COURSE DESCRIPTION CARD - SYLLABUS

Course name
Introduction to cryptography [S1MNT1>F-WdK]

Course

Field of study
Mathematics of Modern Technologies

Year/Semester
3/5

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
elective

Number of hours

Lecture
30

Laboratory classes
0

Other
0

Tutorials
15

Projects/seminars
0

Number of credit points

3,00

Coordinators

dr Anna Iwaszkiewicz-Rudoszańska
anna.iwaszkiewicz-rudoszanska@put.poznan.pl

Lecturers

Prerequisites

Basic knowledge of abstract algebra and discrete mathematics. Logical thinking skills. Understanding of the limitations of one’s knowledge and motivation for further education.

Course objective

The aim of the course is to familiarize students with the mathematical foundations of cryptography and to present the basic algorithms and practical applications of public key cryptography.

Course-related learning outcomes

Knowledge:
• student knows the concepts and theorems of number theory used in the discussed cryptographic algorithms [K_W01(P6S_WG)];
• student explains the idea of public key cryptography and shows examples of such cryptosystems [K_W01(P6S_WG)].

Skills:
• student performs the calculations necessary for encryption and decryption in the discussed crypto-

graphic systems [K_U01(P6S_UW)];
• student uses theorems from number theory and algebra in the analysis of cryptographic systems. Justifies the correctness of selected cryptographic systems [K_U01(P6S_UW)].

Social competences:
• student knows the limitations of her/his knowledge and understands the need for further education [K_K02(P6S_KK)];
• student is aware of the limitations of modern cryptography [K_K01(P6S_KK)].

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lectures: valuation of knowledge and skills during written test.
Tutorials: three short, evenly scored tests.

Programme content

Cryptography - basic concepts, historical methods of encryption, numeric representation of cipher text. Private key systems and public key systems. Block ciphers, stream ciphers. Discrete logarithm, Diffie-Hellman key exchange protocol, ElGamal system. Algorithms for the discrete logarithm problem. RSA. Rabin system. Digital signatures. Elliptic curves. Cryptographic systems using elliptic curves. Primality tests and factorization algorithms. Hash functions.
Secret sharing, zero-knowledge proof, bit commitment. Post-quantum cryptography.

Course topics

Update: 22.05.2024r.
Lectures:
• cryptography - basic concepts, historical methods of encryption (Caesar, Viegenere, Hill ciphers);
• numeric representation of cipher text;
• private key systems and public key systems;
• block ciphers (AES, block ciphers operation modes);
• stream ciphers;
• discrete logarithm (discrete logarithm problem in group $\Phi(p)$ and in any finite cyclic group);
• Diffie-Hellman key exchange protocol;
• ElGamal system (algorithm for generating keys, encryption and decryption, proof of correctness of decryption, examples of encryption in $\Phi(p)$ and in the multiplicative group of finite field Fpf;
• algorithms for the discrete logarithm problem (Shanks, Pohlig-Hellman algorithm, index calculation method);
• RSA (mathematical foundations: Euclidean algorithm, congruences, Fermat and Euler theorems; algorithm of key generation, encryption and decryption, proof of correct decryption, examples, key requirements, attacks examples);
• Rabin system (mathematical basis: chinese remainder theorem, quadratic residues and nonresidues, the symbol of Legendre and Jacobi, quadratic reciprocity theorem; key generation, encryption and decryption algorithm, square root algorithm, examples, examples of attacks)
• digital signatures (digital signature scheme, RSA signature, Rabin signatures, blind signatures, ElGamal signature, subliminal channel, DSA);
• elliptic curves (elliptic curves over any field, adding points on elliptic curves, elliptic curves over finite fields, cryptographic systems using elliptic curves);
• primality tests and factorization algorithms (Fermat, Solovay-Strassen, Miller-Rabin tests, factorization of Mersenne and Fermat numbers, Fermat, Dixon and $\rho - 1$ Pollard, ρ Pollard methods);
• hash functions;
• another use of public key cryptography (secret sharing, zero-knowledge proof, bit commitment);
• post-quantum cryptography.
Tutorials:
• historical methods of encryption;
• the ElGamal system in the group $\Phi(p)$ and in the multiplicative group of finite field Fpf;
• Euclidean algorithm, congruences, Fermat and Euler theorem;
• RSA;
• Chinese remainder theorem, quadratic residues and nonresidues, quadratic reciprocity theorem;

• Rabin’s system;
• adding points on elliptic curves, determination of points on an elliptic curve above a finite field;
• primality tests, factorization algorithms and algorithms for the discrete logarithm problem.

Teaching methods

Lectures: mulimedia presentation accompanied with examples presented on the blackboard as well as asking questions to students.
Tutorials: solving examples on the blackboard, initiating discussions about solutions, real-time feedback from the teacher.

Bibliography

Basic:
• N. Koblitz, Wykład z teorii liczb i kryptografii, WNT, Warszawa 1995;
• A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Kryptografia stosowana, WNT, Warszawa 2005;
• J.-P. Aumasson, Nowoczesna kryptografia, PWN, Warszawa 2018;
• D. Wong, Prawdziwy świat kryptografii, PWN, Warszawa 2023.

Additional:
• D.R. Stinson, kryptografia w teorii i w praktyce, WNT, Warszawa 2005;
• W. Marzantowicz, P. Zarzycki, Elementarna teoria liczb, PWN, Warszawa 2006.

Breakdown of average student's workload

	Hours	ECTS
Total workload	75	3,00
Classes requiring direct contact with the teacher	45	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	30	1,00