## Lecturer

**Name:** Bogdan Groza

**Background:** PhD

**Specialization:** Associate Professor

**Contacts:**

Email: bogdan.groza@aut.upt.ro

## 

## Course Description

**Title:** Introduction to Cryptography

**Fields of activity:** Computer Science

**Examination type:** Written examination

**Number of ECTS credits issued:** 0

**Learning Goals and Objective:** The course is focused on basic principles and designs from modern cryptography. The main intention is to make students familiar with basic building blocks, i.e., cryptographic primitives, and their correct practical use.

## 

## 

## Syllabus

|  |  |
| --- | --- |
| Name of activity | Symmetric cryptography |
| Number of working hours | 3 hours |
| Type of activity | Lecture |
| Lecturer | Assoc. Prof. Bogdan Groza |
| Short summary of content | This course is an introduction to symmetric cryptographic constructions: symmetric encryptions, hash functions and message authentication codes. We do outline existing constructions from practice, the basic design principles and standards. We do also emphasize on security properties, e.g., IND, RoR and some (provable) relations among these notions. |
| Bibliography | There are no prior knowledge requirements and reading of specific bibliography in advance is not needed. |
| Expected effect | Understanding the main concepts and the correct use of symmetric cryptographic primitives, i.e., block ciphers and hash functions. |

|  |  |
| --- | --- |
| Name of activity | Asymmetric cryptography |
| Number of working hours | 3 hours |
| Type of activity | Lecture |
| Lecturer | Assoc. Prof. Bogdan Groza |
| Short summary of content | This course is an introduction to asymmetric cryptographic constructions, i.e., public key cryptosystems and digital signature schemes. We do outline existing constructions from practice, e.g., the RSA, DSA as well as their security properties. Some basic notions of number theory and computational number theory are outlined. We also emphasize on security reductions as a mean for achieving provable secure cryptosystems. |
| Bibliography | There are no prior knowledge requirements and reading of specific bibliography in advance is not needed but some basic notions of number theory and computational complexity are an advantage. |
| Expected effect | Understanding the role of asymmetric cryptographic primitives in practice, e.g., RSA, DSA, etc. |