**Nazwa przedmiotu:**

Algebraiczne podstawy kryptografii

**Koordynator przedmiotu:**

Dr Barbara Roszkowska-Lech

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Matematyka

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

**Semestr nominalny:**

2 / rok ak. 2011/2012

**Liczba punktów ECTS:**

5

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

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

**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:  | 15h |
| Laboratorium:  | 0h |
| Projekt:  | 0h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

Wymagania wstępne:
- znajomość podstawowych faktów z teorii liczb, grup, pierścieni , ciał i przestrzeni wektorowych.
- umiejętność stosowania metod algebry liniowej i ogólnej

Przedmioty poprzedzające:
- Algebra liniowa z geometrią
- Algebra i jej zastosowania

**Limit liczby studentów:**

**Cel przedmiotu:**

Umiejętność stosowania metod algebry w zagadnieniach kryptograficznych.

**Treści kształcenia:**

Program wykładu:
Wykład będzie wstępem do kryptografii ze szczególnym uwzględnieniem metod algebraicznych. Program wykładu obejmować będzie m.in. następujące zagadnienia z teorii liczb: podzielność i algorytm Euklidesa, kongruencje, liczby pierwsze (testy pierwszości) i rozkład na czynniki, reszty kwadratowe i logarytmy dyskretne. Przypomniane też zostaną podstawowe wiadomości z teorii ciał skończonych i pierścieni. Ponadto omówione zostaną proste systemy kryptograficzne, macierze szyfrujące oraz systemy z kluczem publicznym (m. in. RSA, system ElGamala); poufny przekaz informacji, uwierzytelnienie i dzielenie sekretów. Przedstawione zostaną też przykłady kryptosystemów opartych na krzywych eliptycznych.

Program ćwiczeń:
praktyczne rozwiazywanie zadań zwiazanych z tematami poruszanymi na wykładzie.

**Metody oceny:**

Zaliczenie przedmiotu na podstawie dwóch sprawdzianów w ciągu semestru. Ocenę punktową przelicza się na stopnie według poniższych zasad:
a) 3.0 jeżeli uzyskali od 51 do 60 pkt.
b) 3.5 jeżeli uzyskali od 61 do 70 pkt.
c) 4.0 jeżeli uzyskali od 71 do 80 pkt.
d) 4.5 jeżeli uzyskali od 81 do 90 pkt.
e) 5.0 jeżeli uzyskali powyżej 90 pkt.

**Egzamin:**

**Literatura:**

N. Koblitz,  Algebraiczne aspekty kryptografii,  WNT, Warszawa 2000
N. Koblitz,  Wykład z teorii liczb i kryptogafii,  WNT, Warszawa 1995
P. Ribenboim, Mała księga wielkich liczb pierwszych,  WNT, Warszawa, 1996
R. Lidl, H. Niederreiter, Introduction to Finite Field, Cambridge University Press,1996

**Witryna www przedmiotu:**

**Uwagi:**

## Efekty przedmiotowe