Ewa Kozłowska-Walania
Zakład Algebry, Instytut Matematyki UG

Seminarium licencjackie

Algebraiczne aspekty kryptografii

Często gdy stykamy się z abstrakcyjnymi zagadnieniami matematycznymi - jak choćby te związane z teorią grup, pierścieni czy ciał - może nam się wydawać, że nie mają one zastosowania w realnym świecie, prawda jest jednak zupełnie inna. Żyjemy w czasach, gdy jedną z podstawowych walut jest *informacja*. W każdej sekundzie na świecie miliardy danych jest szyfrowanych, przesyłanych, udostępnianych innym użytkownikom, chronionych przed nieautoryzowanym dostępem. Wszystkie te operacje stają się zrozumiałe dla osoby znającej podstawy algebry i teorii liczb, gdyż właśnie te dziedziny matematyki leżą u podstaw kryptografii - od pojawiającego się w Biblii szyfru AtBash i **klasycznego szyfru Cezara** aż po współczesny system RSA i kryptosystemy eliptyczne. Zapraszam do uczestnictwa wszystkich, którzy interesują się algebrą lub teorią liczb i chcieliby poszerzyć swoją wiedzę w tym zakresie, ze szczególnym uwzględnieniem zastosowań w kryptografii. Tematy referatów i prac licencjackich będą dotyczyć zagadnień wymienionych w zamieszczonym poniżej Planie seminarium oraz oczywiście zależeć od indywidualnych zainteresowań Uczestników, przy czym znajdzie się miejsce zarówno dla tematów czysto teoretycznych, jak i tych bardziej nastawionych na zastosowania.

PBOABZWKFB WXMOXPWXJ!

Orientacyjny plan seminarium:

(1) Elementy teorii liczb: oszacowanie czasu wykonywania działań arytmetycznych, kongruencje, algorytm Euklidesa, ułamki łańcuchowe, równanie Pella.
(2) Pewne zagadnienia algebry: własności ciał skończonych, reszty kwadratowe i prawo wzajemności, pierścień wielomianów, tw. Hilberta o bazie i o zerach, bazy Gröbnera.
(3) Podstawy kryptografii: szyfry afiniczne, macierze szyfrujące, systemy z kluczem publicznym, kryptosystem RSA, schemat Diffiego-Hellmana, zagadnienie logarytmu dyskretnego, dzielenie sekretów, problem pakowania plecaka.
(4) Liczby pierwsze i rozkład na czynniki: liczby pseudopierwsze, metoda ρ, metoda Fermata, metoda sita kwadratowego.
(5) Krzywe eliptyczne i hipereliptyczne: reguła dodawania, krzywe nad poszczególnymi ciałami, kryptosystemy eliptyczne i hipereliptyczne.

Literatura:
1. Neal Koblitz, Algebraiczne aspekty kryptografii, Wydawnictwo Naukowo-Techniczne, Warszawa 2000.
2. Neal Koblitz, Wykład z teorii liczb i kryptografii, Wydawnictwo Naukowo-Techniczne, Warszawa 1995.
3. Ian Blake, Gadiel Seroussi, Nigel Smart, Krzywe eliptyczne w kryptografii, Wydawnictwo Naukowo-Techniczne, Warszawa 2004.
4. Jerzy Gawinecki, Janusz Szmidt, Zastosowanie ciał skończonych i krzywych eliptycznych w kryptografii, Wojskowa Akademia Techniczna, Warszawa 1999.
5. Kenneth Ireland, Michael Rosen, A classical introduction to modern number theory, Springer-Verlag 1990.
6. Kenneth H. Rosen, Elementary number theory and its applications, Addison Wesley Publishing Company, 1988.
7. Yan Song Y., Teoria liczb w informatyce, PWN 2006.
8. Donald Knuth, Sztuka programowania, Wydawnictwo Naukowow-Techniczne, 2002.