Program	Level	Second cycle
	Name of the program	Theoretical Computer Science

COURSE

Course title	Selected Topics in Cryptology			
Course code	Semester	Course status	ECTS	Contact hours (L+AE+LE)
CS 530	I	Elective	7	3+2+0
Lecturer				
Course Goals	The goal of the course is to provide the knowledge on Finite Fields, Boolean functions and their use in the cryptography.			
Learning Outcomes	Gaining ability to use modern mathematical tools needed to follow the latest scientific contributions in cryptography.			

COURSE CONTENT

Boolean functions.
Approach over vector spaces.
Approach over finite fields.
Normal basis over finite fields.
Permutation polynomials.
Bent functions, Walsh spectrum.
Resistant functions.
Algebraically immune functions.
Symmetric functions.

LITERATURE

[1] Claude Carlet, Boolean functions in Cryptography and Error correcting Codes, http://www.math.univparis13.fr/~carlet/chap-fcts-Bool-corr.pdf
[2] Thomas E. Cusick, Pantelimon Stănică, Cryptographic Boolean functions and Applications, Academic Press Elsevier, 2009
[3] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, Reading, Massachusetts (1983)

STUDENT WORKLOAD (hours in a semester)

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

GRADING			**REMARKS**
Criterion	Maximum points	Minimum points	
Midterm exams	50	25	
Homework assignment			
Project			
Laboratory assignments			
Final exam	50	25	
T o t a l	100	55	