



COURSE DESCRIPTION CARD - SYLLABUS

Course name

Number Theory and Cryptography

Course

Field of study

Mathematics in Technology

Area of study (specialization)

Level of study

First-cycle studies

Form of study

full-time

Year/Semester

3/6

Profile of study

general academic

Course offered in

Polish

Requirements

elective

Number of hours

Lecture

30

Laboratory classes

Tutorials

15

Projects/seminars

Other (e.g. online)

Number of credit points

4

Lecturers

Responsible for the course/lecturer:

dr Anna Iwaszkiewicz-Rudoszańska

email: anna.iwaszkiewicz-

rudoszanska@put.poznan.pl

tel. 61 665 2812

Faculty of Control, Robotics and Electrical

Engineering

Piotrowo 3A, 60-965 Poznań

Responsible for the course/lecturer:

Prerequisites

Basic knowledge of algebra and discrete mathematics. Basic knowledge of algebra and discrete mathematics. Understanding the necessity of expanding own competences.

Course objective

The course is intended to present the basic schemes of public key cryptography and results in number theory necessary to understand them.

Course-related learning outcomes

Knowledge

1. Formulates definitions and theorems from number theory used in discussed cryptographic



algorithms.

2. Explains basic concepts of public key cryptography and give an account of different cryptosystems.

Skills

1. Performs calculations necessary for encryption and decryption in discussed cryptographic systems.
- 2 Uses theorems from number theory and algebra in the analysis of cryptographic systems. Justifies the correctness of selected cryptographic systems.

Social competences

1. Knows the limits of her/his own knowledge and understands the need for further education.
2. Is aware of the limitations of contemporary cryptography.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lecture: Written test at the end of semester.

Tutorials: Three short tests during semester.

Programme content

Lecture: Congruences (Chinese Remainder Theorem, Euler's function, Euler's Theorem). Arithmetic functions. Quadratic residues, Legendre and Jacobi symbols, Gauss' Law of Reciprocity. Primality testing. Discrete logarithm problem. Diffie-Hellman key exchange systems. Public key cryptography. RSA, Rabin's and ElGamal encryption schemes. Signature schemes. Blind signatures. Elliptic Curves. Elliptic curve cryptosystems. Complexity of selected algorithms.

Tutorials: Congruences (Chinese Remainder Theorem. Euler's function, Euler's Theorem). Quadratic residues, Gauss' Law of Reciprocity. Arithmetic in finite fields. RSA, Rabin's and ElGamal encryption schemes. Signature schemes. Elliptic Curves.

Teaching methods

Lectures: lecture with presentation supplemented with proofs and examples on the blackboard, with questions formulating to group; theory presented with connections of current knowledge.

Tutorials: solving on board example tasks, initiating discussion of solutions.

Bibliography

Basic

1. N. Koblitz, Wykład z teorii liczb i kryptografii, WNT, Warszawa 1995
2. W. Marzantowicz, P. Zarzycki, Elementarna teoria liczb, PWN Warszawa 2006
3. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Kryptografia stosowana, WNT, Warszawa 2005

Additional

1. W. Narkiewicz, Teoria liczb, PWN Warszawa 2003



- 2.W. Sierpiński, Teoria liczb, MM tom 19, IM PAN, Warszawa 1950
3. D.R. Stinson, kryptografia w teorii i w praktyce, WNT, Warszawa 2005

Breakdown of average student's workload

	Hours	ECTS
Total workload	100	4,0
Classes requiring direct contact with the teacher	45	2,0
Student's own work (literature studies, preparation for tutorials, preparation for tests) ¹	55	2,0

¹ delete or add other activities as appropriate