COURSE DESCRIPTION

Course code

INP7766

Kind of studies

Computer Science MSc; Computer Science BSc; PhD;

Course title

Cryptography

First name, surname and title of the lecturer/supervisor

prof. dr hab Mirosław Kutyłowski

First name, surname and title of the team's members

Mirosław Kutyłowski, prof dr hab., M. Gomułkiewicz, mgr inż, W. Rutkowski mgr inż

Course structure

Form of class	Lecture	Problems classes	Laboratory	Project	Seminar	Number of points
Number of hours/week	2	1				3
Course grade based on	Test	Test				

Prerequisites

MAP3707 or MAP1704 or MAP2706

Course description

The aim of the course is presenting modern cryptographic techniques used in computer systems. The subject of the course are mathematical foundations of cryptography as well as practical implementation issues and security aspects.

Lectures

Contents of particular hours	Number of hours

1. Basic application areas.	2
2. Symmetric encryption, encryption modes.	2
3. Standard symmetric encryption algorithms.	2
4. Asymmetric encryption, RSA, ElGamal.	2
5. RSA security.	2
6. Hash functions and MAC.	2
7. Standard hash functions.	2
8. Pseudorandom generators: BBS, LFSR, A5.	2
9. Security of pseudorandom generators, stream ciphers.	2
10. Interactive proofs and zero knowledge proofs.	2
11. Authentication, Fiat-Shamir protocol, Schnorr protocol.	2
12. Key management, key agreement.	2
13. Differential cryptanalysis, linear cryptanalysis, other methods.	2
14. Side channel cryptanalysis.	2
15. Chosen cryptographic protocols.	2

Problems classes

Contents of particular hours	Number of hours
1. Presentation of cryptographic protocols and standard computer security systems.	8
2. Problem solving for current topics presented during the lectures.	7

Material for self preparation

Basic literature

1. Kryptografia, teoria i praktyka zabezpieczania systemów komputerowych, M. Kutyłowski, W. Strothmann, RM, ISBN 83-7147-087-8.
2. Handbook of Applied Cryptography, A. J. Menezes, P. C van Oorschot, S. A. Vanstone, CRC, 1996, ISBN 0-8493-8523-7.

Additional literature

Conditions required for a student to pass the course

Final test.