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	Informatyka i ekonometria
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	• dr Barbara Mędryk

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

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

Wymagania wstępne

Podstawowe wiadomości z algebry i teorii liczb.

Zakres tematyczny

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

Metody kształcenia

Tradycyjny wykład; Dyskusja; Ćwiczenia laboratoryjne w pracowni komputerowej.

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
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.		• sprawdzian, bieżąca kontrola na zajęciach	• Laboratorium

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Student zna proste systemy kryptograficzne i potrafi przedstawić je na konkretnych przykładach		• egzamin pisemny sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie wykładów	• Wykład
Student zna proste systemy z kluczem publicznym: system RSA, problem pakowania plecaka.		• egzamin pisemny sprawdzanie stopnia przygotowania studentów oraz ich aktywności w trakcie wykładów	• Wykład

Warunki zaliczenia

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.

Literatura podstawowa

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.

Literatura uzupełniająca

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

Uwagi

Zmodyfikowane przez dr Robert Dylewski, prof. UZ (ostatnia modyfikacja: 12-09-2019 08:29)