

Study programmes: Master studies - Informatics			
Course name: R312 - Cryptography			
Lecturers: Miodrag Živković and other teachers of the Department of Computing and Informatics			
Status: Optional			
ECTS: 8			
Attendance prerequisites: There are no prerequisites			
Course aims: The aim of the course is to introduce the student into data protection by encryption.			
Course outcome: The student understands the research area, basic problems about cryptography and cryptanalysis.			
Course content:			
<ul style="list-style-type: none"> - Crash Course in Number Theory. - Finite Fields. - Modern Stream Ciphers. - Modern Block Ciphers, AES, Modes of Operation of a Block Cipher - Public Key Cryptography. - Elliptic Curve Cryptography. - Hash functions and Message Authentication Codes, Signatures and Authentication. - Key Management and Salting. - Historical Cryptanalysis - The Vigenere cipher. - Cryptanalysis of modern stream ciphers. - Cryptanalysis of Block Ciphers. - Attacks on Public Key Cryptography Factoring. - Solving the Finite Field Discrete Logarithm Problem. 			
Literature:			
1. Miodrag Živković, Kriptografija - Manuscript (http://www.poincare.matf.bg.ac.rs/~ezivkovm/nastava/kripto.pdf), based on the course of E. Shaefer-a (http://math.scu.edu/~eschaefer/book.pdf) 2. D. Stinson, Cryptography – Theory and Practice, CRC Press, 1996. (the teacher can choose another relevant current literature)			
Number of hours: 7	Lectures: 2	Tutorials: 3	Laboratory: -
Research: 2			
Teaching and learning methods: Frontal, group, and practical.			
Assessment (maximal 100 points)			
Course assignments	points	Final exam	points
Lectures	-	Written exam	-
Exercises / Tutorials	-	Oral exam	-
Colloquia	30	Written-oral exam	70
Essay / Project	-		