**Nazwa przedmiotu:**

Warsztaty matematycznych metod cyberbezpieczeństwa

**Koordynator przedmiotu:**

Dr hab. Agata Pilitowska, Dr Barbara Roszkowska-Lech, Dr hab. Konstanty Junosza-Szaniawski

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Matematyka

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

.

**Semestr nominalny:**

2 / rok ak. 2022/2023

**Liczba punktów ECTS:**

3

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

1. godziny kontaktowe – 50 h; w tym
a) obecność na laboratoriach – 30 h
b) obecność na projekcie – 15 h
c) konsultacje – 5 h
2. praca własna studenta – 45 h; w tym
a) przygotowanie do laboratoriów i projektu – 45 h
Razem 100 h, co odpowiada 3 pkt. ECTS

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

a) obecność na laboratoriach – 30 h
b) obecność na projekcie – 15 h
c) konsultacje – 5 h
Razem 50 h, co odpowiada 2 pkt. ECTS

**Język prowadzenia zajęć:**

polski

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

.

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

|  |  |
| --- | --- |
| Wykład: | 0h |
| Ćwiczenia: | 0h |
| Laboratorium: | 30h |
| Projekt: | 15h |
| Lekcje komputerowe: | 0h |

**Wymagania wstępne:**

Przedmioty poprzedzające:
1. Wprowadzenie do współczesnej kryptologii
2. Algorytmiczna teoria liczb
3. Kody korekcyjne i transmisja danych
4. Algebra w kryptografii
Wymagania wstępne:
1. Znajomość podstawowych algorytmów teorii liczb.
2. Znajomość podstawowych protokołów kryptograficznych
3. Znajomość wybranych metod kodowania i dekodowania liniowego nad dowolnym ciałem skończonym.

**Limit liczby studentów:**

Bez limitu

**Cel przedmiotu:**

Zdobycie umiejętności zastosowania poznanych algorytmów kryptograficznych i teorio-liczbowych oraz metod kodowania i dekodowania liniowego w praktyce.

**Treści kształcenia:**

1. Poznanie środowiska Sage.
2. Analiza danego zagadnienia kryptograficznego, kodowego lub teorio-liczbowego oraz dobór algorytmów.
3. Przygotowanie specyfikacji algorytmu.
4. Stworzenie aplikacji.
5. Testowanie aplikacji.
6. Przygotowanie dokumentacji stworzonej aplikacji.
7. Prezentacja otrzymanych wyników oraz dyskusja.

**Metody oceny:**

Warunkiem zaliczenia przedmiotu jest przygotowanie poprawnie działającej aplikacji wykorzystującej poznane algorytmy oraz sporządzenie jej dokumentacji.
Ostateczna ewaluacja zostanie dokonana na podstawie indywidualnej rozmowy i oceny przygotowanego materiału. Aplikacja wraz dokumentacją oceniana jest w
skali 0-20pkt:
od 11pkt – 3,0
od 13pkt – 3,5
od 15pkt – 4,0
od 17pkt – 4,5
od 19pkt – 5,0

**Egzamin:**

nie

**Literatura:**

1. A. Chrzęszczyk, Algorytmy teorii liczb i kryptografii w przykładach, Wydawnictwo BTC, Legionowo, 2010.
2 N.J.A.Sloane, F.J. MacWilliams, The Theory of Error-Correctin Codes, North-Holland, Amsterdam, 1977.
3. D.R. Stinson, Kryptografia w teorii i w praktyce, WNT, 1995.
4. S.Y.Yan, Teoria liczb w informatyce, PWN, 2006.

**Witryna www przedmiotu:**

brak

**Uwagi:**

.

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka WKK\_W01:**

Zna wybrane algorytmy kodowania i dekodowania kodów cyklicznych, oraz podstawowe algorytmy kryptograficzne.

Weryfikacja:

Raport pisemny

**Powiązane charakterystyki kierunkowe:** M2\_W01, M2\_W02, M2\_W03, M2MCB\_W03, M2MCB\_W04, M2\_W04

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WKK\_W02:**

Zna podstawowe twierdzenia, metody badawcze oraz algorytmy związane z problemami obliczeniowymi wykorzystywanymi w kryptografii.

Weryfikacja:

Raport pisemny

**Powiązane charakterystyki kierunkowe:** M2\_W01, M2\_W02, M2\_W03, M2MCB\_W15, M2\_W04

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Charakterystyka WKK\_U01:**

Potrafi zaadoptować poznane algorytmy do rozwiązania konkretnego problemu dotyczącego bezbłędnej transmisji danych.

Weryfikacja:

Projekt, Prezentacja

**Powiązane charakterystyki kierunkowe:** M2\_U02, M2MCB\_U02, M2MCB\_U04, M2MCB\_U07, M2MCB\_U09, M2\_U03

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WKK\_U02:**

Potrafi zaadoptować poznane algorytmy do rozwiązania konkretnego zagadnienia kryptograficznego.

Weryfikacja:

Projekt, Prezentacja

**Powiązane charakterystyki kierunkowe:** M2MCB\_U07, M2MCB\_U09, M2\_U03, M2\_U02, M2MCB\_U04

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka WKK\_K01:**

Ma umiejętność pracy w zespole, myślenia w sposób przedsiębiorczy i rozumie społeczne aspekty stosowania zdobytej wiedzy oraz potrzebę jej rozwoju.

Weryfikacja:

Projekt

**Powiązane charakterystyki kierunkowe:** M2\_K01, M2MCB\_K01, M2MCB\_K02, M2\_K03

**Powiązane charakterystyki obszarowe:**