COURSE DESCRIPTION CARD - SYLLABUS

Course name
Cryptography and Basics of Cryptanalysis

Course

Field of study
Computing

Year/semester
1/1

Area of study (specialization)
Cybersecurity

Profile of study
general academic

Level of study
Second-cycle studies

Course offered in
English

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
30

Laboratory classes
30

Other (e.g. online)

Tutorials
15

Projects/seminars

Number of credit points

6

Lecturers

Responsible for the course/lecturer:
dr inż. Anna Grocholewska-Czuryło
anna.grocholewska-czurylo@put.poznan.pl
tel: 61 665 3531
Faculty of Computing and Telecommunications

Responsible for the course/lecturer:
dr Joanna Weissenberg
joanna.weissenberg@put.poznan.pl
tel: 61 665 39 46
Faculty of Computing and Telecommunications

Prerequisites

A student beginning this course should have knowledge of basic algorithms and their analysis, operating systems, computer networks and cryptographic algorithms. He/she should be able to use programming environments and platforms to write, execute and test programs. Should be able to construct algorithms and analyze their complexity. Should have the ability to obtain information from indicated sources and be willing to work collaboratively as part of a team.

Course objective

To provide students with knowledge of advanced principles of cryptographic algorithms and to teach their design. To acquaint students with methods of designing selected cryptographic algorithms and protocols, to teach methods of analysis and evaluation of selected cryptographic systems.

Course-related learning outcomes

Knowledge

The student has detailed knowledge of:

- what criteria a secure information system should meet and what protection measures should be used to achieve this,

- has structured and theoretically grounded general knowledge connected with the key issues of cryptographic mechanisms of data protection (symmetric and asymmetric ciphers, hash functions, digital signatures), elliptic curves, authentication protocols, key management algorithms and secret sharing, protocols ensuring network security and mail security

- has advanced detailed knowledge of selected topics in cipher design and evaluation,

- has knowledge about development trends and the most important new achievements in cryptography

Skills

The student will be able to:

- analyze and design selected cipher components that meet specific criteria and are resistant to cryptanalysis

- design and implement selected cryptographic algorithms

- design and implement a system using appropriate cryptographic methods to ensure confidentiality, integrity and authentication of the data stored and processed in it, analyze the performance of the implemented system

- analyze and evaluate the security level of applied cryptographic mechanisms and estimate whether the system is vulnerable to known cryptographic attacks

- propose, design and implement alternative cryptographic mechanisms ensuring higher security level.

Social competences

The student understands that:

- an important aspect is the use of appropriate, up-to-date cryptographic methods,

- the proper implementation of cryptographic algorithms is equally important,

- it is necessary to update knowledge on secure parameters of used algorithms, protocols and tools.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Knowledge acquired during lectures is verified during the one-hour written examination consisting of 5 questions. Pass mark: more than 50% of the points. Credit issues, on the basis of which questions are developed, are available within the eKursy system.

Skills acquired during the exercises and laboratory classes are verified on an ongoing basis during the classes (by checking the completed task or laboratory exercise) and by one 30-minute colloquium after 8th laboratory of the knowledge that was necessary to perform and understand the exercises.

Programme content

Lecture topics

1. Block ciphers - analysis of basic components of block ciphers and design criteria they must meet. Currently used modes of operation of block ciphers - encryption with authentication.

2. Chaos theory and pseudorandom sequence generators, extended sequence randomness tests.

3. Shortcut functions - design of shortcut functions, classification of functions by structure, criteria that good shortcut functions must satisfy, MAC, attacks on shortcut functions, applications, Sponge structure - on the example of Keccak function.

4. Asymmetric cryptography - analysis of selected algorithms and protocols based on asymmetric ciphers. OTR protocol.

5. Digital signatures, managing cryptographic material.

6. Authentication methods - protocols using known cryptographic mechanisms - symmetric, asymmetric and hash functions, review of current authentication methods (procedural, passwordless, through social networks, etc.), biometric methods.

7. Secret sharing methods - Shamir algorithm and its modification with imposter identification, selected steganographic methods.

8. Use of elliptic curves in cryptography - ECRSA, ECDH, ECDSA.

9. Blockchain technology - structure, security, examples of use, cryptocurrencies, iteligent contracts.

Exercises:

During the exercises, students learn those mathematical issues from algebra, discrete mathematics and modular arithmetic, that are needed for the design and analysis of cryptographic algorithms.

Laboratory

1 Analysis of the most important component of block ciphers and the criteria it must satisfy. Implementation of methods to analyze S-blocks: balancedness, avalanche property and nonlinearity.

2. Implementation of random sequence generator based on selected algorithm from chaos theory, and tests to check the randomness of the generated sequence.

3. Implementation of the Berlecamp-Massey algorithm.

4. Implementation of the algorithm for secret sharing or cryptographic material management

5. Implementation of the OTR protocol.

6. Implementation of a selected cryptographic system in teams.

Teaching methods

The lecture is conducted in an interactive manner (with the formulation of questions to students) using multimedia presentations. Materials are made available to students in electronic version.

Blackboard and laboratory exercises - presentation of the problem / exercise to be performed on the blackboard (with the basic level of difficulty and extended for those willing) and the implementation of the exercise in the laboratory, using the programming language chosen by the student.

Bibliography

Basic

Pieprzyk J., Hardjono T., Seberry J., Teoria bezpieczeństwa systemów komputerowych, Helion 2003 (sygnatura w bibliotece PP: W 110215).

Additional

Menezes A. i inni, Kryptografia stosowana, WNT, 2005, (sygnatura w bibliotece PP: W 112188)

Materials provided by the instructor, updated annually.

Breakdown of average student's workload

	Hours	ECTS
Total workload	150	6,0
Classes requiring direct contact with the teacher	75	3,0
Student's own work (literature studies, preparation for laboratory classes, preparation for tests)[1]	75	3,0

[1] delete or add other activities as appropriate