Intermediate Cryptanalysis, CSE 599R

John Manferdelli, University of Washington

This is a one year sequence in cryptanalysis which is rarely taught as the central theme of a class. Despite the rarity, cryptanalysis is a very attractive blend of pure mathematics (algebra, group theory, linear algebra, probability, statistical inference, coding theory, number theory, combinatorial theory), real computation and computer science.

The focus of the class is different from most I've seen. We will try to show you concretely how to implement and solve real cryptosystems. The approach is very concrete and focuses on a few very basic ideas:

1. Clarify the requirements and attack model for a cipher, including the real life computational resources and "side channel" information available to the identified adversary.
2. Study the mathematical model of the cipher (typically equations) and their statistical behavior.
3. Characterize the equations and the computational methods that solve them.
4. Solve the equations (often using a randomizing technique).

The **first quarter** will be a fairly gentle introduction to "mathematical cryptography" emphasizing simple computational techniques and methods. We will cover chapters 1 through 8, 15 and maybe parts of 16, 17 and 18 of *Introduction to Cryptography and Coding Theory* by Trappe and Washington supplemented by a little additional material on equations solving, group theory, statistical inference and linear algebra. I like Trappe and Washington because it gets to the heart of the theory emphasizing computational intuition with a minimum of fuss; however, there are lots of other good books. We'll cover the standard symmetric cipher theory, cryptographic hashes and public key theory. We may do a little on "side channel attacks." One nice thing is that there are several simple new techniques (Shamir's Bug attacks, timing attacks, and algebraic cryptanalysis) that are relatively painlessly explained even in this simple setting. The first quarter will also provide the common vocabulary for the next two quarters. Topics include: DES, AES, algebraic equations, solving large systems of equations, statistical tests and randomized computation, simple linear and differential cryptanalysis, group theoretic aspects of cryptographic transformations, Galois fields, polynomial complexity, inverses, iterated ciphers, key schedule, weak keys; all from a very concrete and down-to-earth point of view. The first quarter will likely be graded on the basis of homework assignments and a few tests, but I don't expect them to be too strenuous.

In the **second quarter**, we will study block ciphers, stream ciphers and cryptographic hashes in a hands - on manner. We will study the theory of functions over finite fields, solving algebraic equations over finite fields, how "iterative" ciphers are built from simple component functions, approximation of such equations (allowing much simpler solutions), re-estimation and other statistical techniques and the Fourier theory of equations over finite fields (Walsh transforms, correlation matrices, representations of the elements in S_n describing underlying cipher elements, etc.). These techniques will be applied to all three types of cryptosystems of interest. Topics include: DES, AES, FEAL, RC4, A5, MD4, MD5, SHAx, big algebraic equations, solving very large systems of equations, sensitive statistical tests and randomized computation (e.g.- Baum's Expectation-Maximization, Berlekamp's method for solving univariate high degree polynomials), linear and differential cryptanalysis in depth, deeper group theoretic aspects of cryptographic transformations, polynomial complexity, representations of iterated ciphers, key schedule, and weak keys all from a much more sophisticated, but still concrete point of view. There will be no text, but Daemen's thesis, the AES book by Daemen and Rijmen, the book of Cid, Robshaw and Murphy, Rueppel's book, Stamp and Low's book and a number of papers of Shamir, Biham, Wang and others will give a good flavor of the topics.

In the **third quarter**, we will study public key ciphers in the same hands-on manner we used to study symmetric systems. We will study the number theory, algebraic geometry, and statistical techniques to solve the equations that arise in public key systems as well as implementation techniques for "large integer" arithmetic. Boneh's survey paper, Washington's *Number Theory and Cryptography* and papers in computational techniques are representative of the level and type of material.

We will not cover cryptographic protocols, "the computational theory of cryptography" (a la Goldreich) or all the really stupid things you can do when you actually implement a strong cryptosystem in the real world (but you'll have a superior intuition about this as a result of the class). These are all taught in more standard courses.

This is a slightly unusual class which I will try to pitch to the actual class population and I hope it will be fun. We may follow it by a reading course or seminar if there is interest.