**Nazwa przedmiotu:**

Cryptography and Information Security

**Koordynator przedmiotu:**

prof. nzw. dr hab. Tomasz Adamski

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia I stopnia

**Program:**

Computer Science

**Grupa przedmiotów:**

Technical Courses

**Kod przedmiotu:**

ECRYPT

**Semestr nominalny:**

7 / rok ak. 2015/2016

**Liczba punktów ECTS:**

6

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

1. Contact Hours - 70h;
a. presence in the lectures – 30 h
b. presence in the tutorials - 15 h
c. presence in the project classes – 15 h
d. consultations – 10 h

2. Preperation to classes – 80h:
a. preparation to the lectures – 40 h
b. preparation to the tutorials - 20 h
c. preparation to the project – 20 h

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

3

**Język prowadzenia zajęć:**

angielski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

3

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład:  | 30h |
| Ćwiczenia:  | 15h |
| Laboratorium:  | 0h |
| Projekt:  | 15h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

**Limit liczby studentów:**

50

**Cel przedmiotu:**

After the course students should understand cryptographic objectives, algorithms, methods and protocols. Students should also learn to solve security problems in real information systems.

**Treści kształcenia:**

Lectures
1. Short introduction to cryptography and data security (2h): cryptographic objectives and primitives, overview of data security problems, alphabet, language, codes, ciphers, private key ciphers, public key ciphers, block ciphers, stream ciphers, product ciphers, one way functions, permutation ciphers, substitution ciphers, homophonic substitution ciphers, polyalphabetic substitution ciphers, classical ciphers (linear and affine ciphers, Hill cipher, Caesar cipher, Playfair cipher, Vigenere cipher, Enigma), ideal ciphers (Vernam cipher), ciphers and information theory approach, Shannon theorem.
2. Mathematical methods in cryptography (4h): divisibility, congruencies, Euler’s theorem, GCD and extended Euclid’s algorithm, Chinese Remainder Theorem, abstract algebra, group theory, discrete logarithm, commutative rings and fields, elliptic curves, point lattices, computational complexity and NP hard problems (integer factorization problem, discrete logarithm problem, Diffi-Hellmann problem).
3. Public key ciphers (4h): RSA, ElGamal, Rabin, Massey-Omura cipher, probabilistic PK ciphers, elliptic curve based ciphers, point lattice based ciphers, Mc Eliece and correcting codes based ciphers, knapsack public key ciphers, generation of public key cipher parameters.
4. Private key ciphers(4h): permutation-substitution networks, avalanche effect, Feistel cipher, round, S-boxes, general private key cipher structures, DES, 3DES, DESX, AES, IDEA, FEAL, Twofish, Blowfish, MARS, CAST 256, SAFER, Serpent, Camelia, RC5, RC6, TEA.
5. Stream ciphers and ciphering modes (2h): stream ciphers based on LFSRs, RC4 stream cipher, ECB, CBC, OFB, CFB.
6. Hash functions and data integrity (2h): properties and classification of hash functions, relationships between the properties, MDC and MAC hash functions, MD5, SHA-1, Whirlpool, Chaum-van Heijst-Pfitzmann hash functions, hash functions based on block ciphers (Rabin method, Davis method, Matyas–Meyer–Oseas method), birthday paradox and cryptanalysis of hash functions.
7. Document authentication (digital signatures) (2h): basic digital signatures properties, different kinds of digital signatures, one time signatures, RSA signatures, ElGamal signatures (classical and on groups), DSA standard, Schnorr signatures, blind signatures, undeniable signatures, fail-stop signatures.
8. Entity authentication (identification) (2h): password methods (weak authentication), challenge-response methods (strong authentication), zero knowledge algorithms, Fiat-Shamir algorithm, Feige-Fiat-Shamir algorithm, Guillou-Quisquater algorithm, digital signatures based on zero knowledge authentication algorithms.
9. Secret sharing (1h): trivial secret sharing, Shamir scheme, Blakley scheme, Chinese Remainder Theorem based secret sharing.
10. Effective implementation of cryptographic algorithms (1h): fast exponentiations algorithms, fast GCD computations, binary extended Euclid algorithm, fast algorithms for multiple–precision residual and integer arithmetic, Barrett algorithm, Mongomery algorithm, specialized hardware solutions.
11. Random and pseudorandom numbers generators for cryptographic aims (1h): true random number generators (TRNG) and pseudorandom number generators (PRNG), ANSI X9.17, FIPS 186 generator, Micalli-Schnorr generator, RSA generator, BBS generator.
12. Primality testing and prime numbers generators: probabilistic and deterministic primality tests, Erastotenes sieve, Solovay-Strassen algorithm, Miller-Rabin algorithm, deterministic tests, AKS primality test
13. Key distribution algorithms and protocols (1h): Diffi-Hellman algorithm, TTP, Wide Mouth Frog Protocol, Needham-Schroeder protocol.
14. Key management (1h): Public Key Infrastructure (PKI) and Certificate Authority (CA).

Tutorials
Classical ciphers and cryptanalysis of classical ciphers (2h): Caesar cipher, Vigenere cipher, Enigma, linear and affine ciphers.
Congruencies (2h): properties of congruencies, set of congruencies, GCD and GCD complexity, Chinese Remainder Theorem and RNS (Residue Number System), quadratic residues.
Abstract algebra (6h): basic properties of groups, multiplicative groups, rings and cyclic groups, discrete logarithms in cyclic groups, rings, finite fields, inverses in rings and finite fields, computations in finite fields and rings, Hamming distance and basic concepts of correcting codes, quotient rings and ideals
Public key ciphers (2h): Examples of public key ciphers (RSA, ElGamal, Rabin) with small parameters
Digital signatures (2h): Examples of digital signatures (RSA, ElGamal) with small parameters

Project
Introduction (4h): some comments on individual projects prepared for students, how to solve practical cryptographic and information security problems, how to use cryptographic libraries (NTL, Cryptlib and so on).
Typical projects are software or hardware implementations (with VHDL description and simulation) of chosen cryptographic algorithms.
The project is done in two steps. The first step is the introductory implementation, the second is the final project presentation. Mid-term acceptance of the project is obligatory.

**Metody oceny:**

There are 3 mid-term tests (during lectures). Maximum score for every mid-term test is 20 points. For the project it is possible to score up to 40 points. For the exam it is possible to score up to 100 points. Additional extra points can be obtained for solving problems during tutorials (2 points for one solved problem) and for homework (5 points for one solved problem).
The final result is based on the following pattern:
• 5.0: 180-200 (or more) points
• 4.5: 160-179 points
• 4.0: 140-159 points
• 3.5: 120-139 points
• 3.0: 100-119 points
• 2.0: 0-99 points

**Egzamin:**

tak

**Literatura:**

[1] A.Menezes, P.van Oorsschot, S.Vanstone; Handbook of Applied Cryptography; CRC Press 1996.
[2] J.Buchmann; Introduction to cryptography; Springer Verlag, 2007, Berlin, Heidelberg 2007.
[3]. V.Shoup; A Computational Introduction to Number Theory And Algebra, Cambridge University Press, Cambridge 2005.
[4] T.Adamski; Cryptography and Information Security; Lecture Notes in PDF format (lecture web site)
[5] T.Adamski; Tutorals from Cryptography and Information Security; in PDF format (lecture web site)

**Witryna www przedmiotu:**

studia.elka.pw.edu.pl/ind

**Uwagi:**

## Efekty przedmiotowe

### Profil ogólnoakademicki - wiedza

**Efekt ECRYP\_W01:**

Student has a broader and deeper knowledge of mathematics (number theory, algebra, probability theory) allowing for the design of secure telecommunication and/or computer systems.

Weryfikacja:

Exam, evaluation of homework, evaluation of project.

**Powiązane efekty kierunkowe:** K\_W01

**Powiązane efekty obszarowe:** T1A\_W01, T1A\_W02, T1A\_W03, T1A\_W07

**Efekt ECRYP\_W02:**

Student has a basic understanding of the role of standardization and techniques to ensure the security of networks

Weryfikacja:

Exam, project

**Powiązane efekty kierunkowe:** K\_W16

**Powiązane efekty obszarowe:** T1A\_W03, T1A\_W07

**Efekt ECRYP\_W03:**

Student has detailed knowledge of cryptography and information security systems

Weryfikacja:

Exam, evaluation of homework, evaluation of project.

**Powiązane efekty kierunkowe:** K\_W17

**Powiązane efekty obszarowe:** T1A\_W04, T1A\_W07

### Profil ogólnoakademicki - umiejętności

**Efekt ECRYP\_U01:**

Student is able to synthesize information from different sources

Weryfikacja:

Exam, project

**Powiązane efekty kierunkowe:** K\_U01

**Powiązane efekty obszarowe:** T1A\_U01

**Efekt ECRYP\_U02:**

Student can use mathematical apparatus, known methods and algorithms for solving engineering problems

Weryfikacja:

Exam, evaluation of homework, evaluation of project.

**Powiązane efekty kierunkowe:** K\_U08

**Powiązane efekty obszarowe:** T1A\_U08, T1A\_U09

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt ECRYP\_K01:**

 Student understands the need for continuous education

Weryfikacja:

Project

**Powiązane efekty kierunkowe:** K\_K01

**Powiązane efekty obszarowe:** T1A\_K01

**Efekt ECRYP\_K02:**

Student is aware of the social role of graduate of good technical university

Weryfikacja:

Difficult to be verified

**Powiązane efekty kierunkowe:** K\_K06

**Powiązane efekty obszarowe:** T1A\_K07