**Nazwa przedmiotu:**

Nieprzemienne struktury algebraiczne i ich zastosowania w kryptografi

**Koordynator przedmiotu:**

Dr hab. Michał Ziembowski, prof. uczelni

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Matematyka

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

.

**Semestr nominalny:**

1 / rok ak. 2022/2023

**Liczba punktów ECTS:**

5

**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 – 55 h; w tym
a) przygotowanie do ćwiczeń i do kolokwium – 50 h
b) zapoznanie się z literaturą – 5 h
Razem 135 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
d) 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:**

Algebra liniowa z geometrią 1 i 2, Algebra i jej zastosowania,

**Limit liczby studentów:**

.

**Cel przedmiotu:**

Zapoznanie studentów z wybranymi nieprzemiennymi strukturami algebraicznymi, takimi jak algebry Hopfa, algebry Liego, grupy kwantowe

**Treści kształcenia:**

Struktura algebry macierzy nad pierścieniem przemiennym. Konstrukcje pierścienie nieprzemiennych i przemiennych, w tym pierścienie grupowe, pierścienie z gradacją. Elementy teorii reprezentacji grup skończonych. Kraty i ich zastosowania w kryptografii. Wybrane schematy kryptograficzne.

**Metody oceny:**

Regulamin zaliczenia przedmiotu

**Egzamin:**

nie

**Literatura:**

1. Introduction to Noncommutative Algebra, Matej Bresar
2. Reprezentacje i charaktery grup, G. James, M. Liebeck.
3. Non-commutative Cryptography and Complexity of Group-theoretic Problems, Alexei Myasnikov Vladimir Shpilrain Alexander Ushakov
4. An Introduction to Mathematical Crypthography, J. Hoffstein, J. Pipher, and Joseph Silverman, Springer-Verlag, 2008.

**Witryna www przedmiotu:**

.

**Uwagi:**

.

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka NSA\_W01:**

Zna podstawowe fakty dotyczące struktury algebr macierzy nad pierścieniem przemiennym

Weryfikacja:

Kolokwium, egzamin

**Powiązane charakterystyki kierunkowe:** M2\_W01

**Powiązane charakterystyki obszarowe:**

**Charakterystyka NSA\_W02:**

Zna obszary kryptografii w których narzędziami są struktury algebraiczne. Zna związki teorii krat z zagadnieniami dotyczącymi kryptografii postkwantowej.

Weryfikacja:

Kolokwium, egzamin

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

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Charakterystyka NSA\_U01:**

Umie posługiwać się językiem algebraicznym w odniesieniu do zagadnień kryptograficznych

Weryfikacja:

Kolokwium, egzamin

**Powiązane charakterystyki kierunkowe:** M2\_U01, M2MCB\_U02

**Powiązane charakterystyki obszarowe:**

**Charakterystyka NSA\_U02:**

Potrafi dostrzec sposób wykorzystania takich struktur algebraicznych jak grupy skończone, macierze czy kraty, w zagadneniach kryptograficznych.

Weryfikacja:

Kolokwium, egzamin

**Powiązane charakterystyki kierunkowe:** M2MCB\_U03

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka NSA\_K01:**

Rozumie potrzebę uczenia się przez całe życie

Weryfikacja:

Kolokwium, egzamin

**Powiązane charakterystyki kierunkowe:** M2MCB\_K02

**Powiązane charakterystyki obszarowe:**