COURSE DESCRIPTION CARD - SYLLABUS

Course name
Encryption and Certification Systems [S2Teleinf2>SSiC]

Course

Field of study
Teleinformatics

Year/Semester
1/1

Area of study (specialization)
–

Profile of study
general academic

Level of study
second-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
14

Laboratory classes
24

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

3,00

Coordinators

dr hab. inż. Mieczysław Jessa prof. PP
mieczyslaw.jessa@put.poznan.pl

Lecturers

mgr inż. Paweł Kubczak
pawel.kubczak@put.poznan.pl

dr hab. inż. Mieczysław Jessa prof. PP
mieczyslaw.jessa@put.poznan.pl

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 course is to familiarize students with the mathematical foundations of cryptography, methods of encryption and certification of messages and to develop the ability to use mathematical methods at the stage of creating, analyzing and using encryption methods and certificates.

Course-related learning outcomes

Knowledge:

He has extended and in-depth knowledge of some branches of mathematics, including elements of mathematical analysis, stochastic processes, optimization methods and numerical methods [K2_W01], [K2_W11].
He has in-depth knowledge in the field of information processing and security in ICT systems [K2_W08], [K2_W10].

Skills:
He/she is able to acquire information from literature, databases, and other sources; integrate the obtained information; interpret and critically evaluate it; draw conclusions; and formulate and thoroughly justify opinions [K2_U01], [K2_U15], [K2_U17].
Can utilize learned mathematical methods and models, modifying them as necessary, to carry out projects in the field of ICT [K2_U06], [K2_U14].
Can identify directions for further learning and engage in self-education processes [K2_U011], [K2_U16].

Social competences:
Is ready to recognize the significance of knowledge in solving cognitive and practical problems and to critically evaluate received content [K2_K01].
Is ready to fulfill social obligations [K2_K02].

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 points. The distribution of thresholds for grades from 2 to 5 is uniform. Credit issues, on the basis of which open questions are developed, are sent to students electronically.
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 from 2 to 5 is uniform.

Programme content

As part of the lecture, students learn the mathematical foundations of cryptography, i.e. groups, multiplicative groups, group generator, rings, bodies, congruences, primality testing, factorization, polynomials with finite state coefficients, Euclid's algorithm, Euler's function, Fermat's Small Theorem, Euler's Theorem, Chinese Residue Theorem, Bezout Identity, inverse of numbers in modular arithmetic, Extended Euclid Algorithm, discrete logarithm, quadratic residues, square roots, properties of the XOR operation, principles of building block ciphers, block ciphers used today, e.g., 3DES, AES, BLOWFISH, SERPENT, CAST, RC5, RC6. The properties of stream ciphers, methods of producing secure pseudorandom sequences, methods of assessing the quality of bit streams used in cryptography by means of statistical tests and restarts, examples of secure pseudorandom number generators and stream ciphers: BBS, RC4, ANSI X9.17, FIPS 186, etc. are also discussed. Students will learn digital signature methods, principles of certification and creation of public key infrastructure (PKI), fundamentals of post-quantum cryptography (PQC), and the basic scenarios for attacking 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's Algorithm, Chinese Theorem about residues, square-and-multiply methods. The use of learned theorems in the design of the RSA algorithm for the purpose of data encryption and authentication are also solved.
The laboratory includes examples of encryption using block ciphers, stream ciphers in which secure pseudorandom sequences are produced based on block cipher operating in OFB or CTR mode,examples of implementations of digital signatures using traditional methods and using PQC.

Course topics

As part of the lecture, students learn the mathematical foundations of cryptography, i.e. groups, multiplicative groups, group generator, rings, bodies, congruences, primality testing, factorization, polynomials with finite state coefficients, Euclid's algorithm, Euler's function, Fermat's Small Theorem,

Euler's Theorem, Chinese Residue Theorem, Bezout Identity, inverse of numbers in modular arithmetic, Extended Euclid Algorithm, discrete logarithm, quadratic residues, square roots, properties of the XOR operation, principles of building block ciphers, block ciphers used today, e.g., 3DES, AES, BLOWFISH, SERPENT, CAST, RC5, RC6. The properties of stream ciphers, methods of producing secure pseudorandom sequences, methods of assessing the quality of bit streams used in cryptography by means of statistical tests and restarts, examples of secure pseudorandom number generators and stream ciphers: BBS, RC4, ANSI X9.17, FIPS 186, etc. are also discussed. Students will learn digital signature methods, principles of certification and creation of public key infrastructure (PKI), fundamentals of post-quantum cryptography (PQC), and the basic scenarios for attacking 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's Algorithm, Chinese Theorem about residues, square-and-multiply methods. The use of learned theorems in the design of the RSA algorithm for the purpose of data encryption and authentication are also solved.
The laboratory includes examples of encryption using block ciphers, stream ciphers in which secure pseudorandom sequences are produced based on block cipher operating in OFB or CTR mode,examples of implementations of digital signatures using traditional methods and using PQC.

Teaching methods

Lecture: a combination of a traditional lecture with a problem lecture.
Exercises: classic problem.
Lab: combination of classical method with group actions.

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	78	3,00
Classes requiring direct contact with the teacher	38	1,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	40	1,50