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

Course

Course title	**Selected Areas of Cryptology**

Course code	Semester	Course status	ECTS credits	Contact hours
AMAT 671	II	elective	10	30

Aims and intended learning outcomes	The primary objective of the course is for students to acquire knowledge and skills in selected advanced areas of cryptology. Upon successfully completing the course, the student should possess a deep understanding of the theory within the studied field and the ability to apply that knowledge in various cybersecurity contexts. Furthermore, the student should develop the capacity for independent research in cryptography and the ability to draw scientific conclusions.

Course content/topics

- Symmetric-key encryption algorithms
- Mathematical structures in stream and block ciphers
- Public-key cryptography – hash functions and MAC algorithms
- Authentication and identification algorithms and protocols
- Cryptographic algorithms in practice and standards
- Advanced cryptanalysis

LITERATURE

[1] Daglas R. Stinson " Cryptography: Theory and Practice"

[2] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone"Handbook of applied cryptography˝

Grading

	Criterion	Points	Cut-off points
1.	Written assignment	30	15
2.	Project	30	15
3	Final exam	40	25
	Total	100	55