**Nazwa przedmiotu:**

Algebra w kryptografii / Przedmiot obieralny I

**Koordynator przedmiotu:**

Dr hab. Agata Pilitowska, prof. PW, Dr hab. Anna Zamojska-Dzienio, prof. PW

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Matematyka

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

.

**Semestr nominalny:**

1 / rok ak. 2023/2024

**Liczba punktów ECTS:**

4

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

1. godziny kontaktowe – 70 h; w tym
 a) obecność na wykładach – 30 h
 b) obecność na ćwiczeniach – 30 h
 c) konsultacje – 5 h
 d) egzamin – 5 h
2. praca własna studenta – 60 h; w tym
 a) przygotowanie do ćwiczeń i do kolokwiów – 40 h
 b) zapoznanie się z literaturą – 10 h
 b) przygotowanie się do egzaminu – 10 h
Razem 130 h, co odpowiada 5 pkt. ECTS

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

a) obecność na wykładach – 30 h
b) obecność na ćwiczeniach – 30 h
c) konsultacje – 5 h
c) egzamin – 5 h
Razem 70 h, co odpowiada 3 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:  | 30h |
| Ćwiczenia:  | 30h |
| Laboratorium:  | 0h |
| Projekt:  | 0h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

Przedmioty poprzedzające:
1. Elementy logiki i teorii mnogości
2. Algebra liniowa z geometrią
3. Algebra i jej zastosowania
Wymagania wstępne:
Znajomość algebry liniowej oraz podstaw teorii grup i pierścieni.

**Limit liczby studentów:**

Bez limitu

**Cel przedmiotu:**

Zdobycie wiedzy o ciałach skończonych i ich wybranych zastosowaniach.

**Treści kształcenia:**

1. Pierścienie całkowite i ich związki z ciałami.
2. Ideały w pierścieniach. Ideały główne, pierwsze, maksymalne.
3. Ciało ułamków pierścienia całkowitego.
4. Pierścienie Euklidesa.
3. Pierścienie wielomianów o współczynnikach w ciele. Wielomiany rozkładalne i nierozkładalne, pierścienie ilorazowe pierścieni wielomianów, ciało rozkładu wielomianu, ciało algebraicznie domknięte.
5. Rozszerzenia ciał, elementy algebraiczne, rozszerzenia algebraiczne. Charakterystyka ciała. Ciała proste.
6. Ciała skończone. Elementy pierwotne ciała. Podciała ciała skończonego. Reprezentacja elementów w ciałach skończonych. Obliczenia w ciałach skończonych.
7. Wielomiany minimalne, pierwiastki z jedności w ciałach skończonych.
8. Endomorfizm Frobeniousa. Grupa automorfizmów ciała skończonego.
9. Zastosowania ciał skończonych w teorii kodów korekcyjnych, kryptografii i przy projektowaniu eksperymentów.

**Metody oceny:**

Zaliczenie przedmiotu odbywa się na podstawie wyników z ćwiczeń oraz egzaminu. W semestrze odbywają się dwa kolokwia (maksymalnie do 15 pkt. z każdego kolokwium). Z aktywności na zajęciach można maksymalnie uzyskać do 10 pkt. Egzamin, za maksymalnie 60 punktów, składa się z części teoretycznej oraz zadaniowej. Uzyskanie w sumie 51 punktów oznacza zaliczenie przedmiotu.

**Egzamin:**

tak

**Literatura:**

1. A. Białynicki-Birula, Zarys Algebry, PWN, Warszawa, 2014
2. W. J. Gilbert, W. K. Nicholson, Algebra Współczesna z Zastosowaniami, WNT, Warszawa, 2008
3. N. Gubareni, Algebra współczesna i jej zastosowania, Wydawnictwo Politechniki Częstochowskiej, 2018
4. R. Lidl, H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, 2012
5. W. Lipski, W. Marek, Analiza kombinatoryczna, PWN, Warszawa, 1986
6. J. Rutkowski, Algebra abstrakcyjna w zadaniach, PWN, 2000

**Witryna www przedmiotu:**

https://pages.mini.pw.edu.pl/~pilitowskaa/

**Uwagi:**

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka AK\_W01:**

Zna podstawowe własności i metody konstrukcji ciał skończonych i ich rozszerzeń.

Weryfikacja:

Egzamin pisemny, kolokwia pisemne, aktywność podczas zajęć

**Powiązane charakterystyki kierunkowe:** M2MCB\_W01

**Powiązane charakterystyki obszarowe:**

**Charakterystyka AK\_W02:**

Ma wiedzę o zastosowaniach ciał skończonych w obszarze bezpieczeństwa cyfrowego.

Weryfikacja:

Kolokwia pisemne, aktywność podczas zajęć

**Powiązane charakterystyki kierunkowe:** M2\_W01, M2MCB\_W01

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Charakterystyka AK\_U01:**

Potrafi skonstruować ciała skończone i wykonywać w nich obliczenia.

Weryfikacja:

Egzamin pisemny, kolokwia pisemne, aktywność podczas zajęć

**Powiązane charakterystyki kierunkowe:** M2MCB\_U02

**Powiązane charakterystyki obszarowe:**

**Charakterystyka AK\_U02:**

Potrafi zastosować ciała skończone do opisu wybranych zagadnień kryptograficznych.

Weryfikacja:

Egzamin pisemny, kolokwia pisemne, aktywność podczas zajęć

**Powiązane charakterystyki kierunkowe:** M2MCB\_U03, M2MCB\_U04

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka AK\_K01:**

Rozumie potrzebę wzbogacania wiedzy przez samokształcenie.

Weryfikacja:

samoocena

**Powiązane charakterystyki kierunkowe:** M2MCB\_K02

**Powiązane charakterystyki obszarowe:**