Politechnika Gdańska
Wydział Fizyki Technicznej i Matematyki Stosowanej

Karta Przedmiotu

Kierunek	Matematyka	**Data**	01.10.08
Specjalność	Matematyka Stosowana		
Rodzaj studiów	stacjonarne		
Przedmiot (po polsku)	Kryptografia	**Kod**	
Przedmiot (po angielsku)	Cryptography	**Egzamin**	Tak

Semestr	9	**Godziny**	w	ć	l	p	s	**Punkty kredytowe**	6
			2		1	1			

Autor	dr inż. Ryszard Sobczak, doc.PG
Katedra	Matematyki Dyskretnej

1. Konspekt przedmiotu i wykaz zalecanej literatury

Wykład:
Wprowadzenie (2g)

Definicja, otoczenie, literatura. Kodowanie, kompresja i szyfrowanie. Historia do roku 1900. Historia współczesnej kryptologii. Kryptologia militarna i dyplomatyczna. Prawne aspekty stosowania kryptologii. Legalne podsłuchiwanie komunikacji

Kryptologia symetryczna (z kluczem tajnym)
- Kryptografia tekstów w tym:
  Algorytmy podstawieniowe. Jakość algorytmu kryptograficznego. Kryptoanaliza statystyczna. Algorytmy przestawieniowe. Teoria informacji i wyniki Shannona. Podsumowanie (2g)
  Enigma: działanie i kryptoanaliza (2g)
- Kryptografia ciągów binarnych w tym:
  Algorytmy blokowe. Algorytm DES. Tryby pracy algorytmu. Jakość algorytmu DES (1g).
  Kryptoanaliza: różnicowa i liniowa (2g)
  Projektowanie algorytmów blokowych. Łączenie algorytmów blokowych (TDES). Inne algorytmy blokowe (1g).
  Algorytm Rijndael (2g).
  Proste protokoły kryptograficzne z zastosowaniem algorytmów symetrycznych (1g)
  Algorytmy strumieniowe. Algorytm A5 (GSM). Generatory ciągów pseudolosowych. Analiza i projektowanie szyfrów strumieniowych (2g).

Kryptografia asymetryczna (z kluczem publicznym)
- Źródła problemu. Algorytm plecakowy. Algorytm RSA. Jakość algorytmu RSA (4g)
- Algorytmy ElGamala i stosujące krzywe eliptyczne (2g).
- Inne algorytmy asymetryczne. Projektowanie algorytmów asymetrycznych (2g)

Jednokierunkowe funkcje skrótu (2g)
- Definicja. Funkcja Snefru. Funkcje MDn. Funkcja SHA. Jakość jednokierunkowych funkcji skrótu

Zaawansowane protokoły kryptograficzne (3g)
- Uczciwe rzucanie monetą. Powierzanie kluczy. Podpisy niezaprzeczalne. Jednoczesne podpisywanie kontraktu. Protokoły ezoteryczne. Bezpieczne wybory. Cyfrowe pieniądze. Ocena jakości protokołów

Stosowanie kryptografii (1g)
- Patentowanie algorytmów. Ochrona przesyłanych i przechowywanych danych. Zasady stosowania algorytmów kryptograficznych. Regulacja prawne. Uwierzytelnianie. Podpis elektroniczny. Stosowanie kryptografii w gospodarce elektronicznej.

Przyszłość kryptologii i inne techniki ochrony informacji (1g)
- Kryptografia kwantowa. Steganografia.

Laboratorium: (z zastosowaniem programu Cryptool)

Ćw. 1 Program Cryptool (1g). Kryptografia tekstów. Szyfry podstawieniowe i przestawieniowe (1g).

Ćw. 2 Kryptoanaliza szyfrów podstawieniowych. Badanie statystyki występowania znaków w plikach tekstowych w języku polskim i angielskim, w języku C i w plikach wykonywalnych. Metoda koincydencji. Wyznaczanie liczby elementów słowa kluczowego szyfru podstawieniowego (2g)

Ćw. 3 Kryptografia z zastosowaniem współczesnych algorytmów symetrycznych (2g).

Ćw. 4 Kryptoanaliza różnicowa uproszczonego algorytmu DES (2g).

Ćw. 5 Kryptografia z zastosowaniem algorytmów niesymetrycznych (2g).
Ćw. 6 Metody generowania kluczy jawnych oraz prywatnych z zastosowaniem generatora liczb pseudolosowych i testów pierwszości (2g)
Ćw. 7 Protokoły kryptograficzne i usługi internetowe. (2g)

Projekt:
Implementacja prostych algorytmów kryptologicznych albo raport z analizy jakości wskazanych algorytmów bądź protokołów kryptograficznych.

Literatura:
Stinson D.R.: Kryptografia. W teorii i praktyce, Warszawa: Wydawnictwa Naukowo-Techniczne, 2005
Stinson D.R.: Cryptography. Theory and practice, CRC Press LLC, Third ed., 2005
Notatki do wykładu ‘Kryptografia’ (w systemie Moodle)

Obowiązkowe przedmioty poprzedzające	**Kod przedmiotu**
Matematyka dyskretna	
Algebra	
Rachunek prawdopodobieństwa	

Autor

.....

Przewodniczący Komisji Programowej/Dziekan

.....