Podstawy kryptografii - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Podstawy kryptografii
Kod przedmiotu	11.0-WK-IiEP-PK-L-S14_pNadGenT19B7
Wydział	Wydział Matematyki, Informatyki i Ekonometrii
Kierunek	Computer science and econometrics
Profil	ogólnoakademicki
Rodzaj studiów	pierwszego stopnia z tyt. licencjata
Semestr rozpoczęcia	semestr zimowy 2019/2020

Informacje o przedmiocie

Semestr	3
Liczba punktów ECTS do zdobycia	6
Typ przedmiotu	obieralny
Język nauczania	polski
Sylabus opracował	

Formy zajęć

Forma zajęć	Liczba godzin w semestrze (stacjonarne)	Liczba godzin w tygodniu (stacjonarne)	Liczba godzin w semestrze (niestacjonarne)	Liczba godzin w tygodniu (niestacjonarne)	Forma zaliczenia
Laboratorium	30	2	-	-	Zaliczenie na ocenę
Wykład	30	2	-	-	Egzamin

Cel przedmiotu

The aim of the course is to familiarize the student with the basic cryptographic systems and their application in everyday life.

Wymagania wstępne

Basic knowledge of algebra and number theory.

Zakres tematyczny

Lecture:

1. Simple cryptographic systems.
2. Cipher matrices.
3. The idea of public key systems.
4. RSA system.
5. Discrete logarithm.
6. Packing the backpack.
7. Cryptographic systems based on elliptic curves.

Laboratory:

1. Using computer programs to encrypt and decrypt information.
2. Creating simple programs that uses algorithms of certain cryptographic systems.

Metody kształcenia

Traditional lecture; Discussion; Laboratory in the computer lab.

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Student knows simple public key systems: RSA system, the problem of packing a backpack.	• K_W01	• egzamin - ustny, opisowy, testowy i inne • obserwacja i ocena aktywności na zajęciach	• Wykład
Student knows simple cryptographic systems and is able to present them on specific examples.	• K_W05 • K_U20	• egzamin - ustny, opisowy, testowy i inne • obserwacja i ocena aktywności na zajęciach	• Wykład

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Student is able to find applications of cryptographic systems in various areas of everyday life. Student can encode an information and decode an encrypted information. Student uses computer programs to encode and decode. Student can write a simple program based on algorithm of a certain cryptographic system.	• K_W05 • K_U01 • K_U20	• bieżąca kontrola na zajęciach • sprawdzian	• Laboratorium

Warunki zaliczenia

Participation in the classes is obligatory.

The grade for the subject consists of the laboratory grade (50%) and the exam grade (50%). In order to pass a student has to have a positive exam grade and the laboratory.

Literatura podstawowa

1. W. Sierpiński, *Elementary Theory of Numbers,* PWN, Warszawa 1987.
2. N. Koblitz, *A Course in Number Theory and Cryptography*, Graduate Texts in Mathematics, 1994
3. L.E. Dickson, *Introduction to the thery of numbers,* New York 1957.

Literatura uzupełniająca

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

Uwagi

Zmodyfikowane przez dr Alina Szelecka (ostatnia modyfikacja: 21-11-2020 06:10)