COURSE DESCRIPTION

Algebra

Academic year 2026-2027

1. Programme-related data

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

2. Course-related data

2.1. Course title	**Public-Key Cryptography**			Course code	**MLE0049**
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	1	2.6. Type of assessment	Viva voce
2.7. Course status	Optional			2.8. Course type	Specialisation subject

3. Total estimated time (hours per semester of teaching activities)

3.1. Number of hours per week	**3**	of which: 3.2. course	**2**	3.3. seminar/ laboratory/ project	**1**
3.4. Total of hours in the curriculum	42	of which: 3.5. course	28	3.6. seminar/ laboratory	**14**
Time allocation for individual study (IS) and self-taught activities (ST)					**hours**
Learning from textbooks, course materials, bibliography, and notes (IS)					14
Additional research in the library, on subject-specific electronic platforms, and on-site					8
Preparing seminars/ laboratories/ projects, assignments, reports, portfolios, and essays					14
Tutoring (professional guidance)					14
Examinations					8
Other activities					0
3.7. Total hours of individual study (IS) and self-taught activities (ST)				**58**	
3.8. Total hours per semester				**100**	
3.9. Number of credits				**4**	

4. Prerequisites (where applicable)

4.1. curriculum-related	
4.2 skills-related	

5. Specific conditions (where applicable)

5.1. course-related	
5.2. seminar/laboratory-related	

6.1. Competencies resulting from the completion of the degree programme *(as referred to in the curriculum)*[1]

Professional competencies	
Competency code	**Competency**
CP1	create software
CP3	analyse software specifications
CP10	use software libraries
Transversal competencies	
Competency code	**Competency**
CT2	Solve problems
CT3	Think analytically

6.2. Learning outcomes relevant to the degree programme (as referred to in the curriculum)[2]

Learning outcomes targeted by the subject		
Competency code	**Knowledge and comprehension**	**Specific academic skills**
CP5	The student/graduate selects, explains and specifies the mathematical foundations applied in computer science, including formal logic, algebra, probability and statistics.	The student/graduate applies, evaluates, and proposes mathematical methods for modeling, simulating and solving computer science problems.

7. Subject-specific learning outcomes

Knowledge and comprehension
1. The student is able to ensure the formation of skills specific to the Mathematics and Algorithmics-related disciplines needed to complete the assignments.
2. The student knows fundamental notions related to Cryptography, and methods of applying them to areas of science related to Mathematics and Computer Science.
Specific academic skills
1. The graduate will develop mathematical and algorithmical thinking, progressing from a procedural/computational understanding of mathematics to a broad understanding encompassing logical reasoning, generalization, abstraction, and formal proof.

8. Contents

8.1. Course	**Teaching and learning methods**	**Remarks**[3]
1. Classical cryptography. Examples	interactive exposure, explanation, didactical demonstration	
2. Algorithm complexity, elements of number theory	interactive exposure, explanation, didactical demonstration	

[1] The professional and/or transversal skills targeted by the subject for which the course description is prepared will be copied from the curriculum of the degree programme. For each competency, the complete entry, including the competency code, will be copied with the exact wording that appears in the curriculum, without any changes. If no competency is copied from either of the two categories, the row corresponding to that category is deleted from the table.

[2] The learning outcomes relevant for the degree programme and targeted by the subject for which the course description is prepared will be listed. The entries, copied without any changes from the Curriculum by subject type (Core Subject/Specialisation Subject/Complementary Subject), are listed under the corresponding competency.

[3] For example, organisational aspects, recommendations for students, specific aspects relating to the course/seminar, such as inviting experts in the field, etc.

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.

8.2. Seminar/ laboratory	**Teaching and learning methods**	**Remarks**
1. Classical cryptography	interactive exposure, algorithmization	The lab is scheduled as 2 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. Evaluation

Type of activity	9.1 Evaluation criteria[4]	9.2 Evaluation methods[5]	9.3 Percentage in the final grade
9.4. Course	Use of basic concepts in examples	Assessments	1/2 of the grade
9.5. Seminar/ laboratory	Implement course concepts and algorithms	Practical examination	1/2 of the grade
9.6 Minimum standard for passing			
The final grade must be at least 5.			

10. SDG labels (Sustainable Development Goals)[6]

	○	Sustainable Development Generic Label

								
○	○	○	○	○	○	○	○	X
								No label applies
○	○	○	○	○	○	○	○	○

Date of entry:
15.04.2026

Signature of course coordinator

Prof. PhD. Septimiu Crivei

Signature of seminar coordinator

Prof. PhD. Septimiu Crivei

[4] The evaluation criteria must directly reflect the learning outcomes targeted at the level of the degree programme respectively at the level of the subject. More specifically, the learning outcomes set out in the expected learning outcomes are assessed.

[5] Both final evaluation methods and ongoing evaluation strategies should be established.

[6] Select a single label which, according to the *Implementation of SDG labels in the academic process*, best matches the subject. If the subject addresses sustainable development in a generic manner (i.e. by presenting/introducing the general framework of sustainable development, etc.), then the Sustainable Development generic label may be applied. If none of the labels describe the subject, select the last option: *"No label applies."*

Date of approval in the department:
23.04.2026

Signature of the head of department

Prof. PhD. Andrei Mărcuș