

SYLLABUS

1. Information regarding the programme

1.1 Higher education institution	Babeş-Bolyai University
1.2 Faculty	Faculty of Mathematics and Computer Science
1.3 Department	Department of Computer Science
1.4 Field of study	Computer Science
1.5 Study cycle	Bachelor
1.6 Study programme / Qualification	Computer Science

2. Information regarding the discipline

2.1 Name of the discipline	Public-Key Cryptography						
2.2 Course coordinator	Prof.PhD. Septimiu Crivei						
2.3 Seminar coordinator	Prof.PhD. Septimiu Crivei						
2.4. Year of study	3	2.5 Semester	5	2.6. Type of evaluation	C	2.7 Type of discipline	Optional

3. Total estimated time (hours/semester of didactic activities)

3.1 Hours per week	3	Of which: 3.2 course	2	3.3 seminar/laboratory	1
3.4 Total hours in the curriculum	42	Of which: 3.5 course	28	3.6 seminar/laboratory	14
Time allotment:					hours
Learning using manual, course support, bibliography, course notes					14
Additional documentation (in libraries, on electronic platforms, field documentation)					8
Preparation for seminars/labs, homework, papers, portfolios and essays					14
Tutorship					14
Evaluations					8
Other activities:					0
3.7 Total individual study hours	58				
3.8 Total hours per semester	100				
3.9 Number of ECTS credits	4				

4. Prerequisites (if necessary)

4.1. curriculum	•
4.2. competencies	•

5. Conditions (if necessary)

5.1. for the course	•
5.2. for the seminar /lab activities	•

6. Specific competencies acquired

Professional competencies	<ul style="list-style-type: none"> • C1.5 Development of program units and corresponding documentation • C3.3 Use of computer science and mathematical models and tools for solving specific problems in the application field
----------------------------------	--

Transversal competencies	<ul style="list-style-type: none"> CT2 Efficient fulfillment of organized activities in an inter-disciplinary group and development of empathic abilities of inter-personal communication, relationship and collaboration with various groups
---------------------------------	--

7. Objectives of the discipline (outcome of the acquired competencies)

7.1 General objective of the discipline	<ul style="list-style-type: none"> To present mathematical algorithms used in public-key cryptography.
7.2 Specific objective of the discipline	<ul style="list-style-type: none"> Number-theoretic and algebra algorithms will be studied and implemented in projects.

8. Content

8.1 Course	Teaching methods	Remarks
1. Classical cryptography. Examples	interactive exposure, explanation, didactical demonstration	
2. Public-key cryptography	interactive exposure, explanation, didactical demonstration	
3. Algorithm complexity	interactive exposure, explanation, didactical demonstration	
4. Congruences	interactive exposure, explanation, didactical demonstration	
5. Primes, quadratic residues	interactive exposure, explanation, didactical demonstration	
6. Algorithms for testing primality	interactive exposure, explanation, didactical demonstration	
7. Factorization algorithms for integers I	interactive exposure, explanation, didactical demonstration	
8. Factorization algorithms for integers II	interactive exposure, explanation, didactical demonstration	
9. Rabin public-key cryptosystem	interactive exposure, explanation, didactical demonstration	
10. ElGamal public-key cryptosystem, finite fields	interactive exposure, explanation, didactical demonstration	
11. Factorization of polynomials: Berlekamp's algorithm	interactive exposure, explanation, didactical demonstration	
12. Discrete logarithms	interactive exposure, explanation, didactical demonstration	
13. Practical aspects of public-key cryptosystems I	interactive exposure, explanation, didactical demonstration	
14. Practical aspects of public-key cryptosystems II	interactive exposure, explanation, didactical demonstration	

Bibliography

- S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to cryptography and coding theory, Editura EFES, 2006.
- C. Gherghe, D. Popescu, Criptografie. Coduri. Algoritmi, Editura Univ. Bucuresti, 2005.
- N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.
- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography. CRC Press, Boca Raton, 1997. (<http://www.math.uwaterloo.ca/~ajmenez>)
- B. Schneier, Applied Cryptography. John Wiley & Sons, 1996.

8.2 Laboratory	Teaching methods	Remarks
1. Classical cryptography	interactive exposure,	The lab is scheduled as 2

	algorithmization	hours every second week
2. Algorithm complexity	interactive exposure, algorithmization	
3. Modular arithmetics	interactive exposure, algorithmization	
4. Algorithms for testing primality	interactive exposure, algorithmization	
5. Factorization algorithms	interactive exposure, algorithmization	
6. Public-key cryptography	interactive exposure, algorithmization	
7. Practical aspects of public-key cryptosystems	interactive exposure, algorithmization	

Bibliography

1. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to cryptography and coding theory, Editura EFES, 2006.
2. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography. CRC Press, Boca Raton, 1997. (<http://www.math.uwaterloo.ca/~ajmeneze>)
3. B. Schneier, Applied Cryptography. John Wiley & Sons, 1996.

9. Corroborating the content of the discipline with the expectations of the epistemic community, professional associations and representative employers within the field of the program

- The contents is directed towards practical applications of public-key cryptography. The topic is present in the computer science study programme of all major universities.

10. Evaluation

Type of activity	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Share in the grade (%)
10.4 Course	Use of basic concepts in examples	Assessments	50
10.5 Lab	Implement course concepts and algorithms	Practical examination	50
10.6 Minimum performance standards			
➤ Grade 5			

Date 30.04.2016 Signature of course coordinator
Prof.PhD. Septimiu CRIVEI

Signature of seminar coordinator
Prof.PhD. Septimiu CRIVEI

Date of approval

Signature of the head of department
Prof.PhD. Octavian AGRATINI