

| | |
|---|--------------------------------------|
| Title Security in Wireless Networks | Code POZ04WTS2ICE33 |
| Field Electronics and Telecommunications | Year / Semester 2 / spring |
| Specialty Information and Communication Technologies | Course elective |
| Hours Lectures: 1 Classes: - Laboratory: 2 Projects / seminars: | Number of credits 2 |

Lecturer:

dr inż. Piotr Remlein
Katedra Radiokomunikacji
tel. (061) 665-3934, fax. (061) 665-3823
e-mail: janusz.kleban@et.put.poznan.pl

Faculty:

Faculty of Electronics and Telecommunications
ul. Piotrowo 3A
60-965 Poznań
tel. (061) 665-2293, fax. (061) 665-2572
e-mail: office_det@put.poznan.pl

Status of the course in the study program:

Elective course for students of Electronics and Telecommunications,
specialization Wireless Communications

Objectives of the course:

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

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.

Initial knowledge:

Basic knowledge of computer networks, wireless transmission systems, programming languages and mathematics.

Teaching methods:

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

Assessment methods:

Individual projects, written exam.

Bibliography:

1. 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

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.
4. Welschenbach M., *Cryptography in C and C++*, APress, 2001
5. Douligeris Ch., Serpanos D.N., *Network Security Current Status and Future Directions*, J. Wiley & Sons, 2007