Course: Cryptology I

Course instructors: Miodrag Mihaljević

Course type: elective

Credit points ECTS: 12

Prerequisites:

Course objectives:
Education on cryptology that provides methods and techniques for information security and privacy.

Learning outcomes:
Background on methods and techniques of cryptology for research activates within cryptology, information security and privacy.

Course description (outline):
Theoretical classes
Introduction and Classical Cryptography, Principles of Modern Cryptography, Provable Security and Real-World Security, Perfectly Secret Encryption, Private-Key (Symmetric) Cryptography, Computational Security, Chosen-Plaintext Attacks and CPA-Security, Chosen-Ciphertext Attacks and CCA-Security, Stream Ciphers, Block Ciphers and Block-Cipher Modes of Operation, Message Authentication Codes, Authenticated Encryption Schemes, Hash Functions and Applications, Practical Constructions of Symmetric-Key Primitives, Theoretical Constructions of Symmetric-Key Primitives, Public-Key (Asymmetric) Cryptography, Number Theory and Cryptographic Hardness Assumptions, Algorithms for Factoring and Computing Discrete Logarithms, Key Management, Public-Key Encryption, Digital Signature Schemes.

Practice classes
Exercises from the recommended literature

References:
Jonathan Katz, Yehuda Lindell**:** ***Introduction to Modern Cryptography*****,** 3rd Edition**,**
ISBN 9780815354369, Published December, 2020 by Chapman and Hall/CRC, 648 Pages 50 B/W Illustrations

Active teaching hours: 5	Theoretical classes: 5	Practice classes:

Methods of teaching:
Consulting, Project Works, Lectures, Homework

Grading structure (100 points)
Pre-Examination activities:
- activity during lectures or consulting: 10 points,
- project work: 30 points,

Oral Examination: 60 points

Начин провере знања могу бити различити : (писмени испити, усмени испт, презентација пројекта, семинари итд.....
Oral examination, Project Presentation

*максимална дужна 1 страница А4 формата