ERASMUS+

EU programme for education, training, youth and sport

Incoming student mobility

UNIOS University Unit: SCHOOL OF APPLIED MATHEMATICS AND INFORMATICS

COURSES OFFERED IN FOREIGN LANGUAGE
FOR ERASMUS+ INDIVIDUAL INCOMING STUDENTS

Department or Chair within the UNIOS Unit	School of Applied Mathematics and Informatics

Study program	Graduate university study programme in mathematics (Master level) Branches: • Financial Mathematics and Statistics-elective • Mathematics and Computer Science-elective

Study level	Graduate (master)

Course title	Cryptography
Course code (if any)	MI006
Language of instruction	English
Brief course description	Syllabus. 1. Basic concepts. Cryptosystems classification. Attacks to cryptosystems. 2. Substitution ciphers. Caesar cipher. Affine cipher. Letter frequency analysis. Keyword Caesar cipher. Vigenere cipher. Playfair cipher. Hill cipher. 3. Transposition cipher. Permutation cipher. Columnar transposition cipher. 4. Primality tests and some factorization methods. Distribution of primes. Pseudoprimes. Fermat factorization method. Pollard factorization method. Continued fraction factorization method. 5. Public key cryptography. RSA cryptosystem and some of its modifications. Rabin cryptosystem. ElGamal cryptosystem.
Form of teaching	
Form of assessment	Lectures and exercises are obligatory. The exam consists of a written and an oral part. Upon completion of the course, students can take the exam. Successful midterm exam scores replace the written exam. Students can improve their grades by writing homework assignments.

Number of ECTS	6
Class hours per week	2+2+0
Minimum number of students	
Period of realization	Winter semester
Lecturer	Ivan Soldo