**Nazwa przedmiotu:**

Podstawy kryptografii

**Koordynator przedmiotu:**

dr hab. Grzegorz Rządkowski, prof. PW

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Zarządzanie Bezpieczeństwem Infrastruktury Krytycznej

**Grupa przedmiotów:**

Kierunkowe

**Kod przedmiotu:**

-

**Semestr nominalny:**

1 / rok ak. 2022/2023

**Liczba punktów ECTS:**

3

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

3 ECTS
18h wykład + 18h ćwiczenia + 12h przygotowanie do ćwiczeń + 5h analiza literatury + 15h przygotowanie do zaliczenia ćwiczeń i wykładu + 7h konsultacje= 75h

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

1,72 ECTS
18h wykład + 18h ćwiczenia + 7h konsultacje = 43h

**Język prowadzenia zajęć:**

polski

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

2,28 ECTS
18h ćwiczenia + 12h przygotowanie do ćwiczeń + 5h analiza literatury + 15h przygotowanie do zaliczenia ćwiczeń i wykładu + 7h konsultacje = 57h

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

|  |  |
| --- | --- |
| Wykład: | 15h |
| Ćwiczenia: | 15h |
| Laboratorium: | 0h |
| Projekt: | 0h |
| Lekcje komputerowe: | 0h |

**Wymagania wstępne:**

Zaliczenie przedmiotu analiza matematyczna

**Limit liczby studentów:**

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

**Cel przedmiotu:**

Celem przedmiotu jest przedstawienie teoretycznych podstaw współczesnej kryptografii oraz głównych problemów dotyczących zagadnień kryptograficznych wraz z algorytmami stosowanymi w rozwiązaniach

**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.
9. Logarytm dyskretny.
10. Pakowanie plecaka.
B. Ćwiczenia (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.
9. Logarytm dyskretny.
10. Pakowanie plecaka.

**Metody oceny:**

A. Wykład:
1. Ocena formatywna: ocena poprawności wnioskowania dotyczącego zadawanych w trakcie wykładu pytań problemowych, częściowo interaktywna forma prowadzenia wykładu.
2. Ocena sumatywna : przeprowadzenie egzaminu, ocena z egzaminu w zakresie 2-5;
B. Ćwiczenia:
1. Ocena formatywna: ocena poprawności ćwiczeń wykonanych przez studentów podczas kolejnych zajęć, ocena zadań domowych
2. Ocena sumatywna: ocena ćwiczeń wykonywanych w trakcie zajęć w skali punktowej i zadań domowych , kolokwium oceniane w skali punktowej.
E. Końcowa ocena z przedmiotu: Przedmiot uznaje się za zaliczony jeśli zarówno ocena z kolokwium końcowego z wykładu jak i z ocena z części ćwiczeniowej >=3.
Ocena z przedmiotu obliczana jest zgodnie z formułą: 0,5 \* ocena z ćwiczeń + 0,5\* ocena z egzaminu.

**Egzamin:**

tak

**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:**

-

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka B2\_W04:**

Absolwent zna i rozumie w pogłębionym stopniu metody kryptografii wspomagające wypracowanie, ocenę i podejmowanie decyzji w procesach zarządzania organizacjami

Weryfikacja:

Egzamin, ćwiczenia (rozwiązywanie zadań, prezentacja rozwiązań zadań domowych)

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Charakterystyka B2\_U03:**

Absolwent potrafi przy identyfikacji i formułowaniu specyfikacji zadań dotyczących kryptografii oraz ich rozwiązywaniu dobierać i wykorzystywać właściwe metody i narzędzia wspomagające

Weryfikacja:

Egzamin, zaliczenie ćwiczeń

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka B2\_K04:**

Absolwent jest gotów do myślenia i działania w sposób przedsiębiorczy i ekonomiczny

Weryfikacja:

Zaliczenia pisemne, ćwiczenia (rozwiązywanie zadań, zespołowe studia przypadków)

**Powiązane charakterystyki kierunkowe:**

**Powiązane charakterystyki obszarowe:**