Class Schedule

Week 1: Introduction, Galois fields theory

Week 2: Implementation of Galois field arithmetic.

Week 3: Advanced Encryption Standard (AES)

Week 4: Implementation of AES

Week 5: Elliptic curve cryptography

Week 6: Long number arithmetic: Montgomery and Karatsuba-Ofman algorithms

Week 7: Midterm exam

Week 8: Identitiy based Encryption

Week 9: Exponentiation algorithms

Week 10: Stream ciphers and linear feedback shift registers

Week 11: True random number generators

Week 12: Attacks against discrete logarithms: Shank's algorithm, Pollard's-rho method, Index calculus method.

Week 13: Side channel analysis

Week 14: Secret sharing, threshold schemes, zero knowledge proofs.

Week 15: Project presentations

Week 16: Final exam

Important Dates

First day of class: Tuesday, January 22nd, 4:15 – 7:10 p.m.

Midterm Exam: Tuesday, March 5th

Spring Break: Tuesday, March 12th

Draft Project Paper Due: Tuesday April 30th

Project Presentations: Tuesday May 7th

Final Project Paper Due: Tuesday May 7th

Final Exam: Tuesday, May 14th, 7:30–10:15 p.m.

This schedule is subject to change.