Faculty of Fundamental Problems of Technology

COURSE CARD

Name in polish	:	**Kryptografia i Bezpieczeństwo**
Name in english	:	**Cryptography and Security**
Field of study	:	Computer Science
Specialty (if applicable)	:	
Undergraduate degree and form of	:	masters, stationary
Type of course	:	compulsory
Course code	:	E2_BI04
Group rate	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	60	30			
The total number of hours of student workload (CNPS)	90	90			
Assesment	exam				
For a group of courses final course mark	X				
Number of ECTS credits	3	2			
including the number of points corresponding to the classes of practical (P)		2			
including the number of points corresponding occupations requiring direct contact (BK)	3	2			

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

knowledge of the basics of cryptology

COURSE OBJECTIVES

C1 Presentation of the complexity of the problem of introducing of a new cryptographic system, and of ensuring its security.

C2 Teaching selected methods and best practices supporting implementation of a new cryptographic system or product.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows the life cycle of a cryptographic component and the basic security rules applying to consecutive phases of the cycle.

W2 Knows basic principles of formalizing and documenting security requirements for a cryptographic product.

W3 Knows exeplary security gaps of some cryptographic standards and implementations.

The student skills:

U1 Is able to indicate security standards relevant for a given product.

U2 Is able to prepare an effective plan of tests.

U3 Is able to utilize her/his own cryptographic knowledge to design protocols and data structures used in the documentation of a future cryptographic product.

The student's social competence:

K1 Is aware of development costs of secure systems and proposes adequate solutions for achieving security goals.

K2 Acknowledges the need of usage of a revision control system and of an issue tracking system when developing documentation of a security product.

K3 Is aware of the progress in cryptanalysis of some of the existing systems and is aware of the risk of making mistakes in the design or implementation of a cryptographic system.

COURSE CONTENT

Type of classes - lectures		
Wy1	The life cycle of a cryptographic component. Formalizing security requirements: protection profiles and security targets.	6h
Wy2	An example of implementation of a complex security system: new German e-ID card (introduction).	1h
Wy3	Various types of public documents supporting implementation of the new German e-ID card.	2h
Wy4	The role of standards for a new security systems. Standards utilized in the German e-ID system.	3h
Wy5	Security gaps in some (currently withdrwan) security standards: security failures of some RSA-padding standards.	8h
Wy6	An attack on implementation of encoding used in RSA - the case of Estonian e-ID card.	2h
Wy7	SSL protocol and dangers connected with CBC encryption mode.	2h
Wy8	Authentication of a server or of a user: certificates and the Public Key Infrastructure (PKI): trust hierarchy and risks.	4h
Wy9	An example of a weak, crucial security component: md5 hash function and creation of a rogue CA certificate.	2h
Wy10	PKI and the series of PKCS standards.	6h
Wy11	CRL, OCSP protocols, and card verifiable certificates.	2h
Wy12	EMV standard for payment cards, "Chip and PIN is broken".	4h
Wy13	Terminals for payment cards: "Optimised to Fail: Card Readers for Online Banking".	2h
Wy14	The need for Hardware Security Modules (HSMs) as security components for high risk transactions - cache attacks on a general purpose computer performing cryptographic computations.	6h
Wy15	HSMs and scalability problems. The issue of trust. Backdoors, kleptography, bug-attacks.	6h
Wy16	Randomness ensured for cryptographic operations. Report eprint.iacr.org/2012/064 and the case of Sony PS3.	2h
Wy17	Summary of the lectures.	2h
Type of classes - exercises		
Ćw1	Writing a protection profile of a chosen security product.	8h
Ćw2	Preparation of deployment documentation for a chosen cryptographic protocol (high level documentation): descryption of protocols, data structures for communication (ASN.1), APDUs, used standards.	8h
Ćw3	Building a prototype based on an open source cryptographic library.	8h
Ćw4	Preparation of a "Test Plan" (incorrect input data must also be taken into account), writing documentation of the tests performed.	6h

Applied learning tools

1. Traditional lecture
2. Solving tasks and problems
3. Creating programming projects
4. Consultation
5. Self-study students

EVALUATION OF THE EFFECTS OF EDUCATION ACHIEVEMENTS

Value	Number of training effect	Way to evaluate the effect of education
F1	W1-W3, K1-K3	evaluation of student's answers given in the examination form
F2	U1-U3, K1-K3	evaluation of the outcome of the exercises produced by the examined student
P=50%*F1+50%*F2		

BASIC AND ADDITIONAL READING

1. BSI, The PP/ST Guide
2. BSI, Guidelines for Developer Documentation according to Common Criteria Version 3.1
3. BSI, TR-03105 Part 3.3 Test plan for eID-Cards with Advanced Security Mechanisms EAC 2.0
4. John Kelsey, Crypto Strength and Attacks (slides), NIST Workshop on Cryptography for Emerging Technologies and Applications, 2011
5. C. Ellison, B. Schneier: Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure, Computer Security Journal, v 16, n 1, 2000, pp. 1-7
6. Carlisle Adams, Mike Just, PKI: Ten Years Later, Proceedings of the 3rd Annual PKI Research Workshop, PKINIST2004
7. Jan Meier, Dieter Gollmann: Caught in the Maze of Security Standards. ESORICS 2010: 441-454
8. RSA Laboratories, Public-Key Cryptography Standards (PKCS)
9. Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, Christophe Wachter: Ron was wrong, Whit is right, Cryptology ePrint Archive: Report 2012/064

SUPERVISOR OF COURSE

dr Przemysław Kubiak

RELATIONSHIP MATRIX EFFECTS OF EDUCATION FOR THE COURSE
Cryptography and Security
WITH EFFECTS OF EDUCATION ON THE DIRECTION OF COMPUTER SCIENCE

Course training effect	Reference to the effect of the learning outcomes defined for the field of study and specialization (if applicable)	Objectives of the course**	The contents of the course**	Number of teaching tools**
W1	K2_W06 K2_W12_S2BKM K2_W13_S2BKM	C1	Wy1-Wy17	1 4 5
W2	K2_W07 K2_W12_S2BKM K2_W13_S2BKM	C1	Wy1-Wy17	1 4 5
W3	K2_W04 K2_W12_S2BKM K2_W13_S2BKM	C1	Wy1-Wy17	1 4 5
U1	K2_U01 K2_U16 K2_U23_S2BKM K2_U24_S2BKM	C2	Ćw1-Ćw4	2 3 4 5
U2	K2_U08 K2_U18 K2_U23_S2BKM K2_U24_S2BKM	C2	Ćw1-Ćw4	2 3 4 5
U3	K2_U12 K2_U23_S2BKM K2_U24_S2BKM	C2	Ćw1-Ćw4	2 3 4 5
K1	K2_K13 K2_K18	C1 C2	Wy1-Wy17 Ćw1-Ćw4	1 2 3 4 5
K2	K2_K08 K2_K11 K2_K18	C1 C2	Wy1-Wy17 Ćw1-Ćw4	1 2 3 4 5
K3	K2_K12 K2_K18	C1 C2	Wy1-Wy17 Ćw1-Ćw4	1 2 3 4 5