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	**Telecommunications**
1.4 Domain of studies	Electronic Engineering, Telecommunications and Information Technology
1.5 Cycle of studies	Bachelor/Undergraduate
1.6 Programme of studies	Networks and Telecommunications Software

2. Date despre disciplină

2.1 Course name (ro) (en)				Securitatea reţelelor şi serviciilor			
2.2 Course Lecturer				Conf. Dr. Octavian Catrina			
2.3 Instructor for practical activities				Conf. Dr. Octavian Catrina			
2.4 Year of studies	3	2.5 Semester	II	2.6. Evaluation type	V	2.7 Course regime	Op
2.8 Course type		S	2.9 Course code	04.S.06.A.227		2.10 Tipul de notare	Nota

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

3.1 Number of hours per week	3	Out of which: 3.2 course	2.00	3.3 seminary/laboratory	1
3.4 Total hours in the curricula	42.00	Out of which: 3.5 course	28	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.					5
Tutoring					0
Examinations					3
Other activities (if any):					0

3.7 Total hours of individual study	8.00
3.8 Total hours per semester	50
3.9 Number of ECTS credit points	2

4. Prerequisites (if applicable) (where applicable)

4.1 Curriculum	Calculus, Algebra, Computer Programming, Data Structures and Algorithms.

4.2 Results of learning	Basic knowledge of computer programming, especially algorithms and object-oriented programming (for the laboratory)

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

5.1 Course	Lecture hall equipped with video projector, screen, blackboard/whiteboard.
5.2 Seminary/ Laboratory/Project	Laboratory equipped with computers and video projector. The software used in the lab, JDK and Eclipse, runs on both WIndows and Linux and is free.

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 course aims at providing the students with specific knowledge and abilities needed for identifying, understanding, and solving a selection of security issues that are essential for the design and operation of communications networks and services. The course material focuses on the cryptographic algorithms and protocols needed to establish secure communication channels that provide authentication of the participants, data authentication, and data confidentiality:
- Cryptographic algorithms for data authentication and encryption based on symmetric (secret-key) cryptography and asymmetric (public-key) cryptography (security models, properties, examples).
- Security protocols that use these algorithms to establish secure channels, with authentication of the participants, establishment of cryptographic keys, and cryptographic protection of the exchanged data using authenticated encryption (security models, attacks, properties, examples).
The limited time available for lecture and laboratory allows only the introduction of basic concepts and the presentation of representative examples of algorithms and protocols. However, the material is selected and presented in such a way as to provide students with the knowledge necessary to understand the security requirements or properties and operation of existing systems, to use in practice the algorithms studied, and to examine and understand other algorithms of the same type.
To this end, the presented material focuses on the precise formulation of the security requirements and properties of fundamental components and types of cryptographic algorithms, using rigorous, established, but relatively simple mathematical models, thus avoiding specific details that cannot be presented in the time available (eg, a block cipher behaves like a pseudorandom permutation, and the internal operations are not relevant to analyzing the security of block cipher-based encryption or authentication algorithms). Similarly, representative types of constructions for security protocols are presented, which represent the cryptographic core of protocols used in practice and are relatively easy to analyze. Knowing these constructions, students can relatively easily understand the operation and security properties of the protocols used in practice.

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	This course extends the competences listed below with specific competences needed for satisfying the security requirements of the telecommunication networks: - Application of basic knowledge, concepts and methods regarding the architecture of computer systems, microcontrollers, programming languages and techniques. Students study security functions, cryptographic algorithms, and security protocols, and apply this knowledge during laboratory work to implement the security functions required by a generic messaging application. - A comprehensive view of data, voice, video, multimedia services, based on understanding and using the fundamental concepts in the field of communications and information transmission. Students study fundamental concepts and techniques needed by current telecommunications systems to provide cryptographic protection of communications (authentication of the participants and ensuring the data authenticity and confidentiality). - Selection, installation and operation of fixed or mobile telecommunications equipment and site design for common telecommunications networks.The discipline provides students with basic knowledge and skills specific to communications security, necessary to identify, understand and solve security issues involved in the design, configuration and operation of telecommunications networks and services.
Transversal (General) Competences	- Methodical analysis of the problems encountered in the activity, identifying the elements for which there are established solutions, and thus ensuring the fulfillment of professional tasks. - Ability to adapt to new technologies and to document oneself (in English and Romanian), for professional and personal development, through continuous training. - Ability to reason using scientific concepts and domain specific terminology, to independently explore and analyze information, as well as to find and present conclusions and/or solutions. - Ability to analyze and summarize the acquired knowledge by systematic analysis.

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.* - Know the rigorous definitions of domain-specific notions: security requirements, security functions, types of cryptographic algorithms, types of security protocols. -Know representative examples of cryptographic algorithms used for data encryption and authentication, using symmetric and asymmetric cryptography. - Know the security models and properties of these algorithms and how they are used to perform security functions so that security requirements are demonstrably met. - Know the representative constructions of security protocols for the authentication of participants and the establishment of the secret keys necessary for the cryptographic protection of data.

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).* - Identifies and formulates the basic security requirements of a telecommunications system regarding the authentication of participants and the authenticity and confidentiality of data. - Analyzes, describes and explains the operation and security properties of the components of a system that ensures the security of communications, using specific terminology. - Develops basic implementation solutions or configuration solutions for the security features mentioned above, ensuring that they meet the security requirements (satisfy the required security properties).
Responsability and autonomy	*The student's capacity to autonomously and responsably apply their knowledge and skills.* - Selects appropriate bibliographic sources and analyzes them. - Respects the principles of academic ethics (for example, correctly citing the bibliographic sources). - 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 or in solving problems. - Realizes the value of his contribution in the field of engineering to the identification of viable and sustainable solutions to solve problems in social and economic life (social responsibility). - Analyzes and capitalizes on business/entrepreneurial development opportunities in the field. - Demonstrates real-life situation management skills.

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.)*

The teaching process will use both expository (lecture) and conversational-interactive teaching methods, based on discovery learning models facilitated by direct and indirect exploration (experiment, demonstration, modeling), but also based on methods. action, such as exercise, hands-on activities and problem-solving.
The teaching activity will use lectures based on PowerPoint presentations illustrated with images and diagrams (scenarios, algorithms, protocols and attacks), so that the information is easy to understand and to assimilate (PowerPoint presentations are supplemented with examples built interactively on the board). The introductory presentations of the courses and laboratory papers highlight the connection with the notions presented earlier.
In the lab, the students make a simple message communication application, starting from an initial application that does not offer any security service and successively adding additional security functions, as they are presented in the course. The application is implemented in the Java language, using the standard library of cryptographic classes provided by the Java Cryptography Architecture (JCA), which is documented in detail and is easy to use. Students use an advanced integrated programming environment, Eclipse, which substantially facilitates program development and testing (https://www.eclipse.org/). Both the Eclipse integrated programming environment and the cryptographic libraries used are available free of charge and students can easily install them on their own computer.

10. Contents

COURSE

Chapter	Content	No. hours
1	Introduction to communications security. Vulnerabilities, threats, security functions.	4
2	Data confidentiality (I): Definitions. Security models for data confidentiality (types of attacks, computational security, formal security requirements).	2
3	Data confidentiality (II): Introduction to secret-key encryption: Block ciphers (definition, security properties, AES algorithm). Secret-key encryption schemes based on block ciphers.	3
4	Data confidentiality (III): Introduction to public key encryption. One-way trapdoor functions. RSA public-key encryption.	3
5	Data authetication (I): Definitions. Security models for data authentication (types of attacks, security requirements). Cryptographic hash functions: security properties and examples.	3
6	Data authetication (II): Introduction to secret-key data authentication. Constructions based on block ciphers and hash functions. Authenticated encryption. Examples of applications in communications (secure channels).	3
7	Data authetication (III): Introduction to public-key data authentication. RSA digital signature.	2
8	Security protocols (I): Secure communication channels (challenges, security requirements). Public-key certificates. Introduction to public-key infrastructures (PKI)	3
9	Security protocols (II): Authentication protocols: elementary constructions and attacks.	2
10	Security protocols (III): Protocols for establishing secret keys (authenticated key exchange)28: elementary constructions and attacks. Examples of protocols used in practice.	3
	Total:	28

Bibliography:

Catrina Octavian, Networks and Services Security, electronic course support (Moodle platform): https://curs.upb.ro/2021/course/view.php?id=9688
Catrina Octavian. Cryptographic Algorithms and Protocols. MATRIX ROM, Bucharest, 2016. ISBN 978-606-25-0249-2.
Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996, 2001. Available online: http://cacr.uwaterloo.ca/hac/
The specifications of the cryptographic algorithms studied in the course are available online in the NIST publications (National Institute of Standards and Technology, USA): https://www.nist.gov/

LABORATORY

Crt. no.	Content	No. hours
1	Confidential communications using secret-key encryption (SeCom1 application). Students extend an application that does not provide security services, called SeCom0, to protect the confidentiality of the transmitted data using secret-key encryption. The application will use for this purpose predefined secret keys.	2

2	Secret-key transport using public-key encryption (SeCom2). The students develop the application SeCom2 (by modifying SeCom1) so that each communication session uses a different secret key instead of a pre-shared key. When a session begins, a user generates a new secret key and sends it to the other user, protecting its confidentiality using RSA public-key encryption. The RSA public key is distributed in advance.	2
3	Secret-key data authentication and authenticated encryption (SeCom3). The students develop the application SeCom3 (by modifying SeCom1) that provides message authentication using secret-key cryptography (message authentication code). A first variant, SeCom3A only provides data authentication. The second variant, SeCom3AE, provides both data authentication and data confidentiality, using authenticated encryption.	2
4	Public-key data authentication and public-key infrastructure (SeCom4). The students develop the application SeCom4 (by extending SeCom0) that provides message authentication using public-key cryptography (digital signature). The public keys are distributed using public-key certificates. To this end, the students set up a basic public-key infrastructure (certification authority that issues certificates to users).	2
5	Authenticated key exchange based on secret-key cryptography (SeCom5). The students develop the application SeCom5 (by extending SeCom3AE), so that session keys can be set up using a protocol based private-key cryptography protocol (pre-shared secret keys, message authentication code).	2
6	Authenticated key exchange based on public-key cryptography (SeCom6). The students develop the application SeCom6, by modifying SeCom5, to enable session key establishment using a protocol based on public-key cryptography (Diffie-Hellmann with authentication based on signatures and certificates).	2
7	Final lab examination.	2
	Total:	14

Bibliography:

Catrina Octavian, Networks and Services Security, Lab descriptions (and initial Java projects) (Moodle): https://curs.upb.ro/2021/course/view.php?id=9688
The documentation of the software libraries used in the lab is available online: Java Cryptography Architecture Reference Guide, documentation of the Java standard cryptographic classes.

11. Evaluation

Activity type	11.1 Evaluation criteria	11.2 Evaluation methods	11.3 Percentage of final grade
11.4 Course	Knowledge of concepts, methods, cryptographic algorithms and security protocols studied in the course.	Verification papers during the semester	30%
	Application of this knowledge to understand and solve basic communications security problems encountered in practice.	Verification papers during the semester	30%

11.5 Seminary/laboratory/project	Analysis, design, implementation and testing of basic communications security applications, based on examples made during laboratory work.	Oral, practical examination. Analysis and implementation of the developed applications.	40%
11.6 Passing conditions			
The students must obtain minimum of 50/100 for the verification papers and minimum 50/100 for the laboratory examination.			

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)

The global communication infrastructure based on the Internet and wireless networks must deal with new and challenging security issues. The success of major, emerging classes of applications, for instance in the area of the Internet of Things and information systems embedded in vehicles, relies to a large extent on the fulfillment of strict and complex security requirements.
The security technologies and protocols presented in this course play an essential role in addressing these issues and, therefore, have become ubiquitous components of current information and communication systems.
The IT industry has a high demand for qualified engineers able to competently handle security aspects of their systems, networks, and applications, with a solid foundation in electronics, communication technology, and information security.

Date	Course lecturer	Instructor(s) for practical activities
10.10.2024	Conf. Dr. Octavian Catrina	Conf. Dr. Octavian Catrina

Date of department approval	Head of department
22.10.2024	Conf. Dr. Serban Georgica Obreja

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

Universitatea Națională de Știință și Tehnologie Politehnica București

Facultatea de Electronică, Telecomunicații și

Tehnologia Informației