POZNAN UNIVERSITY OF TECHNOLOGY

EUROPEAN CREDIT TRANSFER AND ACCUMULATION SYSTEM (ECTS)

COURSE DESCRIPTION CARD - SYLLABUS

Course name
Selected Cryptographic Issues [N1Inf1>WZK]

Course

Field of study Computing	Year/Semester 4/7
Area of study (specialization) –	Profile of study general academic
Level of study first-cycle	Course offered in polish
Form of study part-time	Requirements elective

Number of hours

Lecture 12	Laboratory classes 12	Other (e.g. online) 0
Tutorials 0	Projects/seminars 0	

Number of credit points

2,00

Coordinators

dr inż. Anna Grocholewska-Czuryło
anna.grocholewska-czurylo@put.poznan.pl

Lecturers

Prerequisites

Student starting this subject should have the knowledge of basic algorithms including their analysis, operating systems, computer networks and fundamentals of cryptography. The student should be able to manage programming environments and platforms for applications" writing, executing and testing. Student should be able to design algorithms and perform an analysis of their complexity.

Course objective

The objective of this course is to provide students with selected advanced cryptographic issues. Students should gain the ability to use these methods in practice.

Course-related learning outcomes

Knowledge:
Student has a detailed knowledge about:
- current cryptographic problems and solutions,
- design and analysis of block ciphers, hash functions and asymmetric ciphers,
- advanced protocols and cryptographic algorithms like calculations on elliptic curves, cryptocurrencies, secure multi-party computations.

Skills:
Student is able to:
- design and implement systems with the use of appropriate cryptographic methods in order to ensure privacy and integrity as well as authentication of stored and analyzed data sets in these systems,
- analyze and estimate the level of security of cryptographic mechanisms and evaluate whether a certain system is immune to known cryptographic attacks,
- propose, design and implement alternative cryptographic mechanisms to ensure a higher level of security.

Social competences:
The student understands:
- how important it is to implement adequate data security methods,
- that an implementation of appropriate cryptographic algorithms is equally important,
- the necessity of updating knowledge on security parameters, algorithms, protocols and tools used.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
The knowledge obtained during the lectures is verified by the means of a 45-minutes written test, consisting of 5 question. Passing threshold: over 50% of points. Topics, which are the basis for final exam questions, are sent to students by e-mail at the beginning of the semester.
The knowledge obtained during lab practicals is verified during the practicals (checking the preformed exercises).

Programme content

Lecture:
1. Introduction - challenges of modern cryptography, introduction to the design of block ciphers and hash functions, random number generators.
2. Block cipher components and criteria they must meet. Cryptanalysis of ciphers.
3. Algorithms on elliptic curves.
4. Multi-party computations, examples of practical applications.
5. Authenticated encryption.
6. Cryptocurrencies, smart contracts.

Lab practicals
1. Analysis of selected substitution blocks, permutation blocks and key generation algorithms.
2. Differential cryptanalysis.
3. Implementation of the selected algorithm on an elliptic curve.
4. Analysis of authenticated encryption algorithms.
5. Implementation of the selected problem of bilateral computations.
6. Analysis of cryptocurrency security.

Teaching methods

The lectures are interactive (questions are addressed to students) with the use of multimedia presentations. The digital version of the contents of the presentations are provided to students.
Lab practicals - presentations regaring the problem/exercises to be performed on the board (within the basic level of difficulty and also with higher difficulty for volunteers) and performing an individual exercise in a programming language of choice.

Bibliography

Basic
Pieprzyk J., Hardjono T., Seberry J., Teoria bezpieczeństwa systemów komputerowych, Helion 2003 (reference number in PP library: W 110215).
Menezes A. i inni, Kryptografia stosowana, WNT, 2005, (reference number in PP library: W 112188)
Additional
Materials shared by the lecturer, updated every year.

Breakdown of average student's workload

	Hours	ECTS
Total workload	50	2,00
Classes requiring direct contact with the teacher	24	1,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	26	1,00