**Nazwa przedmiotu:**

Podstawy teoretyczne kryptografii i ochrony informacji - A

**Koordynator przedmiotu:**

prof. dr hab. inż. Zbigniew KOTULSKI

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia I stopnia

**Program:**

Informatyka

**Grupa przedmiotów:**

Kierunkowe

**Kod przedmiotu:**

PTKA

**Semestr nominalny:**

1 / 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:  | 15h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

**Limit liczby studentów:**

**Cel przedmiotu:**

Wykład obejmuje klasyczną teorię szyfrów blokowych i strumieniowych z uwzględnieniem nowoczesnych szyfrów symetrycznych (AES) i metody generowania losowych ciągów binarnych. W drugiej części wykładu omawiane są algorytmy asymetryczne, w tym algorytmy wiel

**Treści kształcenia:**

 Budowa, analiza i implementacja wybranych algorytmów kryptograficznych . Analiza i implementacja wybranych metod testowania algorytmów kryptograficznych. Analiza i implementacja wybranych metod obliczeniowych wspomagających budowę i kryptoanalizę algorytm

**Metody oceny:**

**Egzamin:**

**Literatura:**

Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, <I>"Kryptografia stosowana"</I>, WN-T, Warszawa 2005, ISBN 83-204-2992-7

**Witryna www przedmiotu:**

**Uwagi:**

## Efekty przedmiotowe