POLITEHNICA University of Bucharest
Facultyof Electronics, Telecommunications andInformation Technology

COURSE DESCRIPTION

1. Program identification information

1.1 Higher education institution	POLITEHNICA University of Bucharest
1.2 Faculty	Electronics, Telecommunications and Information Technology
1.3 Department	Applied Electronics and Information Technology
1.4 Domain of studies	Computers and Information Technology
1.5 Cycle of studies	License
1.6 Program of studies/Qualification	Information engineering

2. Course identification information

2.1 Name of the course				**Cryptography and Data Protection**			
2.2 Lecturer				Prof. Dr. ing. Adriana VLAD			
2.3 Instructor for practical activities				S.l. Dr. ing. Mădălin FRUNZETE			
2.4 Year of studies	IV	2.5 Semester	II	2.6 Evaluation type	Verification	2.7 Course choice type	Mandatory

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

3.1 Number of hours per week,out of which	3	3.2 course	2	3.3 practical activities	1
3.4 Total hours in the curricula, out of which	42	3.5 course	28	3.6 practical activities	14

Distribution of time	hours
Study according to the manual, course support, bibliography and hand notes	25
Supplemental documentation (library, electronic access resources, in the field, etc)	3
Preparation for practical activities, home works, essays, portfolios, etc.	5
Tutoring	0
Examinations	3
Other activities	0

3.7 Total hours of individual study	36
3.9 Total hours per semester	78
3. 10 Number of ECTS credit points	3

4. Prerequisites (if applicable)

4.1 curricular	Information Transmission Theory Special Mathematics, Data Structures and Algorithms.
4.2 competence-based	It is complementary to disciplines related to information processing in large computer networks.

5. Requisites (if applicable)

5.1 for running the course	There is no case.
5.2 for running of the applications	Mandatory attendance at laboratories (according to the regulations of the UPB).

6. Specific competences

Professional competences	Mastering the theoretical foundations that allow understanding the functioning of a cryptosystem, and knowledge of the most important methods and practical interest cryptosystems. To develop the ability to design new efficient encryption systems. *Knowledge skills*: C3.1 Identify the problems of the domain and the solving methods, specific to information systems; C3.2 Use of interdisciplinary knowledge, the patterns of theoretical solutions and tools, performing experiments and interpreting their results.
Transversal competences	Use in practice of various and complex knowledge and concepts drawn from subjects studied in Faculty of Electronics, Telecommunications and Information Technology (information transmission theory, random processes, programming, special mathematics, computer networks, image processing, etc.) *Practical skills:* C3.4 Comparative evaluation (by theoretical and experimental means) of different solutions in order to optimize performance. C3.5 Developing and implementing computational solutions for practical problems.

7. Course objectives (as implied by the grid of specific competences)

7.1 General objective of the course	The course is a comprehensive overview of secret and public key cryptosystems, aiming at: (1) providing the student with skills in understanding, evaluating and designing enciphering algorithms and other protection techniques; (2) extending the enciphering methods in other fields (images coding, complex algorithms) and also for other purposes (the natural language modelling, the highlighting and evaluation of the entropy and redundancy of natural sources, the generation of pseudorandom numbers).
7.2 Specific objectives	The students are involved both in theoretical evaluations and in software implementation of various algorithms of conventional and public cryptography. The implementation requires knowledge of several areas of mathematics and also some familiarity with computational complexity.

8. Content

8.1 Lectures	Teaching techniques	Remarks
Basic principles of classical and public–key cryptosystems.	Teaching is based on theoretical foundations exposure in mixed mode using both blackboard and projector (covering communication function and demonstration). Course materials are lecture notes and presentations, issues and themes proposed (theoretical and solving problems using the computer), and various articles and extracts from the bibliography.	2 hrs
Shannon's approach to the classical cryptosystems: • secrecy system equivocation as a measure of the secrecy amount on the message and on the key space; perfect and ideal cryptosystems; illustrative examples . • the redundancy of the language and the breaking of the cryptosystems; the unicity distance; cryptanalytic attacks; an overall evaluation of a secrecy system from the practical demand. • product ciphers; diffusion, confusion and the mixing transformations; practical ciphers.		12 hrs
DES (Data Encryption Standard); **AES (Advanced Encryption Standard)**		4 hrs
Public–key cryptosystems, including: M. E. Hellman's contributions, underlying the mathematical theory, the public–key distribution, public–key cryptosystems (the RSA and knapsack based systems), authentication and digital signature.		8 hrs
Chaos-based cryptography.		2 hrs

Bibliography

1. Adriana Vlad, *Lecture notes.*
2. C.E. Shannon, "*Communication Theory of Secrecy Systems*", Bell Systems Technical Journal, 28 (1949), 656-715.
3. W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory, 22 (1976), 644-654.
4. I. Angheloiu, E. Györfi şi V. Patriciu, *Securitatea şi protecţia informaţiei în sistemele electronice de calcul*, Ed. Militară, Bucureşti, 1986.
5. Nicolae Constantinescu, *Criptografie*, Editura Academiei Romane, 2009
6. Douglas R. Stinson, *Cryptography: Theory and Practice*, Third Edition, Chapman and Hall/CRC - November 01, 2005
7. V. Patriciu, *Criptografia şi securitatea reţelelor de calculatoare cu aplicaţii în C şi Pascal*, Ed. Tehnică, Bucureşti, 1994.
8. Adriana Vlad, M. Mitrea, "*A Study of Confusion Involved by Shannon's Mixing Transformations*", Buletinul Ştiinţific al Universităţii "Politehnica" din Bucureşti, Seria C, Vol. **57-58**, Nr. **1-4**, (1995-1996), pp. 55-64.
9. Adriana Vlad, M. Mitrea, "*Image Enciphering by Means of Cryptographic Mixing Transformations*", Buletinul ştiinţific al Universităţii "Politehnica" din Timişoara, Tom

43(**57**), Fasc. **2**, (1998), pp. 185-190.
10. Adriana Vlad, M. Mitrea, "*Cryptographic Mixing Transformations forImage Applications*", Proc. SPIE, Vol. **3405**, (1997), pp. 477-482.
11. Adriana Vlad, M. Mitrea *"Digital image – protection by means of cryptographic mixing transformations"* Proc. SPIE, Vol. **4430**, (2000), pp. 560-565.
12. Adriana Vlad, A. Luca, O. Hodea, R. Tataru, "Generating chaotic secure sequences using tent map and a running-key approach", Proc. of the Romanian Academy, Series A, vol.14, Special Issue-CRYPTOLOGY SCIENCE, pp.265-302, 2013.

8.2 Practical applications	Teaching techniques	Remarks
Design and software implementation of the enciphering method and their cryptanalytic evaluation. Case study: substitutions methods, transposition methods, mixing transformation based ciphers, data encryption standard (DES).	Teaching is based on the use of the projector (covering communication function and demonstration) and on oral communication method . Students will independently simulate, implement, test and evaluate cryptography problems with secret/public key by using a software environment. The teaching materials are laboratory platforms.	6 hrs
Software implementation and analysis of some public key cryptosystems: RSA cryptosystems, knapsack based systems, Hash functions, authentication and digital signature.		6 hrs
Laboratory assessment		2 hrs

Bibliography

1. M. Mitrea, Adriana Vlad, A. Branea, *"The m-gram Substitution in the Cryptographic Mixing Transformation Applied to Images"*, in Proc. Intl. Symp. on Signal, Circuits & Systems - SCS'99, July 1999, Iaşi, pp. 151-155.
2. Adriana Vlad, A. Mitrea, M. Mitrea, *Limba română scrisă ca sursă de informatie (Printed Romanian, as an information source)*, Ed. Paideia, Bucureşti, 2003.
3. M.S. Baptista, "*Cryptography with chaos*" Physics Letters A, vol. 240 (1998) 50-54.
4. Adriana Vlad, A. Ilyas, A. Luca, "A closer view of running-key cipher on natural languages and its extension for new applications in cryptography", Proc. of the Romanian Academy, Series A, vol. 13, Number 2/2012, pp. 157–166.

9. Bridging the course content with the expectations of the epistemic community representatives, professional associations and employers representatives for the domain of the program

Cryptography was and continues to be an interdisciplinary domain, of great interest and actuality, targeting information confidentiality and protection. Indirectly and at the same time very important for the scientific research in the world, these concerns create a space, an extended working platform, connecting extremely diverse fields and working techniques, while revealing new aspects for the benefit of science in general. The scientific meetings in this field are relevant in this respect, including the two editions of the conference "Romanian Cryptology Days", RCD 2011 and RCD 2013, which created an international forum for the exposition/debate of problems and applications.

The course curriculum concretely responds to these actual development requirements, subscribed to the European economy of services from Computers and Information Technology (CIT). In the context of the present technological progress, cryptography and data protection represent important concerns of the electronic industry both from the point of view of devices/systems and of the algorithms. The robustness of cipher depends on the computational power, and this course permits students' adaptation

and innovation towards new algorithms.
Students are provided with adequate skills required by the needs of present qualifications and a high quality and competitive scientific and technical training, which should enable them to easily find a job immediately after graduation; the training is perfectly adapted to the policy of the POLITEHNICA University of Bucharest both as regards its content and structure and from the point of view of aptitudes and international openness offered to students.

10. Evaluation

Type of activity	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Weight in the final mark
10.4 Lectures	- Knowledge of basic theoretical concepts - Knowledge of the application of theory to specific problems	Two check tests representing 20% each of the final score during the semester, on previously established dates. A theme representing 30% of the final score, under the form of oral presentation.	70%
10.5 Practical applications	- Knowledge of the functioning of the studied encryption algorithms. - The ability to implement an encryption algorithm. - Understanding the principle of secret / public cryptography, Highlighting the concept of secret signature.	Final laboratory examination, including a theoretical (grid test) and a practical exercise (implementing an encryption algorithm).	30%
10.6 Minimal performance standard			
- Making a secret key encryption algorithm, understanding the unique correspondence between message and cryptogram - Understanding the principle of secret key cryptography and public key digital signature highlighting			

Date	Lecturer	Instructor for practical activities
.....	Prof. Dr. ing. Adriana VLAD	S.l. Dr. ing. Mădălin FRUNZETE

Date of department approval — Director of Department,

..... — Prof. Dr. Ing. S. Paşca.