STUDY MODULE DESCRIPTION FORM

Name of the module/subject		Code
Number theory and cryptography		**1010341661010348732**
Field of study: **Mathematics**	Profile of study (general academic, practical): **(brak)**	Year /Semester: **3 / 6**
Elective path/specialty: **Mathematical Modelling**	Subject offered in: **Polish**	Course (compulsory, elective): **obligatory**
Cycle of study: **First-cycle studies**	Form of study (full-time,part-time): **full-time**	
No. of hours: Lecture: **30** Classes: **-** Laboratory: **30** Project/seminars: **-**		No. of credits: **4**
Status of the course in the study program (Basic, major, other): **(brak)**	(university-wide, from another field): **(brak)**	
Education areas and fields of science and art		ECTS distribution (number and %)

Responsible for subject / lecturer:

dr Anna Iwaszkiewicz-Rudoszańska
email: anna.iwaszkiewicz-rudoszanska@put.poznan.pl
tel. 61 665 2812
Wydział Elektryczny
ul. Piotrowo 3A, 60-965 Poznań

Responsible for subject / lecturer:

dr Piotr Rejmenciak
email: piotr.rejmenciak@put.poznan.pl
tel. 61 665 2359
Wydział Elektryczny
ul. Piotrowo 3A, 60-965 Poznań

Prerequisites in terms of knowledge, skills and social competencies:

1	**Knowledge**	The basic knowledge of algebra.
2	**Skills**	Umiejętność przeprowadzania poprawnych wnioskowań logicznych.
3	**Social competencies**	Understanding of limitation of own knowledge and motivation for further education.

Assumptions and objectives of the course:

Number theoretical topics such as divisibility, linear diophantine, primes, linear congruences, Euler's theorem and applications to cryptography. Basic algorithms and practical aplications such as key exchange and digital signature.

Study outcomes and reference to the educational results for a field of study

Knowledge:

1. deduce and prove results in elementary number theory - [K_W04]
2. explain basic concepts of public key cryptography and give an account of different cryptosystems - [K_W01]

Skills:

1. solve linear Diophantine equations using congruences - [K_U01]
2. know mathematical fundaments of cryptography and cryptanalysis, especially those related to number theory. - [K_U05, K_U17]
3. evaluating the safety of an asymmetric cryptosystem - [K_U01, K_U36]

Social competencies:

Assessment methods of study outcomes

Lecture

Valuation of knowledge and skills during oral and written exam.

Laboratories

Two tests (student can use his own notes). Valuation of student answers during lessons. Valuation of activity during lessons. Individual problems to solve at home.

Course description

Divisibility, least common multiples, Euclid's algorithm. Prime numbers. Modular arithmetic, linear congruences. Integer solutions of ax + by = c. Chinese Remainder Theorem. Fermat's Little Theorem, Euler's function, Euler?s Theorem. Quadratic residues. Gauss' Law of Reciprocity. Primality testing and factorisation techniques. 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. Elements of complexity theory.

Basic bibliography:

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 bibliography:

1. W. Narkiewicz, Teoria liczb, PWN Warszawa 2003
2. M. Kutyłowski, W. Strothmann, Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych, Wydawnictwo READ ME, 1999
3. W. Sierpiński, Teoria liczb, MM tom 19, IM PAN, Warszawa 1950
4. D.R. Stinson, Kryptografia w teorii i w praktyce, WNT, Warszawa 2005

Result of average student's workload

Activity	Time (working hours)

Student's workload

Source of workload	hours	ECTS
Total workload	90	4
Contact hours	60	2
Practical activities	30	2