Algebraic and Number Theory Algorithms

Course description

Basic information

Field of study : Analytical Computer Science

Path : -

Organizational unit : Faculty of Mathematics and Computer Science

Education level : first-cycle

Form of study : full-time studies

Study profile : general academic

Mandatory status : optional

Education cycle : 2022/23

Course code : UJ.WMIIANS.1380.03348.22

Language of instruction : Polish

Disciplines : Computer Science

ISCED classification : 0613 Software and applications development and analysis

USOS code : WMI.TCS.AATL.S

Course coordinator

Lech Duraj

Course instructor

Lech Duraj

Periods Semester 4, Semester 5, Semester 6	Form of verification of learning outcomes exam Teaching format and hours lecture: 30 tutorials: 30	Number of ECTS credits 6.0

Educational goals for the course

C1	The aim of the course is to provide knowledge in the field of algorithms related to number theory and algebra, primarily in relation to cryptography as their main application.

Learning outcomes for the course

Code	Outcomes in terms of	Directional learning outcomes	Verification methods
Knowledge – The student knows and understands:			
W1	basic concepts in the field of algebra and number theory listed in "Course content", useful in the work of a computer scientist	IAN_K1_W01	oral exam, credit
W2	algorithms listed in "Course content" (in particular cryptographic algorithms)	IAN_K1_W06, IAN_K1_W08, IAN_K1_W10	oral exam, credit
Skills – The student can:			
U1	conduct proofs of correctness of selected theorems given in "Course content", in particular proofs of correctness and complexity analysis of algorithms in the field of algebra and number theory	IAN_K1_U01, IAN_K1_U10, IAN_K1_U17, IAN_K1_U21	oral exam, credit
U2	implement basic algorithms of algebra and number theory (including cryptographic algorithms) in an efficient way, taking into account communication security issues	IAN_K1_U03, IAN_K1_U17	credit

ECTS credits balance

Student activity form	Average number of hours* dedicated to completed activity types
lecture	30
tutorials	30
solving computer tasks independently	30
preparation for tutorials	30
solving problem tasks	30
exam preparation	29
exam participation	1

Total student workload	Number of hours 180	ECTS 6.0

* hour (lesson) means 45 minutes

Course content

No.	Program content	Learning outcomes for the course
1.	Integers: computer representation, basic arithmetic algorithms (multiplication, division with remainder, calculating the greatest common divisor), complexity of sorting and searching on integers	W1, W2, U1, U2
2.	Algebraic constructions: commutative groups, rings and fields, non-commutative groups (permutations), polynomials and finite fields (including arithmetic operations), elliptic curve arithmetic	W1, W2, U1, U2
3.	Basics of cryptography: symmetric algorithms, public key cryptography, RSA algorithm, Diffie-Hellman protocol, ElGamal algorithm	W1, W2, U1, U2
4.	Prime numbers and factorization: Miller-Rabin probabilistic test, outline of the AKS deterministic test, Pollard's "rho" algorithm, quadratic sieve, number field sieve	W1, W2, U1, U2
5.	Discrete root problem and discrete logarithm problem on integers and in commutative groups (Tonelli-Shanks algorithm, baby-step-giant-step method, Pohlig-Hellman algorithm, index calculus)	W1, W2, U1, U2
6.	Basics of quantum computing, Shor's algorithm	W1, W2, U1, U2

Extended information

Teaching methods:

multimedia presentation lecture, discussion, problem solving, subject tutorials

Class type	Credit forms	Course credit conditions
lecture	oral exam	Positive exam grade and combined positive grade from exam and tutorials
tutorials	credit	Credit for tutorials based on assignment programs and homework

Literature

Required

1. Neal Koblitz, "A Course in Number Theory and Cryptography"

Additional

1. Song Y. Yan, "Number Theory for Computing"