Program	Level	Second cycle		
	Name of the program	Computer Science		
COURSE				
Course title	**Algorithmic Number Theory**			
Course code	Semester	Course status	ECTS	Contact hours (L+AE+LE)
CS 525	III	Elective course	7	3+2+0
Lecturer				
Course Goals	The main goal of the course is to introduce to students selected topics in algorithmic number theory, with special attention to the topics relevant to the application in cryptography.			
Learning Outcomes	After completing this course, students should demonstrate competency in the following skills: - Understand basic terms and their relationships as well as some techniques used in algorithmic number theory; - Understand and be able to implement and use some algorithms for determining prime numbers, number factorization and discrete logarithms.			

COURSE CONTENT

- Number theory and complexity.
- Euclidean algorithm for greatest common divisor, worst case complexity analysis.
- Binary gcd algorithm, continuous fractions.
- Legendre and Jacobi symbols.
- Solving equations over finite fields, roots, Hensel's lemma.
- Basic algorithms for prime numbers, and primality tests for numbers of a special form.
- Pseudoprimes and Carmichael numbers, probabilistic primality tests.
- Sieve primality tests, generating random prime numbers.
- Factorisation algorithms.
- Discrete logarithm algorithm.

LITERATURE

[1] S. Y. Yan: Number theory for computing, Springer, 2002.

[2] W. Stein: Elementary Number Theory: Primes, Congruences, and Secrets, a computational approach, Springer, 2009.

[3] P.J. Giblin: Primes and programming, Cambridge University Press, 1993.

[4] E. Bach, J, Shallit: Algorithmic number theory, Volume I: Efficient Algorithms, MIT Press, 1996.

STUDENT WORKLOAD (hours in a semester)

Lectures	45	Exercises	30	Individual work	100	T o t a l	175

GRADING			**REMARKS**
Criterion	Maximum points	Minimum points	
Midterm exams			
Project			
Final exam			
T o t a l	100	55	