STUDY MODULE DESCRIPTION FORM

Name of the module/subject **Number Theory and Cryptography**		Code
Field of study **Mathematics in Technology**	Profile of study (general academic, practical) **general academic**	Year /Semester **3 / 6**
Elective path/specialty **Modelling in technology**	Subject offered in: **Polish**	Course (compulsory, elective) **elective**
Cycle of study: **First-cycle studies** **(Polish Qualifications Framework level six)**	Form of study (full-time,part-time) **full-time**	
No. of hours Lecture: **15** Classes: **15** Laboratory: **-** Project/seminars: **-**		No. of credits **2**
Status of the course in the study program (Basic, major, other) **basic**	(university-wide, from another field) **university-wide**	
Education areas and fields of science and art **Technical sciences** **Technical sciences**		ECTS distribution (number and %**)** **2 100%** **2 100%**

Responsible for subject / lecturer:

Dr Anna Iwaszkiewicz-Rudoszańska
email: anna.iwaszkiewicz-rudoszanska@put.poznan.pl
tel. 61 665 2812
Faculty of Electrical Engineering
ul. Piotrowo 3A, 60-965 Poznań

Prerequisites in terms of knowledge, skills and social competencies:

1	**Knowledge**	Basic knowledge of algebra and discrete mathematics. [K_W01 (P6S_WG)]
2	**Skills**	Logical and scientific thinking. [K_U01 (P6S_UW), K_U02 (P6S_UW)]
3	**Social competencies**	Understanding the necessity of expanding own competences. [K_K01 (P6S_KK), K_K02 (P6S_KK)]

Assumptions and objectives of the course:

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

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

Knowledge:

1. Formulates definitions and theorems from number theory used in discussed cryptographic algorithms – [K_W01 (P6S_WG)]

2. Explaines basic concepts of public key cryptography and give an account of different cryptosystems - [K_W06 (P6S_WG)]

Skills:

1. Performs calculations necessary for encryption and decryption in discussed cryptographic systems. – [K_U03 (P6S_WG), K_U04 (P6S_UW)]

2 Uses theorems from number theory and algebra in the analysis of cryptographic systems. Justifies the correctness of selected cryptographic systems . – [K_U01 (P6S_WG), K_U03 (P6S_UW)]

Social competencies:

1. Knows the limits of her/his own knowledge and understands the need for further education. - [K_K02 (P6S_KK)]
2. Is aware of the limitations of contemporary cryptography. – [K_K01 (P6S_KK)]

Assessment methods of study outcomes

Lecture: Test at the end of semester.

Exercises: Continuous evaluation, including homeworks. Two tests in the middle and at the end of semester.

Course description

Congruences (Chinese Remainder Theorem. Fermat's Little Theorem, Euler's function, Euler's Theorem). 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.

Update 28.10.2018

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

Result of average student's workload

Activity	Time (working hours)
1. lectures	15
2. exercises	15
3. consultations	4
4. preparation for exercise classes	15
5. preparation for the credit of exercise classes	6
6. preparation for the credit of lectures	5

Student's workload

Source of workload	hours	ECTS
Total workload	60	2
Contact hours	34	1
Practical activities	15	1