Poznan University of Technology **E**uropean **C**redit **T**ransfer **S**ystem
Faculty of Electrical Engineering

STUDY MODULE DESCRIPTION FORM

Name of the module/subject **Cryptography**		Code **1010335421010331905**
Field of study **Information Engineering**	Profile of study (general academic, practical) **(brak)**	Year /Semester **1 / 2**
Elective path/specialty **-**	Subject offered in: **polish**	Course (compulsory, elective) **obligatory**
Cycle of study: **Second-cycle studies**	Form of study (full-time,part-time) **part-time**	
No. of hours Lecture: **16** Classes: **-** Laboratory: **12** Project/seminars: **-**		No. of credits **5**
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 **technical sciences**		ECTS distribution (number and %**)** **5 100%**

Responsible for subject / lecturer:

dr inż. Anna Grocholewska-Czuryło
email: anna.grocholewska-czurylo@put.poznan.pl
tel. 61-665 35 31
Wydział Elektryczny
ul. Piotrowo 3A 60-965 Poznań

Prerequisites in terms of knowledge, skills and social competencies:

1	**Knowledge**	Has extended and deepened knowledge in the area of selected mathematical topics. Has deepened knowledge in the area of data security.
2	**Skills**	Is able to propose and justify improvements to existing information technology solutions.
3	**Social competencies**	Is able to think and act in a creative and entrepreneurial way.

Assumptions and objectives of the course:

Presentation of cryptographic primitives, algorithms, and services.

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

Knowledge:

1. Has deepened knowledge in the area of cryptographu and basic knowledge of cryptanalysis. - [K_W11]

Skills:

1. Is able to integrate knowledge from various scientific domains and disciplines while formulating and solving computer science problems. - [K_U07]

Social competencies:

1. Is able to think and act in a creative and entrepreneurial way. - [K_K01]

Assessment methods of study outcomes

Written or/and oral examination based on lecture.

Laboratory: written test.

Course description

Cryptographic primitives. Block ciphers, designing block ciphers. Pseudorandom sequences generators, their components, randomness of sequences, linear complexity. Stream ciphers, synchronous and self-synchronizing. Exponential ciphers. Hash functions: dedicated, based on block ciphers and using modular arithmetic; attacks on hash functions. Digital signatures; DSA and El Gamal schemes, signatures based on elliptic curves. Authentication: zero-knowledge proofs. Nonrepudiation.

Laboratory:

Cryptographic criteria of S-box design ? S-box testing. Tests and pseudorandom sequences generators. Digital signature protocols. Cryptographic protocols. Steganographic algorithms.

Basic bibliography:

1. Wprowadzenie do kryptografii, Buchmann J. A., Wydawnictwo Naukowe PWN, Warszawa, 2006

2. Bezpieczeństwo danych w systemach informatycznych, Stokłosa J., Bilski T., Pankowski T., Wydawnictwo Naukowe PWN, Warszawa-Poznań, 2001

Additional bibliography:

1. Fundamentals of Computer Security, Pieprzyk J., Hardjono T., Seberry J., Springer, Berlin, 2003

2. Kryptografia dla praktyków, Schneier B., WNT, Warszawa, 2002

3. Kryptologia. Budowa i łamanie zabezpieczeń, Wobst R., Wydawnictwo RM, Warszawa, 2002

4. Kryptografia w praktyce, Ferguson N., Schneier B., Helion, Gliwice, 2004

Result of average student's workload

Activity	Time (working hours)
1. Lecture	30
2. Current work on lectures	15
3. Laboratory	15
4. Preparation to the laboratory	15
5. Preparation to the tests	10
6. Preparation of laboratory reports	10
7. Preparation to the examination	20
8. Pasrticipation in consultations and examination	10

Student’s workload

Source of workload	hours	ECTS
Total workload	125	5
Contact hours	50	2
Practical activities	50	2