**Nazwa przedmiotu:**

Podstawy kryptografii

**Koordynator przedmiotu:**

dr Rządkowski Grzegorz

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia I stopnia

**Program:**

Zarządzanie

**Grupa przedmiotów:**

Specjalność: Zarządzanie w gospodarce cyfrowej

**Kod przedmiotu:**

-

**Semestr nominalny:**

4 / rok ak. 2018/2019

**Liczba punktów ECTS:**

2

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

2 ECTS:
10h wykład + 5h konsultacje+ 10h laboratorium + 15h przygotowanie projektu zespołowego + 10h studiowanie literatury + 10h wykonanie prac domowych = 60h

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

0,9 ECTS:
10h laboratorium + 10h wykład + 5h konsultacje = 25h

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

1,4 ECTS:
10h laboratorium + 15h przygotowanie projektu zespołowego + 10h studiowanie literatury + 10h wykonanie prac domowych = 45h

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład:  | 10h |
| Ćwiczenia:  | 0h |
| Laboratorium:  | 10h |
| Projekt:  | 0h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

Umiejętności matematyczne, wiedza i umiejętności z zakresu analizy matematycznej i algebry

**Limit liczby studentów:**

- od 25 osób do limitu miejsc w sali audytoryjnej (wykład) - od 25 osób do limitu miejsc w sali laboratoryjnej (laboratorium)

**Cel przedmiotu:**

Celem zajęć jest omówienie zagadnień związanych z podstawami teorii liczb i jej zastosowaniem w kryptografii.

**Treści kształcenia:**

A. Wykład:
1. Oszacowanie czasu wykonywania działań arytmetycznych.
2. Podzielność i algorytm Euklidesa.
3. Kongruencje.
4. Zastosowania do problemu rozkładu na czynniki.
5. Proste systemy kryptograficzne.
6. Macierze szyfrujące.
7. Idea systemów z kluczem publicznym.
8. System RSA.
B. Laboratorium (rozwiązywanie zadań):
1. Oszacowanie czasu wykonywania działań arytmetycznych.
2. Podzielność i algorytm Euklidesa.
3. Kongruencje.
4. Zastosowania do problemu rozkładu na czynniki.
5. Proste systemy kryptograficzne.
6. Macierze szyfrujące.
7. Idea systemów z kluczem publicznym.
8. System RSA.

**Metody oceny:**

A. Wykład:
1. Ocena formatywna: aktywność studentów
2. Ocena sumatywna : ocena rezultatów projektu
B. Laboratorium:
1. Ocena formatywna: ocena rezultatów pracy zespołowej wykonywanej przez studentów podczas przygotowania projektu
2. Ocena sumatywna: ocena rezultatów pracy zespołowej podczas prezentacji projektu
E. Końcowa ocena z przedmiotu:, 40% projekt, 60% praca w laboratorium

**Egzamin:**

nie

**Literatura:**

Obowiązkowa:
1. Koblitz, N.,1995. Wykład z teorii liczb i kryptografii. Warszawa: WNT.
2. Sierpiński, W., 1987. Elementary Theory of Numbers. Warszawa: PWN.
Uzupełniająca:
1. Narkiewicz, W., 1997. Teoria liczb, Warszawa: PWN.
2. Dickson, L.E., 1957. Introduction to the theory of numbers, New York.

**Witryna www przedmiotu:**

www.olaf.wz.pw.edu.pl

**Uwagi:**

-

## Efekty przedmiotowe

### Profil ogólnoakademicki - wiedza

**Efekt Z1\_W03:**

Student posiada wiedzę na temat podstawowych twierdzeń z teorii liczb i zna proste systemy kryptograficzne. Posiada znajomość systemów z kluczem publicznym: system RSA

Weryfikacja:

Rozwiązywania zadań podczas ćwiczeń, prezentacja projektu

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Efekt Z1\_U08:**

Student potrafi zastosować proste systemy kryptograficzne do konkretnych przykładów

Weryfikacja:

Przygotowanie i ocena projektu

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt Z1\_K01:**

Student posiada zdolność porządkowania wykonywanych zadań według stopnia ich ważności z punktu widzenia realizacji celu

Weryfikacja:

Przygotowanie i ocena projektu

**Powiązane efekty kierunkowe:**

**Powiązane efekty obszarowe:**