# Fundamentals of Cryptography - course description

## General information

| | |
|---|---|
| Course name | Fundamentals of Cryptography |
| Course ID | 11.0-WK-IiEP-PK-L-S14_pNadGenT19B7 |
| Faculty | Faculty of Mathematics, Computer Science and Econometrics |
| Field of study | Informatics and Econometrics |
| Education profile | academic |
| Level of studies | First-cycle studies leading to Bachelor's degree |
| Beginning semester | winter term 2018/2019 |

## Course information

| | |
|---|---|
| Semester | 5 |
| ECTS credits to win | 6 |
| Course type | optional |
| Teaching language | polish |
| Author of syllabus | • dr Barbara Mędryk |

## Classes forms

| The class form | Hours per semester (full-time) | Hours per week (full-time) | Hours per semester (part-time) | Hours per week (part-time) | Form of assignment |
|---|---|---|---|---|---|
| Laboratory | 30 | 2 | - | - | Credit with grade |
| Lecture | 30 | 2 | - | - | Exam |

## Aim of the course

Celem przedmiotu jest zapoznanie studenta z podstawowymi systemami kryptograficznymi i ich stosowaniem w życiu codziennym.

## Prerequisites

Podstawowe wiadomości z algebry i teorii liczb.

## Scope

**Wykład:**

1. Proste systemy kryptograficzne
2. Macierze szyfrujące
3. Idea systemów z kluczem publicznym
4. System RSA
5. Logarytm dyskretny
6. Pakowanie plecaka
7. Systemy kryptograficzne, w których używa się krzywych eliptycznych

**Laboratorium:**

1. Używanie programów komputerowych do szyfrowania i deszyfrowania informacji.
2. Tworzenie prostych programów wykorzystujących algorytmy pewnych systemów kryptograficznych

## Teaching methods

Tradycyjny wykład; Dyskusja; Ćwiczenia laboratoryjne w pracowni komputerowej.

## Learning outcomes and methods of theirs verification

| Outcome description | Outcome symbols | Methods of verification | The class form |
|---|---|---|---|
| Student potrafi znaleźć zastosowania systemów kryptograficznych w różnych dziedzinach życia codziennego. Umie kodować informacje za pomocą systemów i rozkodować zaszyfrowane . Potrafi szyfrować informacje z wykorzystaniem programów komputerowych. Umie napisać prosty program, wykorzystując gotowy algorytm pewnego systemu kryptograficznego. | • K_U12<br>• K_K03<br>• K_K05 | • sprawdzian, bieżąca kontrola na zajęciach | • Laboratory |
| Student zna proste systemy kryptograficzne i potrafi przedstawić je na konkretnych przykładach | • K_W01 | • egzamin pisemny sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie wykładów | • Lecture |

| Outcome description | Outcome symbols | Methods of verification | The class form |
| --- | --- | --- | --- |
| Student zna proste systemy z kluczem publicznym: system RSA, problem pakowania plecaka. | • K_W01 | • egzamin pisemny<br>sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie wykładów | • Lecture |

## Assignment conditions

Udział w zajęciach jest obowiązkowy.

Na ocenę z przedmiotu składa się ocena z laboratorium (50%) oraz ocena z egzaminu (60%). Warunkiem zaliczenia przedmiotu jest pozytywna ocena z laboratorium i egzaminu.

## Recommended reading


1. W. Sierpiński, *Elementary Theory of Numbers,* PWN, Warszawa 1987.
2. N. Koblitz, *Wykład z teorii i kryptografii,* WNT, Warszawa 1995.
3. L.E. Dickson, *Introduction to the thery of numbers,* New York 1957.


## Further reading


1. W.Narkiewicz, *Teoria liczb,* PWN, Warszawa 1977.


## Notes

Modified by dr Robert Dylewski, prof. UZ (last modification: 04-05-2018 19:24)