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 Mathematics**
1.4 Field of study	**Computer Science**
1.5 Study cycle	**Master**
1.6 Study programme / Qualification	**Distributed Systems in Internet**

2. Information regarding the discipline

2.1 Name of the discipline	**Modular Arithmetics and Cryptography**						
2.2 Course coordinator	**Prof.PhD. Septimiu Crivei**						
2.3 Seminar coordinator	**Prof.PhD. Septimiu Crivei**						
2.4. Year of study	**1**	2.5 Semester	**1**	2.6. Type of evaluation	**E**	2.7 Type of discipline	**DC**

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					28
Additional documentation (in libraries, on electronic platforms, field documentation)					28
Preparation for seminars/labs, homework, papers, portfolios and essays					28
Tutorship					10
Evaluations					14
Other activities:					0
3.7 Total individual study hours	108				
3.8 Total hours per semester	150				
3.9 Number of ECTS credits	6				

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	□ Understanding and use of basic algorithms and mathematical concepts related to cryptography □ Ability to understand and approach problems and projects of information security
Transversal competencies	□ Ability to work independently and/or in a team in order to solve problems and realize projects in defined professional contexts

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

7.1 General objective of the discipline	□ Study of the main algorithms in cryptography
7.2 Specific objective of the discipline	□ Implementation and use of algorithms in cryptographic applications

8. Content

8.1 Course	Teaching methods	Remarks
1. Algorithm complexity, modular arithmetics	exposition, algorithmization	
2. Primality and factorization	exposition, algorithmization	
3. Finite fields and discrete logarithms	exposition, algorithmization	
4. Classical cryptography	exposition, algorithmization	
5. DES, AES	exposition, algorithmization	
6. Stream ciphers	exposition, algorithmization	
7. Block ciphers	exposition, algorithmization	
8. RSA cryptosystem	exposition, algorithmization	
9. ElGamal cryptosystem	exposition, algorithmization	
10. Hash functions	exposition, algorithmization	
11. Digital signatures	exposition, algorithmization	
12. Key-related protocols	exposition, algorithmization	
13. Practical aspects	exposition, algorithmization	
14. Quantum cryptography	exposition, 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.

8.2 Seminar / laboratory	Teaching methods	Remarks
1. Algorithm complexity, modular arithmetics	problematization, exercise	

2. Primality and factorization	problematization, exercise	
3. Finite fields and discrete logarithms	problematization, exercise	
4. Classical cryptography	problematization, exercise	
5. DES, AES	problematization, exercise	
6. Stream ciphers	problematization, exercise	
7. Block ciphers	problematization, exercise	
8. RSA cryptosystem	problematization, exercise	
9. ElGamal cryptosystem	problematization, exercise	
10. Hash functions	problematization, exercise	
11. Digital signatures	problematization, exercise	
12. Key-related protocols	problematization, exercise	
13. Practical aspects	problematization, exercise	
14. Quantum cryptography	problematization, exercise	

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 content is directed towards applications of cryptography. The topic is present in many master programs from other universities and has special interest for prospective employers.

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	Presentation	1/3
10.5 Seminar/lab	Problem solving, project presentation	Test, project	2/3
10.6 Minimum performance standards			
□ Grade 5			

Date	Signature of course coordinator	Signature of seminar coordinator
26.04.2023	Prof. PhD. Septimiu CRIVEI	Prof. PhD. Septimiu CRIVEI

Date of approval	Signature of the head of department
	Prof.PhD. Andrei MARCUS