| | | |
|---|---|---|
| Program | Level | First cycle |
| | Name of the program | Theoretical Computer Science, Mathematics Education, Pure Mathematics, Mathematics and Informatics Education |

### COURSE

| | | | | |
|---|---|---|---|---|
| Course title | **Cryptology** | | | |
| Course code | Semester | Course status | ECTS | Contact hours (L+AE+LE) |
| AMAT 230 | III/V | Mandatory/Elective course | 3 | 2+1+0 |

| | |
|---|---|
| Lecturer | |
| Course Goals | Cryptography is science of the data protection on the commuters and during the transport through the network. The goal of the course is to introduce the theoretical basis of cryptology, cryptographic methods, techniques and algorithms so at the working place students will be able to choose or made appropriate cryptosystem to successfully protect the data. |
| Learning Outcomes | After finishing the course the students will:<br>- Have the knowledge of modern cryptosystems<br>- Be able to apply that knowledge in the future working place. |

### COURSE CONTENT

Definition of cryptology, use of the cryptography. The history, modern and future of cryptography. Theoretical basis.
Simple chippers, stream chipers
Security of the cryptosystems, attacks on the chippers
Symmetric cryptosystems: AES, DES, triple-DES.
Public key cryptography, RSA
Hash functions, autentations, and digital signatures.
Cryptanalysis. Linear and diferential cryptanalysis
Tests of primality of the numbers, factorizations. Chosing the keys.
Permutation polynomials, use of elyptic curves in cryptology. Boolean functions.

### LITERATURE

[1] Richard A. Mollin, An Introduction to cryptography, 2nd edition, (2007), Taylor & Francis Group.
[2] Jonathan Katz, Yehuda Lindel, Introduction to Modern Cryptography, (2008), Taylor & Francis Group.
[3] Lidl, Niederriter, Finite Fields, Encyclopedia of Mathematics and its Applications, (2008).
[4] ByWenbo Mao Hewlett-Packard Company, Modern Cryptography: Theory and Practice, (2003) Prentice Hall.

### STUDENT WORKLOAD (hours in semester)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Lectures | 30 | Tutorial | 15 | Individual work | 30 | Total | 75 |

### GRADING

| Criterion | Maximum points | Minimum points |
|---|---|---|
| Midterm exams | 40 | 23 |
| Homework assignment | 5 | 2 |
| Project | 15 | 8 |
| Laboratory assignments | | |
| Final exam | 40 | 22 |
| Total | 100 | 55 |

### REMARKS