KARTA PRZEDMIOTU

Wydział Automatyki, Elektroniki i Informatyki, Rok akademicki: 2009/2010

Nazwa przedmiotu:	**KRYPTOGRAFIA I OCHRONA DANYCH**	Kod/nr KiOD
Kierunek:	INFORMATYKA	
Specjalność:	PRZEDMIOT OBIERALNY DLA WSZYSTKICH SPECJALNOŚCI	
Tryb studiów:	NIESTACJONARNE DRUGIEGO STOPNIA	
Rodzaj przedmiotu:	TECHNICZNY	**Liczba pkt ECTS 4**
Instytut/ Katedra:	INFORMATYKI	
Semestr:	I	
Prowadzący przedmiot:	dr inż.. Jacek Lach	

Prowadzący zajęcia:	Liczba godzin
Wykład: dr inż. Jacek Lach Ćwiczenia: - Laboratorium: dr inż. Jacek Lach Projekt: - Seminarium: -	Wykład: 30 h Ćwiczenia: - Laboratorium: 30 h Projekt: - Seminarium: -

Powiązanie ze standardami i cel kształcenia

Wykłady mają za zadanie przedstawić podstawowe pojęcia z dziedziny kryptologii — nauki o projektowaniu i stosowaniu szyfrów. W ramach zajęć zostaną również omówione zaawansowane metody: szyfrowania danych, oceny bezpieczeństwa kryptosystemów. Przedmiot dawniej prowadzony pod nazwą Podstawy kryptologii uzupełniony został o praktyczne aspekty zastosowania algorytmów kryptograficznych z punktu widzenia zarówno użytkownika końcowego jak i programisty. Kurs przeznaczony jest dla osób, które nie tylko chcą korzystać z kryptografii, ale zainteresowane są również tym jak działają poszczególne mechanizmy co umożliwi jej świadome wykorzystanie.

Przedmioty wprowadzające oraz wymagania wstępne

Programowanie komputerów, Systemy operacyjne, Algorytmy i struktury danych.

Treść wykładów:

Wprowadzenie

Wybrane zagadnienia z teorii informacji i teorii liczb

Podstawowe zagadnienia z zakresu kryptoanalizy

Zarządzanie kluczami

Szyfry blokowe. Szyfry strumieniowe. Tryby pracy.

Sieci Feistela. Algorytm DES. Algorytmy IDEA, RC5, Rijndael.

Ciągi losowe i pseudolosowe. Szyfry strumieniowe.

Funkcje skrótu.

Algorytmy asymetryczne.

Krzywe eliptyczne w kryptografii.

Podpis cyfrowy.

PKI, PGP

Steganografia, kryptografia wizualna.

Bezpieczeństwo systemów: szyfrowane systemy plików

Bezpieczeństwo systemów: kontrola dostępu.

Bezpieczeństwo systemów i sieci: testy penetracyjne.

Bezpieczeństwo systemów i sieci: ściany ogniowe, systemy wykrywania intruzów.

Treść/Tematy: Ćw./L./P./Sem.

1. Szyfry podstawieniowe i przestawieniowe. Rozkład częstości. Kryptoanaliza szyfru Vigenere'a
2. Kryptoanaliza. Łamanie brutalne i słownikowe.
3. Generatory pseudolosowe. Szyfry strumieniowe
4. Szyfrowanie symetryczne
5. Szyfrowanie z kluczem publicznym
6. Elementy testów penetracyjnych: skanowanie, podsłuch, identyfikacja.

Metody dydaktyczne

Wykład prowadzony z wykorzystaniem prezentacji komputerowych. Laboratorium prowadzone na komputerach klasy PC.

Forma egzaminu/zaliczenia przedmiotu

1. Wykład — Test pisemny.

2. Ćw./L./P./Sem.

Ocenie podlega wykonanie ćwiczeń i dostarczenie raportów z ich wykonania.

Minimalne wymagania do egzaminu /zaliczenia

Wykonanie serii ćwiczeń i oddanie raportów z ich wykonania

Literatura (podstawowa i specjalistyczna)

A. J. Menezes, P. C. Van Oorschot, S.A. Vanstone: Kryptografia stosowana.WNT

N. Koblitz: Algebraiczne aspekty kryptografii. WNT

D. Robling-Denning: Kryptografia i ochrona danych. WNT

B. Schneier: Kryptografia dla praktyków. WNT

R. Wobst: Kryptologia. Budowa i łamanie zabezpieczeń

Zatwierdzono:

……. ……

(data i podpis prowadzącego) (*data i podpis Dyrektora Instytutu/Kierownika Katedry)*