COURSE DESCRIPTION

1. Program Information

1.1 University	**“Alexandru Ioan Cuza”, Iasi**
1.2 Faculty	**Computer Science**
1.3 Department	**Computer Science**
1.4 Study Domain	**Computer Science**
1.5 Study Cycle	**Undergraduate**
1.6 Study Program / Qualification	**Computer Science**

2. Course Information

2.1 Course Name			**Computational Number Theory**				
2.2 Course Teacher			**LECTURER SORIN IFTENE, PHD**				
2.3 Seminary Teacher			**LECTURER SORIN IFTENE, PHD**				
2.4 Study Year	**3**	**2.5** Semester	**II**	**2.6** Evaluation	**M**	**2.7** Course Status*	**OP**

3. Total estimated hours (hours per semester and didactic activities)

3.1 Hours per week	**4**	in which: **3.2** course	**2**	**3.3** laboratory	**2**
3.4 Hours in curriculum	56	in which: **3.5** course	28	**3.6** laboratory	28

Time Distribution	hours
Manual study, Course support, Bibliography, and others	**14**
Supplementary Documentation in library, in electronic forums, and on the field	**14**
Seminaries/laboratories preparation, homeworks, reports, portfolios and essays	**28**
Tutoring	**-**
Evaluation	**4**
Other activities (consultations per student)	**-**

3.7 Total hours individual study	**56**
3.8 Total hours per semester	**116**
3.9 Credits	**5**

4. Preconditions (if necessary)

4.1 Of Curriculum	Algebraic Foundations of Computer Science
4.2 Of Skills	Capacity of applying theoretical concepts from Number Theory for developing and implementing efficient algorithms

5. Conditions (if necessary)

5.1 For Course Operation	**-**
5.2 For Seminary/Laboratory Operation	**-**

6. Specific Skills Acquired

Professional Skills	**Knowledge**: the most important algorithms related to problems from number theory and their applications **Abilities**: the capacity of analysing and implementing efficiently the most important algorithms related to number theory
Transversal Skills	This course combines knowledge from several areas, as Algebraic Foundations of Computer Science and Complexity Theory, and has applications especially in Coding and Cryptography (and Information Security). Thus, the students must use/combine knowledge from several areas of computer science.

7. Course Objectives (from the grid of specific skills acquired)

7.1 General Objectives	Designing efficient algorithms (and providing complexity analysis) for problems from number theory
7.2 Specific Objectives	Understanding, Analyzing, and Implementing the most important algorithms for Primality Testing, Factoring Integers, Computing Discrete Logarithms, Computing Square Roots

8. General Description

8.1	**Course**	**Teaching Methods**	**Observations** (hours and bibliographic references)
1.	Course Overview. Representations of Integers and Polynomials. Basic Operations (I) (addition, subtraction, multiplication)	Blackboard presentation	[1], [4], [5]
2.	Basic Operations (II) (division, division, (extended) gcd, inverse, Chinese remainder theorem)	Blackboard presentation	[1], [4], [5]
3.	Exponentiation Techniques (I)	Blackboard presentation	[4], [5]

4.	Exponentiation Techniques (II)	Blackboard presentation	[4], [5]
5.	Primality Testing (I) (probabilistic approaches)	Blackboard presentation	[2], [5]
6.	Primality Testing (II) (Primality Testing for Numbers of a Special Form)	Blackboard presentation	[2], [5]
7.	Primality Testing (III) (primality test (including detecting perfect powers))	Blackboard presentation	[2], [5]
8.	Midterm Exam	Written exam	-
9.	Computing the Order of an Element and Generating Primitive Roots (and Elements of a Certain Order)	Blackboard presentation	[1], [5]
10.	Computing Discrete Logarithms	Blackboard presentation	[1], [5]
11.	Factoring Integers	Blackboard presentation	[1], [2], [5]
12.	Factoring Polynomials and Tests for and Constructing Irreducible Polynomials	Blackboard presentation	[1], [5]
13.	Solving Equations over Finite Fields (Computing Square Roots)	Blackboard presentation	[1], [5]
14.	The Arithmetic of Elliptic Curves	Blackboard presentation	[3], [5]

BIBLIOGRAPHY
(SELECTIONS)

[1] Abhijit Das. Computational Number Theory. CRC Press, 2013
[2] Hans Riesel. Prime Numbers and Computer Methods for Factorization (2nd Edition). Birkhäuser, 2012
[3] Joseph H. Silverman. The Arithmetic of Elliptic Curves (2nd Edition). Springer, 2009
[4]F. L. Ţiplea, S. Iftene, C. Hriţcu, I. Goriac, R. Gordân, E. Erbiceanu. MpNT: A Multi-Precision Number Theory Package. Number Theoretical Algorithms (I), Technical Report TR03-02, Faculty of Computer Science, “Al. I. Cuza” University, Iaşi, 2003 (http://profs.info.uaic.ro/~tr/tr03-02.pdf)
[5] conference or journal articles which will be announced in advance

8.2	**Seminary / Laboratory**	**Teaching/Evaluation methods**	**Observations** (hours and bibliographic references)
1.	Homework 1 (CRC, Reed-Solomon)	debate/oral questioning	same as the course
2.	Homework 1 (CRC, Reed-Solomon)	debate/oral questioning	same as the course
3.	Homework 1 (CRC, Reed-Solomon)	debate/oral questioning	same as the course
4.	Homework 1 (CRC, Reed-Solomon)	debate/oral questioning	same as the course
5.	Homework 2 (RSA efficient exponentiation)	debate/oral questioning	same as the course
6.	Homework 2 (RSA efficient exponentiation)	debate/oral questioning	same as the course

7.	Homework 2 (RSA efficient exponentiation)	debate/oral questioning	same as the course
8.	Midterm Exam	written exam	-
9.	Homework 3 (primality testing)	debate/oral questioning	same as the course
10.	Homework 3 (primality testing)	debate/oral questioning	same as the course
11.	Homework 3 (primality testing)	debate/oral questioning	same as the course
12.	Homework 4 (computing discrete log)	debate/oral questioning	same as the course
13.	Homework 4 (computing discrete log)	debate/oral questioning	same as the course
14.	Homework 4 (computing discrete log)	debate/oral questioning	same as the course

Bibliography

the same as for the course

9. Course content synchronization with the expectations of the community representatives, professional associations and employers from the program domain

This course is designed and structured so that covers the major topics required to achieve efficient implementations of several important applications in coding theory and cryptography (based on certain algorithms for specific problems of number theory).

10. Evaluation

Activity Type	**10.1 Evaluation criteria**	**10.2 Evaluation methods**	**10.3 The weight of each evaluation form (%)**
10.4 Course	Understanding the algorithms presented in the course, the ability to analyze their complexity and to use them in applications	Midterm Exam (EP) Final Exam (EF)	25% 25%
10.5 Seminary/ Laboratory	The ability to implement the most relevant algorithms presented in class in a certain programming language	Homeworks (TL)	50%
10.6 Minimal performance standards			
The conditions that must be held simultaneously are TL ≥ 5 ≥ 5 EP, EF ≥ 5, which requires the understanding and the implementing of algorithms with moderate complexity.			

Date	Course Teacher	Seminary/Laboratory Teacher
March 22, 2018	LECT. DR. SORIN IFTENE	LECT. DR. SORIN IFTENE

Department Date of Approval Director of the Department