Course: Cryptology II

Course instructors: Miodrag Mihaljević

Course type: elective

Credit points ECTS: 12

Prerequisites: exam on Cryptology I

Course objectives: Additional education within cryptology regarding public key cryptography and quantum cryptography

Learning outcomes:
Background on certain methods and techniques within public key cryptography and quantum cryptography relevant for further research activities

Course description (outline):
Theoretical classes:
EXPONENTIATION, FACTORING AND DISCRETE LOGARITHMS, Primality testing and integer factorisation using algebraic groups, Basic discrete logarithm algorithms, Factoring and discrete logarithms using pseudorandom walks, Factoring and discrete logarithms in subexponential time, LATTICES, Algorithms for the closest and shortest vector problems, CRYPTOGRAPHY RELATED TO DISCRETE LOGARITHMS, The Diffie–Hellman problem and cryptographic applications, Digital signatures based on discrete logarithms, Public key encryption based on discrete logarithms, CRYPTOGRAPHY RELATED TO INTEGER FACTORISATION, The RSA and Rabin cryptosystems, ADVANCED TOPICS IN ELLIPTIC AND HYPERELLIPTIC CURVES, Isogenies of elliptic curves, Pairings on elliptic curves
QUANTUM CRYPTOGRAPHY: Elements of Quantum Information Theory, Quantum Key Distribution, Quantum Conference Key Agreement, Quantum Key Distribution with Imperfect Devices,
Beyond Point-to-Point Quantum Key Distribution, Device-Independent Quantum Cryptography, Quantum Stream Ciphers
Practice classes: Exercises from the recommended literature

References:
Jonathan Katz, Yehuda Lindell**: *Introduction to Modern Cryptography*,** 3rd Edition,
ISBN 9780815354369, Chapman and Hall/CRC, Dec. 2020.
Steven D. Galbraith: ***Mathematics of Public Key Cryptography***, Online ISBN: 9781139012843
DOI: https://doi.org/10.1017/CBO9781139012843, Cambridge University Press, 2012.
Federico Grasselli: ***Quantum Cryptography***, ISBN: 978-3-030-64359-1, Springer, 2021.

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