Tytuł **Kryptologia**	Kod **1010332431010330742**
Kierunek **Informatyka**	Rok / Semestr **2 / 3**
Specjalność **Bezpieczeństwo systemów informatycznych**	Przedmiot **obowiązkowy**
Godziny Wykłady: **2** Ćwiczenia: **-** Laboratoria: **-** Projekty / seminaria: **-**	Liczba punktów **6**
	Język prowadzenia przedmiotu **polski**

Prowadzący:

dr hab. inż. Janusz Stokłosa
Instytut Automatyki i Inżynierii Informatycznej
tel. +48 61 665 37 57
e-mail: janusz.stoklosa@put.poznan.pl

Wydział:

Wydział Elektryczny
ul. Piotrowo 3A
60-965 Poznań
tel. (061) 665-2539, fax. (061) 665-2548
e-mail: office_deef@put.poznan.pl

Miejsce przedmiotu w programie studiów:

- Cryptology

Założenia i cele przedmiotu:

- Celem jest zapoznanie studentów z zasadami działania i projektowania algorytmów kryptograficznych.

Treści programowe przedmiotu (opis przedmiotu):

- Treści prezentowane na wykładzie:

1. Szyfry blokowe
   - Przykłady szyfrów blokowych (CAST-128, RC5, Blowfish, Safer)
   - Permutacje, podstawienia, funkcje boolowskie
   - Kryteria projektowania bloków podstawień
2. Generatory ciągów pseudolosowych
   - Generatory ciągów
   - Komponenty generatorów: LFSR, NFSR, FCSR
   - Losowość ciągów
   - Złożoność liniowa ciągów
3. Szyfry strumieniowe
   - Szyfry synchroniczne i samosynchronizujące
   - Przykłady
4. Szyfry wykładnicze
   - Rabina, ElGamala, Pohlinga-Hellmana, plecakowy
5. Funkcje skrótu
   - Dedykowane (SHA),
   - Zbudowane z wykorzystaniem arytmetyki modularną
   - Atak urodzinowy
6. Podpisy cyfrowe
   - DSA
   - El-Gamal
   - Kryptografia na krzywych eliptycznych
7. Uwierzytelnianie
   - Dowody wiedzy zerowej
8. Niezaprzeczalność

9. Zarządzanie materiałem kryptograficznym
   - Protokół El-Gamala
   - Współdzielenie sekretu - KGH
   - Model Lenstry-Verheula

Przedmioty wprowadzające i wymagane wiadomości wstępne:

- materiał z kursów: podstawy ochrony danych, algebra wyższa

Forma zajęć i metody dydaktyczne:

- Wykłady jako prezentacje multimedialne.

Forma i warunki zaliczenia przedmiotu – wymagania i system oceniania:

- Egzamin pisemny, ustny lub pisemny i ustny.

Bibliografia podstawowa:

-

Bibliografia uzupełniająca:

-