STUDY MODULE DESCRIPTION FORM

Name of the module/subject **Cryptanalysis**	Code **1010332431010337158**

Field of study **Information Engineering**	Profile of study (general academic, practical) **general academic**	Year /Semester **2 / 3**
Elective path/specialty **Safety of Computer Systems**	Subject offered in: **polish**	Course (compulsory, elective) **obligatory**

Cycle of study: **Second-cycle studies**	Form of study (full-time,part-time) **full-time**

No. of hours Lecture: **1** Classes: **-** Laboratory: **1** Project/seminars: **-**	No. of credits **3**

Status of the course in the study program (Basic, major, other) **other**	(university-wide, from another field) **university-wide**

Education areas and fields of science and art **technical sciences**	ECTS distribution (number and %**)** **3 100%**

Responsible for subject / lecturer:

dr inż. Krzysztof Chmiel
email: krzysztof.chmiel@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**	K_W01: has basic knowledge in the field of mathematics, containing algebra, analysis, logic, probability theory, as well as elements of discrete and applied mathematics. K_W04: has systematized and improved theoretically knowledge in the domain of basic algorithms and their analysis, technics of algorithm design, abstract data structures and their implementation, and also computationally hard problems.
2	**Skills**	K_U01: is able to gain (inquire) information from literature, data bases and other sources; is able to integrate acquired information, interpret it, as well as to draw conclusions and also formulate and defend opinions. K_U06: is able to communicate in English, and also to read descriptions and instructions concerning electronic devices, computer hardware and software tools, and similar documents.
3	**Social competencies**	K_K02: is aware of importance and understands beyond technical aspects and consequences of computer science engineer activiti , as well as of responsibility for making decisions. K_K04: is aware of responsibility for individual work, and also is prepared to respect the rules of collective work, and to bear responsibility for collective projects.

Assumptions and objectives of the course:

Knowledge of methods of the differential and the linear cryptanaysis, and also of their extensions, in the scope of generation of the best characteristics as well as identification of the key of a block cipher algorithm.

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

Knowledge:

1. Has systematized and improved theoretically knowledge in the domain of data protection and security of computer systems. - [K_W13]

Skills:

1. Can prepare technical report concerning the realization of the engineering task, and also is able to prepare a text containing the discussion of the results. - [K_U03]

2. Can apply appropriate methods of data protection and ensure a computer system security. - [K_U17]

Social competencies:

1. Is aware of responsibility for individual work, and also is prepared to respect the rules of collective work, and to bear responsibility for collective projects. - [K_K04]

2. Is aware of importance: of the project realization precision, of notational standards, of language correctness, and of task punctuality. - [K_K07]

Assessment methods of study outcomes

Lecture: written exam.

Laboratory exercises: credit for realized exercises and elaborated reports.

Course description

Lectures: Differential and linear approximation of block ciphers. Approximation table computing algorithms. Approximation of random S-boxes. Approximation of arithmetic sum and subtraction functions. Evaluation of a block cipher quality. Intermediate evaluation of the DES algorithm. Differential cryptanalysis of the DES algorithm. Linear cryptanalysis of the DES algorithm. Differential-linear cryptanalysis. Extensions of the differential cryptanalysis. Extensions of the linear cryptanalysis.

Laboratory program: Differential cryptanalysis of the substitution blocks Si. Linear cryptanalysis of the Si substitution blocks. Differential cryptanalysis of the f base function. Linear cryptanalysis of the f base function. Differential cryptanalysis of the DES1 and DES2 algorithms. Linear cryptanalysis of the DES1 and DES2 algorithms. Differential cryptanalysis of the DES3 and DES4 algorithms. Linear cryptanalysis of the DES3 and DES4 algorithms. Differential cryptanalysis of the DES5 and DES6 algorithms. Linear cryptanalysis of the DES5 and DES6 algorithms.

Basic bibliography:

1. Ochrona danych i zabezpieczenia w systemach teleinformatycznych, J. Stokłosa (red.), Wydawnictwo Politechniki Poznańskiej, 1?214, Poznań, 2003, 2005.

2. Metody różnicowej i liniowej kryptoanalizy szyfrów blokowych, K. Chmiel, Rozprawa habilitacyjna Nr 443, Wydawnictwo Politechniki Poznańskiej, 1?212, Poznań, 2010.

Additional bibliography:

1. Ćwiczenie z kryptoanalizy różnicowej algorytmu DES. Program CWAR, K. Chmiel, Raport 498, IAII PP, 1?89, Poznań 2004.

2. Ćwiczenie z kryptoanalizy liniowej algorytmu DES. Program CWAL, K. Chmiel, Raport 499, IAII PP, 1?87, Poznań 2004.

Result of average student's workload

Activity	Time (working hours)
1. Lectures.	15
2. Laboratory exercises.	15
3. Consultations and examination.	20
4. Preparation to laboratory exercises and elaboration of reports.	15
5. Preparation to tests and examination.	10

Student’s workload

Source of workload	hours	ECTS
Total workload	75	3
Contact hours	50	2
Practical activities	25	1