Rzeszów University of Technology

The Faculty of:	Faculty of Electrical and Computer Engineering
Field of study:	Electronics and Telecommunications
Speciality:	
Study degree (BSc, MSc):	First circle full time studies

COURSE UNIT DESCRIPTION

Course title:	Cryptography and secutity of data
Lecturer responsible for course: dr. Kazimierz Lal **Contacts: phone: 48178651767** **e-mail: klal@prz-rzeszow.pl**	
Department : Department of Electrical Engineering and Informatics	

Semester	**Weekly load**	**Type of classes**				**Number of ECTS credits**
		L Lectures	**C Theoretical Classes**	**Lb Laboratory**	**P Project**	
6	3	30		15		3

Course description
Lecture: Introduction to the security of computer systems - user consciousness, basis of cryptography, code types, data encryption modes. Present cryptography algorithms - symetric algorithms, algorithms with public key, digital signature, messages entity authentication codes. Public key infrastructure - X.509, Certification Authority, PKI elements. Entity authentication and autorisation in Linux, Unix and Windows operating systems. Data security - file encription, digital signature, Redundant Array of Independent Disks, devices and application to data protection, Uninterruptible Power Supply. Data transmission security - PGP, S/MIME, SSL/TLS, SSH, IPSec protocols. Firewall types. Using OpenSSL to: files encryption, keys generating, digital signature, creation of Certification Authority, certificates generating for presentation servers (WWW). Security communication with remote computer by using Secure Shell.
Classes:

Laboratory:
Installation of authorization centre - Windows 2008 server.

e-Directory on SLES10 server installation.

Installation and configuration of IPSec connections for chosen operating system.

Installation, configuration and tests of data storage matrix.

Firewall configuration and tests.

Installation and tests of selected tools to the workstation data encryption.

Tools to testing computer networks security.

Project:

Objectives of the course
Student should obtain theoretical knowledge and practical understanding of subject and skill of maintaining security computer networks.
Examination method
Final examination, oral or written test on each laboratory, credit test from laboratory.

Bibliography
Kutyłowski M., Strothmann W.: Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych. Oficyna Wydawnicza Read Me. Warszawa 1999; Mochnacki W.: Kody korekcyjne i kryptografia. Oficyna Wydawnicza Politechniki Wrocławskiej. Wrocław 2000; Stallings W.: Ochrona danych w sieci i intersieci – w teorii i praktyce. WNT Warszawa 1997; Stokłosa J., Bilski T., Pankowski T.: Bezpieczeństwo danych w systemach informatycznych. PWN Warszawa 2001; Welschenbach M.: Kryptografia w C i C++. Mikom Warszawa 2002; Sportack M.: Sieci komputerowe Księga eksperta, Wydanie II – poprawione, HELION 2004; Hunt C.: TCP/IP - Administracja sieci, RM 2003 ; Lal K., Rak T.: Linux a technologie klastrowe, PWN-MIKOM, 2005; Lal K., Rak T.: Po prostu własny serwer internetowy, HELION, 2002; Rak T.: Tworzenie sieci komputerowej. Ćwiczenia praktyczne, HELION, 2006.

Lecturer signature	
Head of Department signature	
Dean signature	