UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

Classical and Quantum Cryptography

Educational subject description sheet

Basic information

Study programme Fizyka	**Didactic cycle** 2024/25
Speciality INFORMACJA KWANTOWA I SPINTRONIKA	**Subject code** 04FIZIKSS.22KU.04352.24
Organizational unit Faculty of Physics and Astronomy	**Lecture languages** English
Study level Second-cycle programme	**Course type** Elective
Study form Full-time	**Block** Complementary major subjects
Education profile General academic	

Subject coordinator	Adam Miranowicz
Lecturer	Adam Miranowicz

Period	**Activities and hours**	**Number of ECTS points**
Semester 2	• Lecture: 30, Exam • Seminar: 15, Graded credit	4

Goals

Code	Goal
C1	Providing students with basic knowledge of cryptography within the scope defined by the program content, i.e., introducing students to basic concepts and algorithms of classical cryptography, quantum cryptography, and quantum cryptoanalysis.
C2	Developing in students the ability to plan and implement various classical and quantum cryptographic algorithms in a programming language chosen by students.
C3	Forming in students the skills of independent self-education and teamwork skills.

Subject learning outcomes

Code	Outcomes in terms of	Learning outcomes	Examination methods
Knowledge – Student:			
W1	Upon completion of the module and confirmation of achievement, the students should know: basic cryptology terminology, methods of cryptoanalysis of basic ciphers, how to implement selected symmetric cryptosystems, how to implement selected public-key cryptosystems, several digital signature algorithms, basic quantum key distribution protocols, basic classical and quantum factorization algorithms, and how to numerically simulate selected quantum cryptographic systems.	FIZ_K2_W01, FIZ_K2_W02, FIZ_K2_W03, FIZ_K2_W04, FIZ_K2_W05	Written exam, Written colloquium, Project, Multimedia presentation
Skills – Student:			
U1	will be able to understand and apply basic cryptographic concepts and algorithms based on the acquired knowledge, as well as to perform numerical implementations and/or simulations of selected algorithms.	FIZ_K2_U01, FIZ_K2_U02, FIZ_K2_U03, FIZ_K2_U04, FIZ_K2_U05, FIZ_K2_U06, FIZ_K2_U07	Written exam, Written colloquium, Project, Multimedia presentation
U2	will be able to actively engage in solving problems posed, independently develop and expand their competencies.	FIZ_K2_U01, FIZ_K2_U02	Written exam, Written colloquium, Project, Multimedia presentation
Social competences – Student:			
K1	is ready to critically evaluate his/her knowledge and content received, and to consult the knowledge and problems with experts, while trying to maintain independent and critical thinking, following the motto of Richard Feynman: "Science is the belief in the ignorance of experts. When someone says 'science teaches such and such', he is using the word incorrectly. Science doesn't teach it; experience teaches it."	FIZ_K2_K01, FIZ_K2_K02	Written exam, Written colloquium, Project, Multimedia presentation

Study content

No.	Course content	Subject learning outcomes	Activities

No.	Course content	Subject learning outcomes	Activities
1.	week 1: Introduction to cryptography. Tasks of cryptography: 1. message confidentiality, 2. message authentication, 3. message integrity, 4. message non-repudiation. War ciphers: 1. Enigma - Rejewski's bomb and Turing's bomb. 2. Ciphers of the Polish-Soviet war of 1920: Miracle on the Vistula. 3. Ciphers of the Wielkopolska Uprising. 4. Global e-intelligence networks: Echelon, PRISM, MUSCULAR and others. Cryptanalysis of a simple substitution cipher (i.e., the Poe ciphertext). Basic cryptographic terms: Cryptanalysis, decryption, and eavesdropping. Private keys, public keys, and hash functions. Simple ciphers: 1. substitution ciphers, 2. transposition ciphers, 3. wandering key ciphers, 4. poly-alphabetic ciphers, 5. one-time pad (Vernam's cipher). Principles of secure encryption: diffusion and confusion. Shannon's pastry dough mixing.	W1, U1, U2, K1	Lecture, Seminar
2.	week 2: Introduction to quantum cryptography: Application of no cloning theorem for secure information transfer. BB84 protocol for quantum key distribution. Wiesner's protocol of quantum money. Optical implementations of the BB84 and Wiesner protocols. A brief overview of other quantum protocols and algorithms.	W1, U1, U2, K1	Lecture, Seminar
3.	weeks 3 and 4: Elements of number theory in cryptography: 1. Euclid's algorithm. 2. Euler's algorithm of modular exponentiation. 3. Fermat's little theorem. 4. Euler's theorem. 5. Chinese remainder theorem and Gauss's algorithm. 6. Multiplicative groups, cyclic groups, and their generators. 7. Quadratic residues (modular square roots): properties and algorithms, Legendre and Jacobi symbols, and Blum numbers.	W1, U1, U2, K1	Lecture, Seminar
4.	week 5: Asymmetric cryptography (public-key cryptography): Basic concepts and algorithms. Mathematical computational problems of cryptographic interest. Number of keys in symmetric and asymmetric cryptography. Rivest-Shamir-Adleman (RSA) algorithm. Naive methods of attack on the RSA cryptosystem. RSA hypothesis.	W1, U1, U2, K1	Lecture, Seminar
5.	week 6: Shamir's three-step protocol. A hybrid cryptographic protocol. Cryptographic control of the arms race during the Cold War. Simple symmetric and asymmetric message authentication protocols. Diffie-Hellman key exchange algorithm. A generalized Diffie-Hellman algorithm for three correspondents. Knapsack algorithms: Merkle-Hellman algorithm.	W1, U1, U2, K1	Lecture, Seminar
6.	week 7: Message encryption and authentication protocols: ElGamal's encryption algorithm, ElGamal's signature algorithm, Rabin's encryption algorithm, Rabin's signature algorithm.	W1, U1, U2, K1	Lecture, Seminar

No.	Course content	Subject learning outcomes	Activities
7.	week 8: Probabilistic encryption: Goldwasser-Micali and Blum-Goldwasser algorithms. Zero-knowledge proofs of identity: Fiat-Shamir and Feige-Fiat-Shamir identification protocols.	W1, U1, U2, K1	Lecture, Seminar
8.	week 9: Towards the cryptanalysis of RSA: Number primality tests: 1. Fermat's test, 2. Euler's test, 3. Agrawal-Kayal-Saxena (AKS) test, 4. elliptic curve primality test, 6. Miller's test. Classical algorithms for number factorization: 1. Eratosthenes sieve, 2. Monte Carlo method, 3. standard and generalized Fermat's methods, 4. Legendre method of continued fractions, 5. Square sieve method, 6. Comparison of their efficiencies. Prime numbers: Mersenne prime numbers. Great Internet Mersenne Prime Search (GIMPS). Twin prime numbers. Lucas-Lehmer test of Mersenne numbers. Ulam's spiral of prime numbers.	W1, U1, U2, K1	Lecture, Seminar
9.	week 10: The Riemann hypothesis and prime numbers: Euler's Z function. Riemann's zeta function. Millennium Problems. Zeroes of the Riemann zeta function and the eigenvalues of Hamiltonians. Bender's PT-symmetric quantum mechanics. The Riemann problem and superluminal communication.	W1, U1, U2, K1	Lecture, Seminar
10.	week 11: Computational complexity of problems in cryptography: Deterministic Turing machine and P-type problems (polynomial time algorithms). Non-deterministic Turing machine and NP-type (non-deterministic polynomial time) problems. Types of problems: NTIME, NP, NEXPTIME, NSPACE, NPSPACE, and NEXPSPACE. NP-hard problems. NP-complete problems. The hypothesis whether P = NP. Universal Turing machine. Quantum Turing machine as a universal quantum computer. BQP (Bounded-error Quantum Polynomial-time) type problems. NP-hard problems in cryptography: McEliece cryptosystem, NTRUEncrypt, and Merkle-Hellman cryptosystem. Computational complexity of knapsack algorithms. Is factorization of numbers an NP-complete problem?	W1, U1, U2, K1	Lecture, Seminar
11.	week 12: Quantum algorithms in the cryptanalysis of classical cryptosystems: Shor's factorization algorithm. Implementation of Shor's algorithm using NMR spectroscopy.	W1, U1, U2, K1	Lecture, Seminar
12.	week 13: First and second generation quantum technologies. Quantum annealing for cryptoanalysis. Implementation of quantum annealing using superconducting qubits. Algorithm of factorization by Gauss sums (and Schroedinger cats). Implementation of the Gauss-sum algorithm using NMR spectroscopy.	W1, U1, U2, K1	Lecture, Seminar

No.	Course content	Subject learning outcomes	Activities
13.	week 14: Quantum key distribution protocols: 1. BB84 protocol - a brief reminder. 2. Ekert E91 protocol using entangled states. 3. Bennett B92 protocol using Mach-Zehnder interferometers. 4. Renes R04 protocol. 5. Implementations of BB84 and E91 protocols using a quantum satellite.	W1, U1, U2, K1	Lecture, Seminar
14.	week 15: Post-quantum cryptography, i.e. classical cryptography resistant to quantum cryptanalysis by Shor's algorithm. Recommended public key lengths. RSA challenges and rewards. McEliece cryptosystem. Concluding remarks: The future of public-key cryptography. The future of quantum cryptography.	W1, U1, U2, K1	Lecture, Seminar

Additional information

Activities	Teaching and learning methods and activities
Lecture	Lecture with a multimedia presentation of selected issues, Problem-based learning
Seminar	Solving tasks (e.g. computational, artistic, practical), Work in groups

Activities	Credit conditions
Lecture	Grading criteria: 60% either an oral exam or solving and describing a selected research cryptographic problem in the form of a report, which should include the student results of numerical simulations and/or analytical calculations; 20% passing the calculus exercises; 20% activity during lectures.
Seminar	Grading criteria: 80% performing numerical calculations of selected cryptographic algorithms or a multimedia presentation of a given cryptosystem; 20% activity during seminars

Literature

Obligatory

1. selected chapters in: A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

Optional

1. B. Schneier, "Applied Cryptography", Wiley, 2010.
2. M. A. Nielsen and I.L. Chuang "Quantum Computation and Quantum Information", Cambridge University Press, Cambridge, 2000.
3. N. Gisin, G. Rinordy, W. Tittel, H. Zbinden, "Quantum cryptography", Reviews of Modern Physics, Vol. 74, 2002.
4. C.H. Bennett, G. Brassard, A.K. Ekert, "Quantum cryptography," Science World, December 1992.

Calculation of ECTS points

Activities	Activity hours*

Lecture	30
Seminar	15
Preparation for classes	10
Preparation of a multimedia presentation	5
Preparation of a project	15
Preparation for the exam	30
Student workload	**Hours** 105
Number of ECTS points	**ECTS** 4

* academic hour = 45 minutes

Efekty uczenia się dla kierunku

Kod	Treść
FIZ_K2_K01	The graduate is ready to critically evaluate own knowledge and received content
FIZ_K2_K02	The graduate is ready to recognize the importance of knowledge in solving cognitive and practical problems and seeking expert opinion (also from other scientific disciplines) to overcome difficulties during independent problem solving
FIZ_K2_U01	The graduate can use their knowledge to formulate and solve complex and unusual problems in the field of physical sciences; select and apply appropriate methods and tools necessary to solve a given problem (including advanced IT techniques), as well as adapt existing methods and tools or develop completely new ones
FIZ_K2_U02	The graduate can find the necessary information in the professional literature, databases and other sources, in particular in scientific journals basic to physics, and perform critical analysis, synthesis and creative interpretation of the collected information
FIZ_K2_U03	The graduate can formulate and test hypotheses related to simple research problems in physics (plan and perform observations, experiments, theoretical calculations or computer simulations and critically evaluate and discuss the results obtained)
FIZ_K2_U04	The graduate can prepare, for various audiences, oral presentations and written studies presenting specialized topics in the field of physical sciences in a communicative way, as well as debate on such topics
FIZ_K2_U05	The graduate can use English in accordance with the requirements set out for level B2+ of the Common European Framework of Reference for Languages, as well as specialist English terminology in the field of physical sciences
FIZ_K2_U06	The graduate can interact with others as part of teamwork and take a leading role in such work; manage team work
FIZ_K2_U07	The graduate can independently determine the directions of further learning and implement a self-education program, learn throughout lifetime using the available international literature and be able to guide others in this regard
FIZ_K2_W01	The graduate knows and understands in-depth selected facts, phenomena, concepts and theories specific to physics and complex relationships between them (constituting advanced general knowledge in the field of physical sciences and representing both key and other selected issues in the field of advanced detailed knowledge in this discipline)
FIZ_K2_W02	The graduate knows and understands in-depth selected research methods and tools as well as mathematical models used in physics
FIZ_K2_W03	The graduate knows and understands in-depth selected computational methods and information technology tools and techniques used to solve complex problems in physics
FIZ_K2_W04	The graduate knows and understands main development trends in the discipline of physical sciences
FIZ_K2_W05	The graduate knows and understands the role of physical sciences in the context of fundamental dilemmas and challenges of modern civilization