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 2016/2017
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	18	1,2	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

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)

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 podstawowe definicje i twierdzenia z teorii liczb Student zna proste systemy kryptograficzne i potrafi je zastosować na konkretnych przykładach. Student zna systemy z kluczem publicznym: system RSA, problem pakowania plecaka.		• przygotowanie referatu	• 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: 26-07-2016 10:10)