STUDY MODULE DESCRIPTION FORM

Name of the module/subject **Security in Wireless Networks**		Code **1010802131010812928**
Field of study **Electronics and Telecommunications**	Profile of study (general academic, practical) **general academic**	Year /Semester **2 / 3**
Elective path/specialty **Information and Communication**	Subject offered in: **English**	Course (compulsory, elective) **elective**
Cycle of study: **Second-cycle studies**	Form of study (full-time,part-time) **full-time**	
No. of hours Lecture: **1** Classes: **-** Laboratory: **2** Project/seminars: **-**		No. of credits **2**
Status of the course in the study program (Basic, major, other) **major**	(university-wide, from another field) **from field**	
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 inż. Piotr Remlein
email: remlein@et.put.poznan.pl
tel. 665-3934
Wydział Elektroniki i Telekomunikacji
ul. Piotrowo 3A 60-965 Poznań

Prerequisites in terms of knowledge, skills and social competencies:

1	**Knowledge**	K2_W06: Has a systematic, advanced knowledge of contemporary mobile communication systems and state-of-the-art techniques applied in these systems K2_W05: Has a systematic knowledge, together with the necessary mathematical background, related to information and coding theory K2_W00: Has extended, in-depth knowledge of those branches of mathematics which are used in formulating and solving problems in electronic and telecommunications
2	**Skills**	K2_U01: Is able to communicate English, to discuss professional matters and to use knowledgeably English language professional sources. K2_U02: Is able to write a short paper, in Polish or English, on a technical subject from his/her field of study. Is able to present a problem from his/her field of study and a solution to this problem, and participate in the discussion to follow K2_U08: Is oriented in rules of activities in the area of standardization, knows Polish and international standardization bodies (ITU, ISO, ETSI, CISPR, 3GPP, etc.).
3	**Social competencies**	K2_K06: Demonstrates responsibility for designed electronic and telecommunication systems. Is aware of the hazards they pose for individuals and communities if they are improperly designed or produced K2_K03: Understands the legal framework of Polish and international standards in electronics and telecommunication

Assumptions and objectives of the course:

The main aim of the lecture is introduction to cryptographic methods in wireless communications and computer systems

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

Knowledge:

1. Has a practical knowledge of safety systems or methods which ensure safety of information transmitted in computer networks and mobile networks. - [K2_W12]

2. Has a systematic, advanced knowledge of contemporary mobile communication systems and state-of-the-art techniques applied in these systems. - [K2_W06]

3. Has a wide, systematic knowledge, with necessary mathematical background, of ICT networks and signal transmission methods. - [K2_W13]

Skills:

1. Is able to use and/or design professional monitoring and safety systems in various telecommunication systems and networks. - [K2_U14]
2. Knows the rules of operation of Polish and international standardization bodies (ITU, ISO, ETSI, CISPR, 3GPP, etc.). Knows the standardization procedures. - [K2_U08]
3. Is able to prepare a scientific paper or technical report and give a presentation (in English or in Polish) on solving a problem in the area of electronics and/or telecommunication; is able to participate in a discussion related to the presented problem. - [K2_U02]

Social competencies:

1. Understands the legal framework of Polish and international standards in electronics and telecommunications. - [K2_K03]
2. Is aware of the necessity to approach solving technical problems with responsibility and professionalism. - [K2_K05]
3. Is aware of the main challenges facing electronics and telecomunication in the 21st century. Is aware of the impact electronics and ICT systems and networks will have on the development of the information society. - [K2_K07]

Assessment methods of study outcomes

Lectures in the form of multi-media presentations and laboratory.

Individual projects, written exam.

Course description

Lectures: Presentation of threats and corresponding security solutions in wireless networks. Adequate information security services and mechanisms will be presented. The taxonomy of wireless network attacks and protection procedures will be shown. Data security in wireless data transmission systems: GSM, UMTS, TETRA, WLAN 802.11, WiMax, Bluetooth, 802.15.4, DTN. Security policy. Basic terminology and concepts in cryptography. Classical ciphers (Cesear, Playfair, Vigenaire, Vernam, ideal ciphers, substitution ciphers, transposition ciphers). Symmetric cryptography and block ciphers (DES, AES). Public key ciphers (RSA, ElGamal's). Hash functions and data integrity. Attacks on cryptographic systems and elements of cryptoanalysis. IDS systems.

Laboratory: Designing individual projects with classical ciphers.

Basic bibliography:

1. Network Security, Christos Douligeris, Dimitrios N. Serpanos, John Wiley & Sons, 2007
2. Information Security Management Handbook, Krause M., Tipton H.F, (Fourth Edition), CRC Press - Auerbach Publications, 1999
3. 3GPP Specifications: TS 23.002 v3.0.0, TS 23.002 v4.0.0, TS23.002 v5.0.0, TS 22.105 v3.10.0, www. 3gpp. org
4. Materials from IEEE journals and conferences

Additional bibliography:

1. Cryptography in C and C++, M. Welschenbach, APress, 2001.
2. Specification Volume 1, 2, Specification of the Bluetooth System, Version 1.1, February 2001
3. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press 1997

Result of average student's workload

Activity	Time (working hours)
1. Lecture	15
2. Project	30
3. Preparations for the project/labs	15
4. Preparation for the completion of the course	10
5. Consultations	3
6. participation in completion of the course	2

Student's workload

Source of workload	hours	ECTS
Total workload	75	2
Contact hours	50	2
Practical activities	45	1