

Cryptography, what is it? - course description

General information	
Course name	Cryptography, what is it?
Course ID	11.1-WK-UZP-KRYP-W-S14_gen4TKNR
Faculty	Inter-faculty courses offer
Field of study	Inter-faculty courses offer
Education profile	-
Level of studies	
Semester	summer term 2018/2019
Head faculty	Faculty of Mathematics, Computer Science and Econometrics

Course information	
ECTS credits to win	2
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
Lecture	30	2	18	1,2	Credit

Aim of the course

Zapoznanie studenta z podstawowymi pojęciami teorii liczb i ich zastosowaniami w kryptografii.

Prerequisites

Brak wymagań

Scope

I. Zagadnienia elementarnej teorii liczb

1. Oszacowanie czasu wykonywania działań arytmetycznych. (2 godz. S/2 godz. N)
2. Podzielność i algorytm Euklidesa. (2 godz. S/1 godz. N)
3. Kongruencje. (2 godz. S/1 godz. N)
4. Zastosowania do problemu rozkładu na czynniki. (2 godz. S/1 godz. N)

II. Liczby pierwsze i ich własności

1. Zbiór liczb pierwszych. (2 godz. S/1 godz. N)
2. Różne typy liczb pierwszych. (2 godz. S/1 godz. N)

III. Kryptografia

1. Proste systemy kryptograficzne. (3 godz. S/2 godz. N)
2. Macierze szyfrujące. (3 godz. S/2 godz. N)

IV. Publiczne klucze

1. Idea systemów z kluczem publicznym. (3 godz. S/2 godz. N)
2. System RSA. (4 godz. S/2 godz. N)
3. Logarytm dyskretny. (2 godz. S/1 godz. N)
4. Pakowanie plecaka. (3 godz. S/2 godz. N)

Teaching methods

Wykład tradycyjny połączony z dyskusją na temat omawianych problemów

Learning outcomes and methods of theirs verification

Outcome description	Outcome symbols	Methods of verification	The class form
Student zna podstawowe definicje i twierdzenia z teorii liczb		an ongoing monitoring during classes	Lecture

Outcome description	Outcome symbols	Methods of verification	The class form
Student zna proste systemy kryptograficzne i potrafi je zastosować na konkretnych przykładach.		a research paper	Lecture
Student zna systemy z kluczem publicznym: system RSA, problem pakowania plecaka.		a preparation of a project	Lecture

Assignment conditions

Zaliczenie przedmiotu na podstawie obecności na zajęciach, a także na podstawie referatów i projektów przygotowanych przez studentów.

Recommended reading

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

Further reading

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

Notes

Modified by mgr Renata Kubiak (last modification: 26-04-2018 08:52)

Generated automatically from SylabUZ computer system