**Nazwa przedmiotu:**

Zaawansowane metody kryptografii i ochrony informacji

**Koordynator przedmiotu:**

prof. dr hab. inż. Zbigniew Kotulski

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Telekomunikacja

**Grupa przedmiotów:**

Przedmioty techniczne - zaawansowane

**Kod przedmiotu:**

MKOI

**Semestr nominalny:**

3 / rok ak. 2018/2019

**Liczba punktów ECTS:**

5

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

125

**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:**

1,5

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

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

**Wymagania wstępne:**

Zalecane przedmioty poprzedzające:
OINS, PKRY

**Limit liczby studentów:**

60

**Cel przedmiotu:**

Celem wykładu jest zaznajomienie słuchaczy ze współczesnymi algorytmami kryptograficznymi oraz metodami matematycznymi wykorzystywanymi w ich konstrukcji i analizie bezpieczeństwa. Wykład dostarcza informacji niezbędnych projektantom i administratorom systemów teleinformatycznych w zakresie stosowanych w nich zabezpieczeń kryptograficznych. Stanowi również wprowadzenie do metod projektowania i kryptoanalizy praktycznie stosowanych algorytmów kryptograficznych.
Pierwsza część wykładu obejmuje współczesną teorię kryptograficznych funkcji skrótu, szyfrów blokowych i strumieniowych, jak również metody generowania losowych ciągów binarnych dla potrzeb kryptografii. W drugiej części wykładu omawiane są algorytmy asymetryczne, w tym algorytmy wielomianowe i algorytmy oparte na krzywych eliptycznych. Silny nacisk położony jest na analizę bezpieczeństwa omawianych algorytmów oraz na ich praktyczne zastosowanie w ochronie informacji.

**Treści kształcenia:**

1. Historia kryptografii, metody matematyczne klasycznej kryptografii, teoria permutacji i elementy kombinatoryki.
2. Klasyfikacja algorytmów kryptograficznych. Teoria Shannona i jej rozszerzenia. Podstawy teoretyczne bezpieczeństwa algorytmów kryptograficznych.
3. Szyfry strumieniowe. Podstawy budowy i przykłady. Prymitywy wykorzystywane do projektowania szyfrów strumieniowych: LFSR, FCSR, rejestr kołowy. Tryby pracy szyfrów strumieniowych.
4. Elementy teorii liczb. Wielomiany nad ciałami skończonymi, Wielomiany nierozkładalne. Faktoryzacja wielomianów nad ciałami skończonymi. Przekształcenia nieliniowe w ciałach skończonych.
5. Kryptograficzne funkcje skrótu. Podstawy matematyczne i bezpieczeństwo algorytmów.
6. Podstawy budowy szyfrów blokowych. Funkcje boolowskie. Zasady budowy szyfrów, S-boxy, permutacje.
7. Przegląd współczesnych algorytmów blokowych, tryby pracy szyfrów blokowych.
8. Generatory liczb losowych, podstawowe typy generatorów i ich własności. Statystyczne metody testowania algorytmów kryptograficznych.
9. Podstawy matematyczne algorytmów asymetrycznych. Szyfrowanie i podpis elektroniczny.
10. Przegląd algorytmów asymetrycznych, testowanie pierwszości liczb naturalnych.
11. Algorytmy asymetryczne, RSA i problem faktoryzacji dużych liczb
12. Algorytmy asymetryczne, ElGamal i problem logarytmu dyskretnego
13. Szyfry wielomianowe – podpisy cyfrowe wielomianowe
14. Krzywe eliptyczne, podstawowe działania, izomorfizm krzywych, bezpieczne kryptograficznie krzywe eliptyczne, wykorzystanie do uzgodnienia klucza i podpisu elektronicznego ECDSA.
15. Podstawy kryptoanalizy, kryptoanaliza liniowa, różnicowa i wielomianowa. Ataki na tryby pracy algorytmów kryptograficznych.
Zakres ćwiczeń:
Działania w ciałach skończonych, operacje na wielomianach, działania na krzywych eliptycznych, podstawowe algorytmy teorii liczb i obliczeniowej teorii liczb, działanie elementów składowych algorytmów kryptograficznych, badanie obliczeniowych i statystycznych własności algorytmów kryptograficznych.
Zakres projektu:
Zaprogramowanie zadań ilustrujących budowę, analizę i realizację wybranych algorytmów kryptograficznych. Analiza i implementacja wybranych metod testowania algorytmów kryptograficznych. Analiza i implementacja wybranych metod obliczeniowych wspomagających konstruowanie i kryptoanalizę algorytmów.

**Metody oceny:**

Wymagane jest niezależne zaliczenie ćwiczeń i projektu (ponad 50% punktów) oraz zdanie egzaminu końcowego z tematyki wykładu.
Ćwiczenia są zaliczane na podstawie dwóch kolokwiów obejmujących metody rachunkowe będące przedmiotem zajęć. O zaliczeniu decyduje suma punktów z obu kolokwiów.
Projekt zaliczany jest na podstawie prezentacji zrealizowanego zadania i krótkiego sprawozdania.
Egzamin ma formę pisemną i dotyczy treści zagadnień przedstawionych na wykładzie. Dopuszczalne jest korzystanie z notatek.

**Egzamin:**

tak

**Literatura:**

Materiały dydaktyczne: po wykładzie na prywatnej stronie internetowej przedmiotu udostępniana jest treść wykładu oraz materiały dodatkowe niezbędne do uzupełnienia tematyki wykładu.
Literatura dodatkowa:
Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, “Kryptografia stosowana”, WN-T, Warszawa 2005, ISBN 83-204-2992-7

**Witryna www przedmiotu:**

https://studia.elka.pw.edu.pl/priv/12L/MKOI.A/

**Uwagi:**

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka MKOI\_W01:**

Zna zasady budowy i działania algorytmów kryptograficznych: symetrycznych, asymetrycznych i bezkluczowych

Weryfikacja:

Kolokwia 1 i 2, aktywny udział w ćwiczeniach, konsultacje, egzamin

**Powiązane charakterystyki kierunkowe:** K\_W03, K\_W08

**Powiązane charakterystyki obszarowe:** I.P7S\_WG

**Charakterystyka MKOI\_W02:**

zna podstawy matematyczne konstrukcji i analizy bezpieczeństwa algorytmów kryptograficznych

Weryfikacja:

Kolokwia 1 i 2, aktywny udział w ćwiczeniach, egzamin, konsultacje

**Powiązane charakterystyki kierunkowe:** K\_W01, K\_W14

**Powiązane charakterystyki obszarowe:** I.P7S\_WG

**Charakterystyka MKOI\_W03:**

zna zasady działania i praktycznej implementacji algorytmów kryptograficznych oraz ich zastosowań w systemech bezpieczeństwa teleinformatycznego

Weryfikacja:

sprawozdanie z projektu, konsultacje, egzamin

**Powiązane charakterystyki kierunkowe:** K\_W08, K\_W10, K\_W11

**Powiązane charakterystyki obszarowe:** I.P7S\_WG

### Profil ogólnoakademicki - umiejętności

**Charakterystyka MKOI\_U01:**

Potrafi samodzielnie zaimplementować algorytm kryptograficzny lub algorytm do kryptoanalizy i przeanalizować efekty jego działania

Weryfikacja:

implementacja zadania projektowego, konsultacje

**Powiązane charakterystyki kierunkowe:** K\_U01, K\_U09, K\_U13

**Powiązane charakterystyki obszarowe:** I.P7S\_UK, I.P7S\_UW

**Charakterystyka MKOI\_U02:**

Potrafi zaprezentować rozwiązanie problemu technicznego i ocenić jego jakość w formie raportu realizacji i testów

Weryfikacja:

sprawozdanie z projektu, konsultacje

**Powiązane charakterystyki kierunkowe:** K\_U14, K\_U15, K\_U02, K\_U04, K\_U06

**Powiązane charakterystyki obszarowe:** III.P7S\_UW.3.o, I.P7S\_UW, I.P7S\_UO, III.P7S\_UW.2.o, III.P7S\_UW.4.o, I.P7S\_UK, III.P7S\_UW.1.o

**Charakterystyka MKOI\_U03:**

ma umiejętność oceny przydatności alternatywnych rozwiązań technologicznych do rozwiązania zadań inżynierskich

Weryfikacja:

egzamin, konsultacje

**Powiązane charakterystyki kierunkowe:** K\_U06, K\_U08, K\_U12

**Powiązane charakterystyki obszarowe:** I.P7S\_UW, III.P7S\_UW.1.o, III.P7S\_UW.3.o, III.P7S\_UW.2.o

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka MKOI\_K01:**

potrafi pracować indywidualnie i w zespole

Weryfikacja:

aktywność na ćwiczeniach, realizacja zadania projektowego

**Powiązane charakterystyki kierunkowe:** K\_K01

**Powiązane charakterystyki obszarowe:** I.P7S\_KO

**Charakterystyka MKOI\_K02:**

uzyskuje świadoność konieczności stosowania zabezpieczeń kryptograficznych w praktyce telekomunikacyjnej

Weryfikacja:

konsultacje, aktowność na ćwiczeniach i wykładzie

**Powiązane charakterystyki kierunkowe:** K\_K02

**Powiązane charakterystyki obszarowe:** I.P7S\_KK, I.P7S\_KR