Title **Cryptology**	Code **1010332431010330742**
Field **Computer Science**	Year / Semester **2 / 3**
Specialty **Security of IT systems**	Course **core**
Hours Lectures: **2** Classes: **-** Laboratory: **-** Projects / seminars: **-**	Number of credits **6**
	Language **polish**

Lecturer:

dr hab. inż. Janusz Stokłosa
Instytut Automatyki i Inżynierii Informatycznej
tel. +48 61 665 37 57
e-mail: janusz.stoklosa@put.poznan.pl

Faculty:

Faculty of Electrical Engineering
ul. Piotrowo 3A
60-965 Poznań
tel. (061) 665-2539, fax. (061) 665-2548
e-mail: office_deef@put.poznan.pl

Status of the course in the study program:

- Obligatory course at the Faculty of Electrical Engineering, field of study Computer Science

Assumptions and objectives of the course:

- Presentation of cryptographic primitives, algorithms, and services.

Contents of the course (course description):

Cryptographic primitives. Block ciphers, designing block ciphers. Pseudorandom sequences generators, their components, randomness of sequenaces, 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.

Introductory courses and the required pre-knowledge:

- Algebra, arithmetic, data security

Courses form and teaching methods:

- Lecture.

Form and terms of complete the course - requirements and assessment methods:

- Written or/and oral examination based on lecture.

Basic Bibliography:

-

Additional Bibliography:

-