Topics in Cryptography, CS 381/780

Spring, 2015, Prof. K. D. Boklan

Course Prerequisites: Though we have no formal course prerequisites (more than a course in Discrete Mathematics – or CS220), students should have a good background and comfort with Mathematics. In particular, they should be familiar with basic number theory (congruences, primitive roots, quadratic residues,…) and algebra (finite fields). It would also be a good idea for students who have not had a Cryptography class before to familiarize themselves with some basic cryptographic protocols. Basic programming skills will be useful (but not absolutely demanded). Masters-level students need to have completed all of their required conditional classes to take 780.

**We** begin with an introduction to elliptic curves (over the field F\_p) and how this leads to a beautiful version of the Diffie-Hellman protocol through the deep theory of pairings. From there we will discuss Lenstra’s elliptic curve factoring algorithm and then onto other topics including Shamir’s attack on Knapsack, vulnerabilities in A5 (GSM encryption), linear complexity and the Berlekamp-Massey algorithm for LFSR’s and the Pohlig-Hellman algorithm for discrete logarithms and index calculus ‘attacks’ against elliptic curves.

We’ll probably have a take-home exam or two and a few small projects.