Class Schedule

Week 1: Introduction

Week 2: Galois fields theory and implementation of Galois field arithmetic.

Week 3: Advanced Encryption Standard

Week 4: Elliptic curve cryptography

Week 5: Long number arithmetic: Montgomery and Karatsuba-Ofman algorithms

Week 6: Exponentiation algorithms

Week 7: Midterm exam

Week 8: Stream ciphers and linear feedback shift registers

Week 9: True random number generators

Week 10: Attacks against discrete logarithms: Shank's algorithm, Pollard's-rho method, Index calculus method.

Week 11: Side channel analysis

Week 12: Secret sharing, threshold schemes, zero knowledge proofs.

Week 13: Quantum cryptography

Week 14: Project presentations

Week 15: Project paper due

Week 16: Final exam

Important Dates

First day of class: Tuesday, January 25th, 7:20–10:00 p.m.

Midterm Exam: Tuesday, March 8th

Spring Break: Tuesday, March 15th

Project Presentations: Tuesday May 3rd

Final Project Paper Due: Tuesday May 10th

Final Exam: Tuesday, May 17th, 7:30–10:15 p.m.

This schedule is subject to change.