COURSE DESCRIPTION

COURSE NAME	SECURITY PROTOCOLS: MODELING AND VERIFICATION	CODE: MSD2207

STUDY YEAR	MASTER II	SEMESTER	II	STATUS(C-compulsory/OP-optional/F-facultative)	C

HOURS PEER WEEK				TOTAL HOURS PER SEMESTER	TOTAL HOURS OF INDIVIDUAL ACTIVITY	CREDITS	EVALUATION TYPE (D-during semester, C-colloquy, E-exam, M-mixed)	TEACHING LANGUAGE
C	S	L	Pr.					
2	2	0	0	56	184	8	E	ENGLISH

TAUGHT BY	ACADEMIC AND SCIENTIFIC TITLE, NAME	DEPARTMENT
	TEACHING ASSISTANT, PHD. CĂTĂLIN BÎRJOVEANU	COMPUTER SCIENCE

REQUIRED COURSES	

OBJECTIVES	Understand the key vulnerabilities that occur in security protocols and ways to eliminate them. Acquiring major modeling and verification techniques for security protocols.
GENERAL THEMATICS	Security properties Attack strategies Principles for designing security protocols Modelling security protocols Techniques for verifying security protocols: BAN logic, inductive method, strand spaces, etc. Tools for automatic verification of security protocols Complexity of security protocols analysis.
SEMINARY/ LABORATORY THEMATICS	The seminars theme will follow the theme of the course, adding new techniques and protocols to those studied in class. Presentation by students of recent articles in the course area.
TEACHING METHODS	Slides, combined with teaching at the blackboard.

BIBLIOGRAPHY	
	1. P. Ryan and S. Schneider. Modelling and Analysis of Security Protocols. Addison-Wesley, 2001. 2. Research papers, oriented on topics of the course.

EVALUATION		
	conditions	Project. Final exam.
	criterials	For each condition from above at least grade 5 must be obtained.
	modes	Project and final exam
	formula	50% project+50% final exam