**Nazwa przedmiotu:**

Podstawy kryptografii

**Koordynator przedmiotu:**

Dr Barbara Roszkowska-Lech

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Matematyka

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

M2PKR

**Semestr nominalny:**

2 / rok ak. 2012/2013

**Liczba punktów ECTS:**

5

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

Udział w wykładach 15x2 = 30 godzin
Udział w ćwiczeniach 15x 1= 15 godzin
Przygotowanie do kolejnych wykładów 15 godzin
Przygotowanie do ćwiczeń 15 godzin
Przygotowanie do kolokwium , udział w konsultacjach 8+2 = 10 godzin
Udział w konsultacjach związanych z realizacją projektu 3x2 = 6 godzin
Przygotowanie projektu 30 godzin
Prezentacja projektu 1 godzina
Razem 122 godziny
4-5 punktów ECTS

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

2

**Język prowadzenia zajęć:**

polski

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

2

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

|  |  |
| --- | --- |
| Wykład:  | 30h |
| Ćwiczenia:  | 15h |
| Laboratorium:  | 0h |
| Projekt:  | 15h |
| 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:**

Bez limitu

**Cel przedmiotu:**

Celem przedmiotu jest przedstawienie teoretycznych podstaw współczesnej kryptografii oraz głównych problemów dotyczacych zagadnień kryptograficznych

**Treści kształcenia:**

Wstep historyczny.Systemy kryptograficzne z kluczem symetrycznym. Podstawowe pojecia kryptografii i krypto analizy
Szyfry strumieniowe i blokowe. Tryby działania lagorytmów blokowych. Szyfry permutacyjne, podstawieniowe i permutacyjno podstawieniowe, Enigma, Algorytmy DES i AES
Teorio liczbowe podstawy kryptografii(arytmetyka modularna, algorytm Euklidesa, chińskie twierdzenie o resztach, twierdzenie Fermata i Eulera reszty kwadratowe i logarytmy dyskretne, algorytmy faktoryzacji
Kryptosystemy z kluczem publicznym: kryptosystem RSA, algorytm Diffie- Hellmana, logarytmy dyskretne i krypto system ElGamala
Funkcje skrótu, dzielenia sekretu, dowody z wiedzą zerową, zobowiązania (gry na odległość)
Podpisy cyfrowe
Podstawowe wiadomości o krzywych eliptycznych i podstawy kryptografii z użyciem krzywych eliptycznych

**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:**

nie

**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:**

brak

**Uwagi:**

## Efekty przedmiotowe

### Profil ogólnoakademicki - wiedza

**Efekt PKR\_W01:**

zna struktury algebraiczne występujące w teorii liczb i w kryptografii

Weryfikacja:

zaliczenie

**Powiązane efekty kierunkowe:** MNI\_W04

**Powiązane efekty obszarowe:** X2A\_W01, X2A\_W02

**Efekt PKR\_W02:**

ma podstawową wiedzę dotyczącą konstrukcji systemów kryptograficznych;

Weryfikacja:

zaliczenie

**Powiązane efekty kierunkowe:** MNI\_W07

**Powiązane efekty obszarowe:** X2A\_W01, X2A\_W02, X2A\_W04

**Efekt PKR\_W03:**

zna klasyczne systemy kryptograficzne i kryptosystemy z kluczem publicznym;

Weryfikacja:

zaliczenie

**Powiązane efekty kierunkowe:** MNI\_W08

**Powiązane efekty obszarowe:** X2A\_W09, X2A\_W10, X2A\_W03, X2A\_W04, X2A\_W07, X2A\_W08

### Profil ogólnoakademicki - umiejętności

**Efekt PKR\_U01:**

umie posługiwać się językiem algebraicznym interpretując zagadnienia z różnych obszarów zastosowań kryptograficznych

Weryfikacja:

projekt

**Powiązane efekty kierunkowe:** MNI\_U04

**Powiązane efekty obszarowe:** X2A\_U04

**Efekt PKR\_U02:**

potrafi stosować metody algebry i teorii liczb w zagadnieniach kryptograficznych takich jak szyfrowanie i deszyfrowanie wiadomości w systemach symetrycznych i asymetrycznych, podpisywanie wiadomości, dzielenie sekretu, wymiana kluczy;

Weryfikacja:

projekt

**Powiązane efekty kierunkowe:** MNI\_U08

**Powiązane efekty obszarowe:** X2A\_U04

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt PKR\_K01:**

potrafi współdziałać i pracować w zespole, przyjmując w nim różne role;

Weryfikacja:

projekt

**Powiązane efekty kierunkowe:** MNI\_K01

**Powiązane efekty obszarowe:** X2A\_K02