Program	Type of studies (cycle)	Third cycle
	Name of the program	SEE Doctoral Studies in Mathematical Science

Course				

Course title	**Selected topics in cryptography**			

Course code	Semester	Course status	ECTS credits	Contact hours
AMAT 670		Optional	10	30

Teaching staff	Teacher	Prof. Dr. Enes Pasalic
	Other staff	

Course goals	Give a moderate knowledge in contemporary cryptography, thus covering the design, elementary cryptanalysis and implementation issues of most important cryptographic primitives and algorithms

Course content/topics

- Symmetric key encryption schemes – design rationales and cryptanalysis.
- Mathematical structures in stream and block ciphers
- Public key cryptography
- Hash functions and MAC algorithms
- Authentication and identification schemes and diverse cryptographic protocols
- Real-life applications and algorithms

LITERATURE	Grading			
		Criterion	Points	Cut-off points
[1] Daglas R. Stinson " Cryptography: Theory and Practice"	1.	Written assignment	20	10
[2] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone"Handbook of applied cryptography"	2.	Project	20	10
	3	Final exam	60	35
		Total	100	55