

Kryptografia, co to takiego? - przedmiot ogólnouczelniany - opis przedmiotu

Informacje ogólne	
Nazwa przedmiotu	Kryptografia, co to takiego? - przedmiot ogólnouczelniany
Kod przedmiotu	11.1-WK-UZP-KRYP-W-S14_gen4TKNR
Wydział	Oferta ogólnouczelniana
Kierunek	Oferta ogólnouczelniana
Profil	-
Rodzaj studiów	
Semestr	semestr zimowy 2019/2020
Jednostka obsługująca przedmiot	Wydział Matematyki, Informatyki i Ekonometrii

Informacje o przedmiocie	
Liczba punktów ECTS do zdobycia	2
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
Wykład	30	2	0	0	Zaliczenie

Cel przedmiotu

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

Wymagania wstępne

Brak wymagań

Zakres tematyczny

I. Zagadnienia elementarnej teorii liczb

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

II. Liczby pierwsze i ich własności

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

III. Kryptografia

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

IV. Publiczne klucze

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

Metody kształcenia

Wykład tradycyjny połączony z dyskusją na temat omawianych problemów

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
-------------	-----------------	--------------------	-------------

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Student zna proste systemy kryptograficzne i potrafi je zastosować na konkretnych przykładach.		• referat	• Wykład
Student zna systemy z kluczem publicznym: system RSA, problem pakowania plecaka.		• przygotowanie projektu	• Wykład
Student zna podstawowe definicje i twierdzenia z teorii liczb		• bieżąca kontrola na zajęciach	• Wykład

Warunki zaliczenia

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

Literatura podstawowa

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.

Literatura uzupełniająca

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

Uwagi

Zmodyfikowane przez mgr Renata Kubiak (ostatnia modyfikacja: 29-04-2019 10:38)

Wygenerowano automatycznie z systemu SylabUZ