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	**Master**
1.6 Study programme / Qualification	**High Performance Computing and Big Data Analytics**

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	**2**	2.5 Semester	**3**	2.6. Type of evaluation	**E**	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					42
Additional documentation (in libraries, on electronic platforms, field documentation)					28
Preparation for seminars/labs, homework, papers, portfolios and essays					56
Tutorship					18
Evaluations					14
Other activities:					0

3.7 Total individual study hours	158
3.8 Total hours per semester	200
3.9 Number of ECTS credits	8

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. Notions of algorithms complexity, congruences	exposition, algorithmization	
2. Primality and factorization	exposition, algorithmization	
3. Quadratic residues	exposition, algorithmization	
4. Finite fields and discrete logarithms	exposition, algorithmization	
5. Classical cryptosystems	exposition, algorithmization	
6. Private-key cryptography	exposition, algorithmization	
7. Block ciphers	exposition, algorithmization	
8. Stream ciphers	exposition, algorithmization	
9. RSA cryptosystem	exposition, algorithmization	
10. ElGamal cryptosystem	exposition, algorithmization	
11. Hash functions	exposition, algorithmization	
12. Digital signatures	exposition, algorithmization	
13. Key-related protocols	exposition, algorithmization	
14. Quantic cryptography	exposition, algorithmization	

Bibliography

1. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to coding theory and cryptography, Editura EFES, Cluj-Napoca, 2006.
2. C. Gherghe, D. Popescu, Criptografie. Coduri. Algoritmi, Editura Univ. Bucuresti, 2005.
3. N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.
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. B. Schneier, Applied Cryptography, John Wiley & Sons, 1994.

8.2 Seminar / laboratory	Teaching methods	Remarks
1. Notions of algorithms complexity, congruences	problematization, exercise	2 hours classes
2. Primality	problematization, exercise	
3. Factorization	problematization, exercise	
4. Quadratic residues	problematization, exercise	
5. Fintie fields and discrete logarithms	problematization, exercise	

6. Private-key cryptography	problematization, exercise	
7. Public-key cryptography	problematization, exercise	

Bibliography

1. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to coding theory and cryptography, Editura EFES, Cluj-Napoca, 2006.

2. N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.

3. 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]

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 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	Assignments	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
30.04.2015	Prof.PhD. Septimiu CRIVEI	Prof.PhD. Septimiu CRIVEI

Date of approval	Signature of the head of department
30.04.2015	Prof.PhD. Octavian AGRATINI