COURSE DESCRIPTION CARD - SYLLABUS

Course name

Zaawansowane systemy szyfrowania - Advanced encryption systems

Course

Field of study
Teleinformatics

Year/Semester
1/1

Area of study (specialization)

Profile of study
general academic

Level of study
second-cycle studies

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
15

Laboratory classes
15

Other (e.g. online)

Tutorials
15

Projects/seminars
0/0

Number of credit points

3

Lecturers

Responsible for the course/lecturer:

dr hab. inż. Mieczysław Jessa, prof. PP
Institute of Multimedia Telecommunications
Phone: +48 61 665 3854, email:
mieczyslaw.jessa@put.poznan.pl

Responsible for the course/lecturer:

Prerequisites

A student starting this subject should have basic systematized knowledge about the operation of ICT networks. It should know the basic security risks for data transmitted, processed and collected in ICT

networks. He should know the basic concepts of cryptography and understand the importance of international standards for ensuring security in ICT. He should also have the ability to obtain information from literature, databases and other sources in Polish or English.

Course objective

The aim of teaching the subject is to familiarize students with the mathematical foundations of cryptography and to develop the ability to use mathematical methods at the stage of creation, analysis, use of advanced encryption methods and deepen knowledge about encryption systems used in ICT.

Course-related learning outcomes

Knowledge

1. Has extensive knowledge in the field of number theory, probability theory and mathematical statistics necessary to describe and evaluate the quality of operation of block ciphers and stream ciphers used in ICT.
2. Knows advanced encryption methods and how to use them to protect information sent and stored in ICT systems.
3. Understands the importance of cryptography for ensuring the security of data transmitted in ICT networks and collected in databases.

Skills

1. Can predict the effects of the lack of cryptographic security of devices and networks on the security of data sent and collected in the ICT system.
2. Knows how to work in a group on solving the problem of data protection and ICT network against unauthorized access or modification.

Social competences

1. It is ready to acquire new knowledge necessary to ensure the security of ICT systems by cryptographic methods.
2. Has a sense of responsibility for the security of the designed ICT systems and is aware of the potential dangers for other people or society of their inadequate security.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

The knowledge acquired as part of the lecture is verified on the basis of a written credit, consisting of 5 open questions, identically scored. The passing threshold is 50% of the points. The distribution of thresholds for grades 2 to 5 is even. A set of questions is drawn individually from a set of issues. Credit issues, on the basis of which open questions are developed, are sent to students by e-mail using university e-mail.
Knowledge and skills acquired during accounting exercises are verified on the basis of a written credit, consisting of 5 accounting tasks. The passing threshold is 50%. The distribution of thresholds for grades 2 to 5 is even.

Programme content

As part of the course, students will learn the mathematical basics of cryptography, the principles of building block ciphers, examples of block ciphers used today, the principles of building stream ciphers, methods of producing truly random numbers, secure pseudorandom numbers, methods of assessing the quality of bit streams used in cryptography using statistical tests and restarts, examples of secure pseudorandom number generators and stream ciphers. Students will learn the methods of digital signature, the principles of creating a public key infrastructure (PKI), the basics of post-quantum cryptography and the basic scenarios of an attack on a cryptographic system divided into general and specialized methods.

As part of the lecture, students will learn the mathematical basics of cryptography, i.e. groups, multiplicative groups, group generator, rings, bodies, congruences, number primacy testing, factorization, polynomials with coefficients in a finite body, Euclid's algorithm, Euler's function, Fermat's Small Theorem, Euler's Theorem, Chinese Residue Theorem, Bezout Identity, number inverse in modular arithmetic, Extended Euclid Algorithm, discrete logarithm, quadratic residues, square roots, properties of the XOR operation, principles of construction of block ciphers, block ciphers used today, e.g. 2DES, 3DES, AES, BLOWFISH, SERPENT, CAST, RC5, RC6. The properties of stream ciphers, methods of producing truly random numbers, secure pseudorandom numbers for stream ciphers, methods of assessing the quality of random bit streams used in cryptography using statistical tests and restart mechanism. Examples of secure pseudorandom number generators and stream ciphers: BBS, RC4, ANSI X9.17, FIPS 186, etc. are also discussed. Students will learn the methods of digital signature, the principles of creating a Public Key Infrastructure (PKI), the basics of post-quantum cryptography and the basic scenarios of an attack on a cryptographic system divided into general and specialized methods. As part of the exercises, tasks are solved illustrating the use of Euclid's algorithm, Fermat's Theorem, Euler's Theorem, methods for calculating the inverse of a number in modular arithmetic, the Extended Euclid Algorithm, Chinese Theorem about residues, square residues, square-and-multiply methods and the use of learned theorems in the design of the RSA algorithm.
The lab includes examples of encryption using a symmetric block cipher, production of a truly random numbers, production of a secure pseudorandom numbers, examples of encryption using a symmetric stream cipher, and examples of encryption using an asymmetric cipher.

Teaching methods

1. Lecture: a multimedia presentation, illustrated with examples given on the board.
2. Exercises: classic problem.
3. Laboratory: classic problem.

Bibliography

Basic

1. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone „Kryptografia stosowana”, WNT, Warszawa 2005.
2. B. Schneier „Kryptografia dla praktyków”, WNT, Warszawa, 2002.
3. W. Stallings „Kryptografia i bezpieczeństwo sieci komputerowych”, Wyd. V, Helion 2012.

Additional

1. J. Hoffstein, J. Pipher, J. H. Silverman „An Introduction to Mathematical Cryptography, Springer, 2008."
2. J. A. Buchmann „Wprowadzenie do kryptografii", PWN, 2006.
3. M. Karbowski, Podstawy kryptografii, Helion, 2014.
4. M. Kutyłowski, W-B. Strothmann „Kryptografia, teoria i praktyka zabezpieczania systemów komputerowych", Read Me, Warszawa, 1999.
5. N. Ferguson, B. Schneier „Kryptografia w praktyce", Helion, 2004.

Breakdown of average student's workload

	Hours	ECTS
Total workload	86	3.0
Classes requiring direct contact with the teacher	45	2.0
Student's own work (preparation for tests, preparation for tutorials, preparation for laboratory classes, literature studies)	41	1.0