**Nazwa przedmiotu:**

Warsztaty: kody i kryptografia

**Koordynator przedmiotu:**

Dr hab. Agata Pilitowska, dr Barbara Roszkowska-Lech

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Matematyka

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

.

**Semestr nominalny:**

2 / rok ak. 2017/2018

**Liczba punktów ECTS:**

2

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

1. godziny kontaktowe – 65 h; w tym
a) obecność na laboratoriach – 30 h
b) obecność na projekcie – 30 h
c) konsultacje – 5 h
2. praca własna studenta – 35 h; w tym
a) przygotowanie aplikacji – 30 h
b) zapoznanie się z literaturą – 5 h
Razem 100 h, co odpowiada 4 pkt. ECTS

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

a) obecność na laboratoriach – 30 h
b) obecność na projekcie – 30 h
c) konsultacje – 5 h
Razem 65 h, co odpowiada 2 pkt. ECTS

**Język prowadzenia zajęć:**

polski

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

a) obecność na laboratoriach – 30 h
b) obecność na projekcie – 30 h
c) konsultacje – 5 h
d) przygotowanie aplikacji – 30 h
e) zapoznanie się z literaturą – 5 h
Razem 100 h, co odpowiada 4 pkt. ECTS

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

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

**Wymagania wstępne:**

Przedmioty poprzedzające:
1. Podstawy kryptografii
2. Algorytmiczna teoria liczb
3. Kody korekcyjne
Wymagania wstępne:
1. Znajomość podstawowych algorytmów teorii liczb.
2.Znajomośc podstawowych protokołów kryptograficznych
3. Znajomość wybranych metod kodowania i dekodowania liniowego nad dowolnym ciałem skończonym.

**Limit liczby studentów:**

.

**Cel przedmiotu:**

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

**Treści kształcenia:**

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

**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. Song.Y.Yan, Teoria liczb w informatyce, PWN, 2016.
2. Neal Koblitz, Wykład z teorii liczb i kryptografii, Wydawnictwo Naukowo-Techniczne, Warszawa, 1995.
3. N.J.A.Sloane, F.J. MacWilliams, The Theory of Error-Correctin Codes, North-Holland, Amsterdam, 1977.

**Witryna www przedmiotu:**

.

**Uwagi:**

.

## Efekty przedmiotowe

### Profil ogólnoakademicki - wiedza

**Efekt WKK\_W01:**

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

Weryfikacja:

Przygotowanie działającego programu wraz z dokumentacją

**Powiązane efekty kierunkowe:** M2\_W01, M2\_W02, M2MNI\_W03, M2MNI\_W04, M2\_W04

**Powiązane efekty obszarowe:** , , , ,

**Efekt WKK\_W02:**

Zna podstawowe twierdzenia, metody badawcze oraz algorytmy związane z problemami obliczeniowymi w teorii liczb.

Weryfikacja:

Przygotowanie działającego programu wraz z dokumentacją

**Powiązane efekty kierunkowe:** M2\_W01, M2\_W02, M2MNI\_W15, M2\_W04

**Powiązane efekty obszarowe:** , , ,

### Profil ogólnoakademicki - umiejętności

**Efekt WKK\_U01:**

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

Weryfikacja:

Przygotowanie działającego programu wraz z dokumentacją

**Powiązane efekty kierunkowe:** M2\_U02, M2MNI\_U02, M2MNI\_U04, M2MNI\_U09, M2\_U03

**Powiązane efekty obszarowe:** , , , ,

**Efekt WKK\_U02:**

Potrafi zaadoptować poznane algorytmy do rozwiązania konkretnego zagadnienia kryptograficznego.

Weryfikacja:

Przygotowanie działającego programu wraz z dokumentacją

**Powiązane efekty kierunkowe:** M2\_U02, M2MNI\_U02, M2MNI\_U04, M2MNI\_U09, M2\_U03

**Powiązane efekty obszarowe:** , , , ,

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt WKK\_K01:**

Ma umiejętność pracy w zespole.

Weryfikacja:

Przygotowanie działającego programu wraz z dokumentacją

**Powiązane efekty kierunkowe:** M2\_K01, M2MNI\_K01, M2\_K03

**Powiązane efekty obszarowe:** X2A\_K06, ,

**Efekt WKK\_K02:**

Rozumie przydatność nabytej wiedzy i umiejętności obliczeniowych do stawiania hipotez oraz z ich weryfikacji w możliwych zastosowaniach w kryptografii, teorii liczb i teorii kodowania informacji.

Weryfikacja:

Przygotowanie działającego programu wraz z dokumentacją

**Powiązane efekty kierunkowe:** M2MNI\_K02

**Powiązane efekty obszarowe:**