-specific notions. Describes/classifies notions/processes/phenomena/structures. It highlights consequences and relationships. Knows and applies specific methodologies and tools for creating a logical and physical database structure (logical data structures, diagrams, modeling methodologies, relationships between entities).
Skills	*The capacity to apply the knowledge and use the know-how for completing tasks and solving problems. The skills are described as being cognitive (requiring the use of logical, intuitive and creative thinking) or practical (implying manual dexterity and the use of methods, materials, tools and intrumentation).* Select and group relevant information in a given context. Uses reasoned specific principles in order to analyze the relationships of dependence / independence, causality / association. Work productively in a team. Elaborate a scientific text. Solve practical applications. Argue the identified solutions / workarounds. It applies schemes and models for validation and analysis of cryptographic algorithms and protocols, performs data processing / comparisons / interpretations. Acquire, correct or improve knowledge of cryptographic algorithms and protocols, using scientific methods and techniques.
Responsability and autonomy	*The student's capacity to autonomously and responsably apply their knowledge and skills.* Select appropriate bibliographic sources and analyze them. Respect the principles of academic ethics, correctly citing the bibliographic sources used. Demonstrates responsiveness to new learning contexts. Demonstrates collaboration with other colleagues and teaching staff in carrying out teaching activities Demonstrates autonomy in organizing the learning situation/context or the problem situation to be solved Demonstrates social responsibility through active involvement in student social life/involvement in academic community events Promotes/contributes through new solutions related to the specialized field to improve the quality of social life. Realizes the value of its contribution in the field of engineering to the identification of viable/sustainable solutions to solve problems in social and economic life (social responsibility). Apply principles of professional ethics/deontology in the analysis of the technological impact of the solutions proposed in the specialized field on the environment. Analyzes and capitalizes on business/entrepreneurial development opportunities in the specialty area. Demonstrates real-life situation management skills (collaborative vs. conflict time management). The identification of opportunities for continuous training and the effective use, for one's own development, of information sources and resources of communication and assisted professional training (Internet portals, specialized software applications, databases, online courses, etc.) both in the Romanian language, as well as in an international language. The ability to communicate with the superior hierarchical structures and with the subordinate team.

9. Teaching techniques *(Student centric techniques will be considered. The means for students to participate in defining their own study path, the identification of eventual fallbacks and the remedial measures that will be adopted in those cases will be described.)*

Starting from the analysis of students' learning characteristics and their specific needs, the teaching process will explore both expository (lecture, exposition) and conversational-interactive teaching methods, based on discovery learning models facilitated by direct exploration and indirect of reality (experiment, demonstration, modelling), but also on action-based methods, such as exercise, practical activities and problem solving.

In the teaching activity, lectures will be used, based on Power Point presentations or different videos that will be made available to the students. Each course will start with a recap of the chapters already covered, with an emphasis on the concepts covered in the last course.

Presentations use images and diagrams so that the information presented is easy to understand and assimilate.

This discipline covers information and practical activities designed to support students in their learning efforts and the development of optimal collaborative and communicative relationships in a climate conducive to discovery learning.

10. Contents

COURSE		
Chapter	**Content**	**No. hours**
1	Probability theory. Classical probability schemes. Probability distributions. Central limit theorem.	1
2	Parameter estimation. Point estimate. The method of moments and the method of maximum likelihood.	2
3	Confidence intervals. Statistical tests.	1
4	Statistical tests used in the evaluation of random and pseudo-random generators.	2
5	Cryptographic techniques and methods. Classical encryption algorithms; Symmetric encryption algorithms (AES, operating modes); Security assessment,	2
6	Cryptographic protocols (identification and authentication, key exchange: Diffie-Hellman).	2
7	Security assessment of communication infrastructure (algorithm, cryptographic module: ISO19790/FIPS 140-3, cryptographic products: ISO 15408/EUCC, systems: ISO27001, NIS-2 directive).	2
8	Case studies (ransomware attack analysis, security analysis).	2
	Total:	14

Bibliography:
1. A.J. Menezes, P. Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1999.
2. D. Naccache, E. Simion ş.a, Criptografie şi Securitatea Informaţiei. Aplicaţii, MATRIXROM, 2011.
3. B. Schneier, Applied Criptography, Second Edition, John Wiley & Sons, 1996.
4. E. Simion, V. Preda şi A. Popescu, Criptanaliza. Rezultate şi Tehnici Matematice, Ed. Univ. Buc., ISBN 973575975-6, 2004.
5. D. Stinton, Cryptography, Theory and Practice, Chapman &Hall/CRC, Third Edition, 2006.
6. W. Stalings, Cryptography and Network Security: Principles and Practice (6th Edition)- 6th Edition, 2013.
7. FIPS 140-2, Security Requirements for Cryptographic Modules, 2001.
8. National Institute of Standards and Technologies, SP 800-22, A statistical test suite for random and pseudorandom number generators for cryptographic applications, 2010.

SEMINARY

Crt. no.	Content	No. hours
1	Applications of the central limit theorem	2
2	Applications regarding parameter estimation. Point estimate. The method of moments and the method of maximum likelihood.	2
3	Confidence intervals. Statistical tests.	2
4	Cryptanalysis of classic encryption systems. Cryptanalysis and security evaluation of symmetric algorithms.	2
5	Security evaluation of asymmetric cryptographic algorithms	2
6	Case studies on ransomware attacks	4
	Total:	14

Bibliography:
1. A.J. Menezes, P. Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1999.
2. D. Naccache, E. Simion ş.a, Criptografie şi Securitatea Informaţiei. Aplicaţii, MATRIXROM, 2011.
3. B. Schneier, Applied Criptography, Second Edition, John Wiley & Sons, 1996.
4. E. Simion, V. Preda şi A. Popescu, Criptanaliza. Rezultate şi Tehnici Matematice, Ed. Univ. Buc., ISBN 973575975-6, 2004.
5. D. Stinton, Cryptography, Theory and Practice, Chapman &Hall/CRC, Third Edition, 2006.
6. W. Stalings, Cryptography and Network Security: Principles and Practice (6th Edition)- 6th Edition, 2013.
7. FIPS 140-2, Security Requirements for Cryptographic Modules, 2001.
8. National Institute of Standards and Technologies, SP 800-22, A statistical test suite for random and pseudorandom number generators for cryptographic applications, 2010.

11. Evaluation

Activity type	11.1 Evaluation criteria	11.2 Evaluation methods	11.3 Percentage of final grade

11.4 Course	- knowledge of theoretical notions fundamentals; - knowing how to apply a theory to specific problems; - differential analysis of techniques and theoretical methods.	Scientific article and final exam	67%
11.5 Seminary/laboratory/project	- knowledge of the application, by examples concrete of the theoretical elements exemplified in the course.	Grading during the semester	33%
11.6 Passing conditions			
Obtaining 50% of the total score. Obtaining 50% of the score related to the activity during the semester.			

12. Corroborate the content of the course with the expectations of representatives of employers and representative professional associations in the field of the program, as well as with the current state of knowledge in the scientific field approached and practices in higher education institutions in the European Higher Education Area (EHEA)

Through the activities, students develop skills to offer solutions to problems and propose ideas to improve the situation of existence in the statistics field.

In the development of the content of the discipline, knowledge / aspects / phenomena described by specialized literature / published / presented own research.

Through the activities at the seminar, the aim is to develop the graduate's skills to manage practical situations that he may face in real life in order to increase his contribution to the improvement of the socio-economic environment.

Date	Course lecturer	Instructor(s) for practical activities
11.10.2024	Conf. Dr. Emil SIMION	Conf. Dr. Emil SIMION

Date of department approval

Head of department

Conf. dr. ing. Marian VLĂDESCU

Universitatea Națională de Știință și Tehnologie Politehnica București

Facultatea de Electronică, Telecomunicații și

Tehnologia Informației

Date of approval in the Faculty Council	Dean
01.11.2024	Prof. Dr. Mihnea Udrea