**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:**

1120-MAMNI-NSP-0035

**Semestr nominalny:**

1 / rok ak. 2017/2018

**Liczba punktów ECTS:**

5

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

1. godziny kontaktowe – 65 h; w tym
a) obecność na wykładach – 30 h
b) obecność na ćwiczeniach – 15 h
c) obecność na laboratoriach – 15 h
d) konsultacje – 5 h
2. praca własna studenta – 60 h; w tym
a) przygotowanie do ćwiczeń i do testu – 30 h
b) zapoznanie się z literaturą – 10 h
c) przygotowanie do laboratorium – 20 h
Razem 125 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 – 15 h
c) obecność na laboratoriach – 15 h
d) 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 – 15 h
b) przygotowanie do laboratorium – 20 h
Razem 35 h, co odpowiada 1 pkt. ECTS

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

|  |  |
| --- | --- |
| Wykład:  | 30h |
| Ćwiczenia:  | 15h |
| Laboratorium:  | 15h |
| Projekt:  | 0h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

Przedmioty poprzedzające
1. Algebra i jej zastosowania I
2. Algebra i jej zastosowania II
3. Algebra liniowa z geometrią
Zalecane: Elementarna teoria liczb
Wymagania wstępne
1. Znajomość przestrzeni liniowych, ich bazy i wymiaru, przekształceń liniowych, macierzy.
2. Znajomość zagadnień związanych z podstawowymi własnościami pierścienia liczb całkowitych: kongruencje, arytmetyka modularna, algorytm Euklidesa, twierdzenie Chińskie o resztach.
3. Posiadanie wiedzy na temat konstrukcji i najważniejszych własności ciał skończonych

**Limit liczby studentów:**

Bez limitu

**Cel przedmiotu:**

Celem przedmiotu jest przedstawienie teoretycznych podstaw współczesnej kryptografii oraz głównych problemów dotyczących zagadnień kryptograficznych wraz z algorytmami stosowanymi w rozwiązaniach.

**Treści kształcenia:**

1. Wstęp historyczny. Systemy kryptograficzne z kluczem symetrycznym. Podstawowe pojęcia kryptografii i kryptoanalizy
2. Szyfry strumieniowe i blokowe. Tryby działania. Szyfry permutacyjne, podstawieniowe i permutacyjno podstawieniowe,
3. Maszyny szyfrujące na przykładzie Enigmy. Elementy Kryptoanalizy Enigmy.
4. Standardy szyfrowania DES, AES
5. Teorio liczbowe podstawy kryptografii (arytmetyka modularna, algorytm Euklidesa, chińskie twierdzenie o resztach, twierdzenie Fermata i Eulera reszty kwadratowe i logarytmy dyskretne, algorytmy faktoryzacji
6. Kryptosystemy z kluczem publicznym: kryptosystem RSA, algorytm Diffie- Hellmana, logarytmy dyskretne i krypto system ElGamala
7. Funkcje skrótu: własności, atak urodzinowy zastosowanie w kryptografii.
8. Dzielenie sekretu, dowody z wiedzą zerową, zobowiązania (gry na odległość)
9. Podpisy cyfrowe
10. Podstawowe wiadomości o krzywych eliptycznych i podstawy kryptografii z użyciem krzywych eliptycznych

**Metody oceny:**

Aktywność na warsztatach i laboratorium, test zaliczeniowy
Test końcowy (kolokwium) 50 punktów
Aktywność na ćwiczeniach 10 punktów
Laboratorium 40 punktów

**Egzamin:**

nie

**Literatura:**

1. Buchmann J. A. „Wprowadzenie do kryptografii”, PWN, 2006 rok, 244 s.
2. Stinson D. R. „Kryptografia w teorii i praktyce”, WNT, 2005 rok, 438 s
3. L.C. Washington, W. Trappe.. Introduction To Cryptography With Coding Theory
4. Neal Koblitz, Algebraiczne aspekty kryptografii, Wydawnictwo Naukowo-Techniczne, Warszawa 2000.
5. Neal Koblitz, Wykład z teorii liczb i kryptografii, Wydawnictwo Naukowo-Techniczne, Warszawa 1995.

**Witryna www przedmiotu:**

brak

**Uwagi:**

## Efekty przedmiotowe

### Profil ogólnoakademicki - wiedza

**Efekt PKR\_W01:**

Zna struktury algebraiczne występujące w teorii liczb i w kryptografii.

Weryfikacja:

Aktywność na zajęciach, kolokwium

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

**Powiązane efekty obszarowe:** , ,

**Efekt PKR\_W02:**

Ma podstawową wiedzę dotyczącą konstrukcji systemów kryptograficznych.

Weryfikacja:

Aktywność na zajęciach, kolokwium

**Powiązane efekty kierunkowe:** M2MNI\_W04

**Powiązane efekty obszarowe:**

**Efekt PKR\_W03:**

Zna klasyczne systemy kryptograficzne i kryptosystemy z kluczem publicznym.

Weryfikacja:

Aktywność na zajęciach, kolokwium

**Powiązane efekty kierunkowe:** M2MNI\_W04

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Efekt PKR\_U01:**

Umie posługiwać się językiem algebraicznym interpretując zagadnienia z różnych obszarów zastosowań kryptograficznych.

Weryfikacja:

Kolokwium, zaliczenie laboratorium

**Powiązane efekty kierunkowe:** M2MNI\_U02, M2MNI\_U03

**Powiązane efekty obszarowe:** ,

**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:

Kolokwium, zaliczenie laboratorium

**Powiązane efekty kierunkowe:** M2MNI\_U04

**Powiązane efekty obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt PKR\_K01:**

Potrafi współdziałać i pracować w zespole, przyjmując w nim różne role. Rozumie przydatność zdobytej wiedzy.

Weryfikacja:

Kolokwium, zaliczenie laboratorium

**Powiązane efekty kierunkowe:** M2MNI\_K02

**Powiązane efekty obszarowe:**