CMPT 881/MATH 800
Course Project, Fall 2006

Michael Monagan

Please choose one of the following three projects.
The project is due Wednesday December 13th at 5pm.

Project 1 involves quite a bit of programming and finite fields.
Project 2 involves proving some theorems and doing some programming.
Project 3 involves some programming, some experimentation and finite fields.

Project 1: The Advanced Encryption Standard

Implement AES and answer exercises 3.5 and 3.6 from the text and also show how to decrypt the ciphertext from 3.6 using AES.

In your implementation of the 8 bit S-box, use algorithm 3.4. You can use Maple to do the finite field arithmetic needed to construct the S-box.

Project 2: The Pohlig-Hellman Algorithm

Exercises 6.4, 6.5 and 6.7 on page 276.
Use your solution to 6.5 to answer 6.4 (d).

Project 3: The Index Calculus Algorithm

Implement the index calculus algorithm for computing discrete logs in $\mathbb{Z}_p^*$ and use your implementation to do exercise 6.1. You can use Maple's `msolve` command to solve a linear system modulo n or (a good exercise) write your own.

But how how many primes should the factor base B have? Pick a prime p of a suitable size (e.g. 12 digits), such that $p = 2q + 1$ and q is also prime. Pick a primitive element α and and generate $\beta = \alpha^x \bmod p$. Now time your indexed calculus algorithm to compute x using different sizes for B, e.g., $|B| = 10, 20, 40, 80, 160, ...$ to determine the optimal size for factor base B.

Now design and implement the index calculus algorithm to compute discrete logs in the finite field $GF(p^k)^*$. Test your algorithm out in the field GF(2^{50}), the finite field with 2^{50} elements, with your own example.