Course title:	**Cryptography**
Institute/Division:	F-3, Institute of Computer Modelling
Course code:	F31-C
Erasmus subject code:	Informatics, Computer Science
Number of contact hours:	45 hours
Course duration:	1 semester
ECTS credits:	6
Course description:	Integers. Divisibility of integers. Prime numbers. Euclidean algorithm. Factoring into primes. Congruences. Operations modulo. Fermat's Little Theorem. The Chinese Remainder Theorem. Euler function. Fast exponentiation. Finite groups and fields. Element orders. Encryption schemes. Symmetric cryptosystems: substitution ciphers, block ciphers, permutation ciphers. System DES. Public – Key systems: RSA, discrete logarithm. Hash functions. Digital signatures.
Literature:	J.A.Buchmann, Introduction to cryptography, Springer, New York 2000. N.Ferguson, B.Schneier, Practical cryptography, Wiley & Sons, New York 2003. N.Koblitz, A course in number theory and cryptography, Springer, Berlin 1998.
Course type:	Lectures and exercises
Assessment method:	Attendance, ability of solving of simple exercises, exam
Prerequisites:	General algebra
Primary target group:	3-th – 4-th year computer science students
Lecturer:	Agnieszka Jakóbik, PhD
Contact person:	Agnieszka Jakóbik, PhD, agneskrok@gmail.com
Deadline for application:	15th of September