Faculty of Information and Communication Technology/Department of Fundamentals of Computer Science

COURSE CARD

| | | |
|---|---|---|
| Name of the course in polish | : | **Kryptografia** |
| Name of the course in english | : | **Cryptography** |
| Field of study | : | Algoritmic Computer Science |
| Specialty (if applicable) | : | |
| Level and form of studies | : | II degree, stationary |
| Type of course | : | compulsory |
| Course code | : | W04INA-SM0008G |
| Group of courses | : | Yes |

| | Lectures | Exercides | Laboratory | Project | Seminar |
|---|---|---|---|---|---|
| Number of classes held in schools (ZZU) | 30 | 30 | 15 | | |
| The total number of hours of student workload (CNPS) | 45 | 60 | 45 | | |
| Assesment | exam | | | | |
| For a group of courses final course mark | X | | | | |
| Number of ECTS credits | 2 | 2 | 1 | | |
| including the number of points corresponding to the classes of practical (P) | | 2 | 1 | | |
| including the number of points corresponding occupations requiring direct contact (BK) | 2 | 2 | 1 | | |

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

Standard knowledge of the field: abstract algebra, algorithms and data structures, probability, computational complexity.

COURSE OBJECTIVES

**C1** presentation of advanced cryptographic techniques used in practice

**C2** understanding advanced mechanisms of modern cryptography

**C3** getting skills in implementing cryptographic techniques

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

**W1** knows most important techniques of modern cryptography

**W2** knows tools and mathematical structures used to construct cryptographic schemes

**W3** knows the most important problems and challenges of modern cryptography and cryptoanalysis

The student skills:

**U1** is able to build cryptographic tools to ensure security

**U2** is able to build and use cryptographic tools

**U3** is able to use abstract mathematical structures used to implement cryptographic schemes

**U4** is able to evaluate and select apropriate cryptographic schemes according to a set of given requirements

The student's social competence:

**K1** understands need of use of cryptographic techniques

**K2** is able to apply cryptographic techniques to the end-user needs and behaviours

**K3** is able to adjust a cryptographic solution to the law and economical requirements

**K4** is able to estimate and predict possible treads and attack surfaces

COURSE CONTENT

| Type of classes - lectures | | |
|---|---|---|
| Wy1 | Cryptography - history and overview | 2h |
| Wy2 | One time pad. Stream ciphers | 2h |
| Wy3 | Block ciphers | 2h |
| Wy4 | PRPs and PRFs as block cipher abstractions | 2h |
| Wy5 | Message integrity. Collision resistant hash functions. | 2h |
| Wy6 | Security against active attacks - authenticate encryption | 2h |
| Wy7 | Discrete-log assumptions | 2h |
| Wy8 | Cryptography using arithmetic modulo composites | 2h |
| Wy9 | Digital signatures | 2h |
| Wy10 | Secure Multi Party Computation. Obliovious transfer | 2h |
| Wy11 | Zero knowledge proofs | 2h |
| Wy12 | Bit commitments, verifiable secret sharing | 2h |
| Wy13 | Quantum cryptography | 2h |
| Wy14 | Post Quantum Cryptography | 4h |
| | Sum of hours | 30h |

| Type of classes - exercises | | |
|---|---|---|
| Ćw1 | Perfect secrecy. Ciphertext-only attacks | 2h |
| Ćw2 | Attacks on block ciphers | 2h |
| Ćw3 | Attacks on stream ciphers. Properties of pseudorandom generators | 2h |
| Ćw4 | Hash functions, message authentication codes. Properties of pseudorandom functions. | 2h |
| Ćw5 | Attacks on RSA. Integer factorization. | 2h |
| Ćw6 | Key agreement. ElGamal. Discreete log problem | 2h |
| Ćw7 | CPA and CCA | 2h |
| Ćw8 | Timing attacks on RSA implementation | 2h |
| Ćw9 | Oblivious transfer | 2h |
| Ćw10 | Interactive proofs. Zero-knowledge proofs | 4h |
| Ćw11 | Homomorphic encryption | 2h |
| Ćw12 | Secure multiparty computations | 2h |
| Ćw13 | Quantum cryptography | 2h |
| Ćw14 | Post-Quantum cryptography | 2h |
| | Sum of hours | 30h |

| Type of classes - laboratory | | |
|---|---|---|
| Lab1 | How to implement a cryptographic provider | 2h |
| Lab2 | Securing data | 2h |
| Lab3 | Hash functions | 2h |
| Lab4 | Primality testing | 2h |
| Lab5 | Discrete logarithm | 2h |
| Lab6 | Factoring | 2h |
| Lab7 | Implementation of a chosen digital signature scheme | 3h |
| | Sum of hours | 15h |

Applied learning tools

1. Traditional lecture
2. Solving tasks and problems
3. Solving programming tasks
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-K4 | |
| F2 | U1-U4, K1-K4 | |
| F3 | U1-U4, K1-K4 | |
| P=%*F1+%*F2+%*F3 | | |

| BASIC AND ADDITIONAL READING |
| --- |
| 1. Introduction to modern cryptography. Jonathan Katz, Yehuda Lindell<br>2. Handbook of Applied Cryptography. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, ISBN:0-8493-8523-7<br>3. Cryptography. Theory and practice - Douglas R. Stinson<br>4. The Foundations of Cryptography (https://www.wisdom.weizmann.ac.il/ oded/foc-drafts.html) - Oded Goldreich<br>5. Lecture Notes on Cryptography (https://cseweb.ucsd.edu/ mihir/papers/gb.pdf) - S. Goldwasser, M. Bellare |
| SUPERVISOR OF COURSE |
| dr Filip Zagórski |

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT

Kryptografia

WITH LEARNING OUTCOMES IN THE FIELD OF ALGORITHMIC COMPUTER SCIENCE

| Subject learning effect | Relating the subject effect to the learning outcomes defined for the field of study | Objectives of the course** | Program content** | Teaching tool number** |
|---|---|---|---|---|
| W1 | K2_W01 K2_W02 K2_W03 K2_W04 | C1 | Wy1-Wy14 | 1 4 5 |
| W2 | K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W07 K2_W08 | C1 | Wy1-Wy14 | 1 4 5 |
| W3 | K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W08 | C1 | Wy1-Wy14 | 1 4 5 |
| U1 | K2_U05 K2_U06 K2_U10 K2_U12 | C2 C3 | Ćw1-Ćw14 Lab1-Lab7 | 2 3 4 5 |
| U2 | K2_U01 K2_U03 K2_U04 K2_U05 K2_U06 K2_U12 K2_U13 | C2 C3 | Ćw1-Ćw14 Lab1-Lab7 | 2 3 4 5 |
| U3 | K2_U03 K2_U06 | C2 C3 | Ćw1-Ćw14 Lab1-Lab7 | 2 3 4 5 |
| U4 | K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U09 K2_U10 K2_U11 K2_U12 | C2 C3 | Ćw1-Ćw14 Lab1-Lab7 | 2 3 4 5 |
| K1 | K2_K02 K2_K03 K2_K05 K2_K07 K2_K09 K2_K10 | C1 C2 C3 | Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7 | 1 2 3 4 5 |
| K2 | K2_K02 K2_K03 K2_K05 K2_K07 K2_K08 K2_K09 K2_K10 | C1 C2 C3 | Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7 | 1 2 3 4 5 |
| K3 | K2_K01 K2_K05 K2_K09 K2_K12 | C1 C2 C3 | Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7 | 1 2 3 4 5 |
| K4 | K2_K01 K2_K02 K2_K03 K2_K05 K2_K07 K2_K09 K2_K10 | C1 C2 C3 | Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7 | 1 2 3 4 5 |