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	e dis	iscipline Public-Key Cryptography					
2.2 Course coor	rdin	ator	Prof.PhD. Septimiu Crivei				
2.3 Seminar coordinator Prof.PhD. Septimiu Crivei							
2.4. Year of	3	2.5	5	2.6. Type of	C	2.7 Type of	Optional
study		Semester		evaluation		discipline	_

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

et i otal estillatea tille (noais/sellies		1 0100000000000000000000000000000000000				
3.1 Hours per week	3	Of which: 3.2 course	2	3.3	1	
				seminar/laboratory		
3.4 Total hours in the curriculum	42	Of which: 3.5 course	28	3.6	14	
				seminar/laboratory		
Time allotment:						
Learning using manual, course support, bibliography, course notes						
Additional documentation (in libraries, on electronic platforms, field documentation)						
Preparation for seminars/labs, homework, papers, portfolios and essays						
Tutorship						
Evaluations						
Other activities:						
0.5 m - 11 11 11 1 - 1 1		=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

ofessional	mpetencies
Pro	com

- 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

• 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	To present mathematical algorithms used in public-key cryptography.
7.2 Specific objective of the discipline	 Number-theoretic and algebra algorithms will be studied and implemented in projects.

8. Content

8.1 Course	Teaching methods	Remarks
Classical cryptography. Examples	interactive exposure, explanation, didactical demonstration	
2. Algorithm complexity, elements of number theory	interactive exposure, explanation, didactical demonstration	
3. Public-key cryptography. RSA	interactive exposure, explanation, didactical demonstration	
4. Algorithms for testing primality	interactive exposure, explanation, didactical demonstration	
5. Algorithms for factoring integers	interactive exposure, explanation, didactical demonstration	
6. Quadratic residues. Rabin public-key cryptosystem	interactive exposure, explanation, didactical demonstration	
7. Polynomials. Finite fields	interactive exposure, explanation, didactical demonstration	
8. ElGamal public-key cryptosystem	interactive exposure, explanation, didactical demonstration	
9. Algorithms for computing discrete logarithms	interactive exposure, explanation, didactical demonstration	
10. Factorization of polynomials: Berlekamp's algortihm	interactive exposure, explanation, didactical demonstration	
11. Digital signatures	interactive exposure, explanation, didactical demonstration	
12. Key-related protocols	interactive exposure, explanation, didactical demonstration	
13. Practical aspects of public-key cryptosystems	interactive exposure, explanation, didactical demonstration	
14. Eliptic-curve cryptography	interactive exposure, explanation, didactical demonstration	

Bibliography

- 1. M. Cozzens, S.J. Miller, The Mathematics of Encryption: An Elementary Introduction, American Mathematical Society, 2013.
- 2. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to coding theory and cryptography, Editura EFES, Cluj-Napoca, 2006.
- 3. C. Gherghe, D. Popescu, Criptografie. Coduri. Algoritmi, Editura Univ. Bucuresti, 2005.
- 4. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997. [http://www.cacr.math.uwaterloo.ca/hac]
- 5. C. Paar, J. Pelzl, Understanding Cryptography, Springer, 2009.

		c j_1 c j j j	,	
8.2 Laborator	У		Teaching methods	Remarks

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. Algorithms for factoring integers	interactive exposure,	
	algorithmization	
6. Public-key cryptography	interactive exposure,	
	algorithmization	
7. Practical aspects of public-key cryptosystems	interactive exposure,	
	algorithmization	

Bibliography

- 1. M. Cozzens, S.J. Miller, The Mathematics of Encryption: An Elementary Introduction, American Mathematical Society, 2013.
- 2. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to coding theory and cryptography, Editura EFES, Cluj-Napoca, 2006.
- 3. C. Gherghe, D. Popescu, Criptografie. Coduri. Algoritmi, Editura Univ. Bucuresti, 2005.
- 4. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997. [http://www.cacr.math.uwaterloo.ca/hac]
- 5. C. Paar, J. Pelzl, Understanding Cryptography, Springer, 2009.

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

10. Evaluation						
Type of activity	10.1 Evaluation criteria	10.2 Evaluation	10.3 Share in the			
		methods	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 Signature of course coordinator Signature of seminar coordinator 30.04.2019 Prof.PhD. Septimiu CRIVEI Prof.PhD. Septimiu CRIVEI

Date of approval

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