**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 | Masters |
| 1.6 Programme of studies | Advanced Wireless Communications |

## 2. Date despre disciplină

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2.1 Course name (ro)<br>(en) | | | | Algoritmi criptografici pentru comunicații wireless<br>Cryptographic Algorithms for Wireless Communications | | | |
| 2.2 Course Lecturer | | | | Conf. Dr. Octaviana DATCU, Prof. Dr. Calin Vladeanu | | | |
| 2.3 Instructor for practical activities | | | | Conf. Dr. Octaviana DATCU, Prof. Dr. Calin Vladeanu | | | |
| 2.4 Year of studies | 1 | 2.5 Semester | II | 2.6. Evaluation type | E | 2.7 Course regime | Ob |
| 2.8 Course type | | DS | 2.9 Course code | UPB.04.M2.O.21-05 | | 2.10 Tipul de notare | Nota |

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

| | | | | | |
|---|---|---|---|---|---|
| 3.1 Number of hours per week | 2.5 | Out of which: 3.2 course | 1.50 | 3.3 seminary/laboratory | 1 |
| 3.4 Total hours in the curricula | 35.00 | Out of which: 3.5 course | 21 | 3.6 seminary/laboratory | 14 |
| Distribution of time: | | | | | hours |
| Study according to the manual, course support, bibliography and hand notes<br>Supplemental documentation (library, electronic access resources, in the field, etc)<br>Preparation for practical activities, homework, essays, portfolios, etc. | | | | | 57 |
| Tutoring | | | | | 0 |
| Examinations | | | | | 8 |
| Other activities (if any): | | | | | 0 |

| | |
|---|---|
| 3.7 Total hours of individual study | 65.00 |
| 3.8 Total hours per semester | 100 |
| 3.9 Number of ECTS credit points | 4 |

## 4. Prerequisites (if applicable) (where applicable)

| | |
|---|---|
| 4.1 Curriculum | The student is familiar with at least one programming language. Example:Python, Matlab. |
| 4.2 Results of learning | Basic notions of signal processing. |

**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 laboratory will take place in a room equipped with computers. |

**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 lectures and the laboratory work are aimed at enabling students to accumulate knowledge about the basics of cryptanalysis. The accumulated knowledge is relevant nowadays in the academic, industrial and economic context, where the exchange of sensitive information is increasing.

**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** | The students:<br>• know, understand and use the language specific to the field;<br>• correlate the knowledge specific to the domain of cryptography with that of others disciplines belonging to the area of electronic engineering, telecommunications and technologies informational.<br>• apply standardized, specific knowledge, methods and tools in practice field, for carrying out the evaluation and diagnosis process of a situations, depending on the reported problems and identify solutions.<br>• argue and analyze coherently and correctly the context of application a basic knowledge of the field, using key concepts of the discipline and specific methodology.<br>• use the scientific vocabulary specific to the field, to communicate effectively, in written and oral. |

| | |
|---|---|
| **Transversal (General) Competences** | • Students:<br>• work in person and communicate effectively, coordinating efforts with other colleagues at solving problematic situations of medium complexity.<br>• have autonomy and critical thinking: the ability to think in scientific terms, to search and analyze data independently, as well as extract and present conclusions / identification of solutions.<br>• have the ability to analyze and synthesize the knowledge acquired along the way synthetic, following a systematic process of analysis.<br>• respect the principles of academic ethics: correctly cites in the completed documentation the bibliographic sources used. puts into practice elements of emotional intelligence in managing the context socio-emotional.<br>• behave appropriately in 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.*<br>The students:<br>• list the most important stages that marked the development of the field.<br>• define domain-specific notions.<br>• describe and apply concepts/processes/algorithms.<br>• highlight the consequences and relationships between algorithms. |
| **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).*<br>The students:<br>• comparatively describe the learned algorithms and methods.<br>• implement Caesar's encryption algorithm for text encryption and decryption.<br>• implement the algorithm to crack Caesar's cipher.<br>• implement the Vigenere cipher for text encryption and decryption.<br>• implement the algorithms to break Vigenere's cipher.<br>• implement Baptista's cipher for image encryption and decryption.<br>• implement algorithms for metrics that evaluate the quality of encryption and decryption on images. |

| | |
|---|---|
| **Responsability and autonomy** | *The student's capacity to autonomously and responsably apply their knowledge and skills.*<br>The students:<br>• select appropriate bibliographic sources and analyze them. respect the principles of academic ethics, correctly citing the bibliographic sources used. demonstrate responsiveness to new learning contexts.<br>• demonstrate collaboration with other colleagues and teaching staff in carrying out the activity didactic.<br>• demonstrate autonomy in organizing the learning situation/context or situation problem it solves.<br>• demonstrate social responsibility through active involvement in student social life/ involvement in the events of the academic community.<br>• promote/contribute new solutions related to area of expertise for improvement the quality of social life.<br>• are aware of the value of their contribution to the field of engineering and to the identification of solutions viable/sustainable for solving problems in social and economic life (social responsibility).<br>• apply the principles of professional ethics/deontology in the analysis of the technological impact of the solutions proposed in the field specific to the environment.<br>• analyze and capitalizes on business/entrepreneurial development opportunities in the field specialty. demonstrate skills in managing real-life situations (time management, collaboration vs. conflict). |

**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 the learning characteristics of the students and their specific needs, the teaching process will explore both expository (lectures, exposition) and interactive conversational teaching methods based on learning models by discovering the facility of direct and indirect exploration of reality (experiment, demonstration, modelling), but also on action-based methods, such as exercises, activities practice and problem solving. Lectures based on Power Point presentations or various videos will be used in the didactic activity which will be made available to students. Each course will begin with a recap of the chapters covered, with focus on the concepts covered in the last course. The presentations use images and diagrams so that the information presented is easy to understand and assimilate. This topic covers information and practical activities designed to support students in their learning endeavours and the development of optimal collaboration and communication relationships in a climate conducive to learning through discovery. Practice of active listening and assertive communication skills as well as mechanisms will be considered of feedback construction, as ways to regulate behavior in various situations and to adapt of the pedagogical approach to the students' learning needs. Teamwork skills will be practiced to solve different learning tasks.

**10. Contents**

| **COURSE** | | |
|---|---|---|
| **Chapter** | **Content** | **No. hours** |
| 1 | Cryptology - terminology and basic notions [1 - 5]. | 2 |
| 2 | Symmetric key cryptography, using [1 - 3]. | 3 |
| 3 | Public key cryptography using [7]. | 3 |

| | | |
|---|---|---|
| 4 | Symmetric key cryptanalysis using [2 - 5]. | 3 |
| 5 | Public key cryptanalysis using [7]. | 3 |
| 6 | Analysis of image decryption quality, using [8]. | 3 |
| 7 | Relevant topics related to cryptography - cryptoeconomics, digital management rights. | 2 |
| 8 | Preparation for the exam. | 2 |
| | **Total:** | 21 |

**Bibliography:**

Bibliography:
[1] Caesar's cipher, mentioned in paragraph 56 of 'SVETONI TRANQVILII VITA DIVI IVLI', online at http://thelatinlibrary.com/suetonius/suet.caesar.html#56 on 28th of February 2021.
[2] Breaking Caesar's cipher, available online at https://en.wikipedia.org/wiki/Caesar_cipher on 7.03.2022.
[3] MA/CS358 Cryptography, Automating Vigenère Cipher Cracking, online at https://macs358.org/chapters/08/4/find-keylength-with-ic#Determining-the-Key-Length-using-Index-of-Coincidence, October 2024
[4] Henk C.A. van Tilborg, ed. (2005). Encyclopedia of Cryptography and Security(First ed.). Springer. p. 115. ISBN 0-387-23473-X.
[5] Practical Cryptography, online at http://practicalcryptography.com/cryptanalysis/text-characterisation/chi-squared-statistic/, October 2024.
[6] MS Baptista, Physics letters A 240 (1-2), 50-54, online at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.476.9974&rep=rep1&type=pdf, October 2024.
[7] Imam, Raza, et al. "Systematic and critical review of RSA based public key cryptographic schemes: Past and present status." IEEE Access 9 (2021): 155949-155976.
[8] Mahendiran, N., and C. Deepa. "A comprehensive analysis on image encryption and compression techniques with the assessment of performance evaluation metrics." SN Computer Science 2.1 (2021): 29.
[9] Ferdous, Md Sadek, Mohammad Jabed Morshed Chowdhury, and Mohammad A. Hoque. "A survey of consensus algorithms in public blockchain systems for crypto-currencies." Journal of Network and Computer Applications 182 (2021): 103035.

**LABORATORY**

| Crt. no. | Content | No. hours |
|---|---|---|
| 1 | Implementation of Caesar's and Vigenere's ciphers, using [1, 3, 4, 5]. | 4 |
| 2 | Cryptanalysis of Caesar and Vigenere ciphers, using [2 - 5]. | 4 |
| 3 | Comparative analysis of image decryption quality using own implementation a Baptista's cryptosystem and the implementation of another given algorithm using [6, 7]. | 4 |
| 4 | Colloquium. | 2 |
| | **Total:** | 14 |

**Bibliography:**
[1] Caesar's cipher, mentioned in paragraph 56 of 'SVETONI TRANQVILII VITA DIVI IVLI', online at http://thelatinlibrary.com/suetonius/suet.caesar.html#56 on 28th of February 2021.
[2] Breaking Caesar's cipher, available online at https://en.wikipedia.org/wiki/Caesar_cipher on 7.03.2022.
[3] MA/CS358 Cryptography, Automating Vigenère Cipher Cracking, online at https://macs358.org/chapters/08/4/find-keylength-with-ic#Determining-the-Key-Length-using-Index-of-Coincidence, October 2023.
[4] Henk C.A. van Tilborg, ed. (2005). Encyclopedia of Cryptography and Security(First ed.). Springer. p. 115. ISBN 0-387-23473-X.
[5] Practical Cryptography, online at http://practicalcryptography.com/cryptanalysis/text-characterisation/chi-squared-statistic/, October 2023.
[6] MS Baptista, Physics letters A 240 (1-2), 50-54, online at http://citeseerx.ist.psu.edu/viewdoc/download? doi=10.1.1.476.9974&rep=rep1&type=pdf, October 2024.
[7] Mahendiran, N., and C. Deepa. "A comprehensive analysis on image encryption and compression techniques with the assessment of performance evaluation metrics." SN Computer Science 2.1 (2021): 29.

**11. Evaluation**

| Activity type | 11.1 Evaluation criteria | 11.2 Evaluation methods | 11.3 Percentage of final grade |
|---|---|---|---|
| 11.4 Course | • knowledge terminology used in cryptology.<br>• appropriate use A notions from cryptology.<br>• understanding basic principles of algorithms in cryptology.<br>• the ability to build and analyze figures more complexity starting from basic algorithms. | Written exam - Matlab implementations/ Python and theoretical aspects - Moodle assignment. | 40 |
| 11.5 Seminary/laboratory/project | | Homework (Moodle assignments) and colloquium - Matlab implementations/ Python and theory. | 60 |
| 11.6 Passing conditions | | | |

The students must be able to:

- answer specific questions such as what is a cipher, what is the difference between encryption and encryption, what is a secret key/public key cryptosystem, what does a cipher mean single/multiple substitution.
- how a simple substitution cipher like Caesar's cipher works - the algorithm and how to implement the software that implements it.
- how a simple substitution cipher can be attacked.
- apply cryptanalytic attacks: brute force (ciphertext only), known plaintext (or ciphertext), statistical cryptanalysis, frequency attacks.

**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 activities, students develop their skills in providing solutions to problems and proposing ideas for improvement of the existing situation in the field of advanced wireless communications. The course has similar content to the courses offered by the Massachusetts Institute of Technology in Cambridge, Massachusetts. Through laboratory and course activities, the development of management skills is achieved the master's degree considering practical situations that students can face in real life to increase their contribution to the improvement of the socio-economic environment.

| Date | Course lecturer | Instructor(s) for practical activities |
|---|---|---|
| | Conf. Dr. Octaviana DATCU, Prof. Dr. Calin Vladeanu | Conf. Dr. Octaviana DATCU |
| | | Prof. Dr. Calin Vladeanu |

| Date of department approval | Head of department |
|---|---|
| 27.10.2024 | Conf. Dr. Serban Georgica Obreja |

**Universitatea Națională de Știință și Tehnologie Politehnica București**

**Facultatea de Electronică, Telecomunicații și**

**Tehnologia Informației**

| | |
|---|---|
| Date of approval in the Faculty Council | Dean |
| 25.10.2024 | Prof. Dr. Mihnea Udrea |