Fall 2008: Math 295A/395A: Cryptography

Ever wonder what it means when that little padlock appears on your web browser?

We live an information age, with technology increasingly integrated into our daily lives. As a result, the *security* of our information is of the utmost concern, even as the interconnectedness of the Internet makes our data more vulnerable to attack. The ability to encrypt secrets and to conduct a trusted exchange of digital information, once a subject of interest primarily to governments and the military, is now a matter of necessity for us all.

At the end of the day, the foundation of modern cryptography relies upon the difficulty of solving certain mathematical problems; this course is intended to address them from both a mathematical and algorithmic point of view. We will cover some subset of the following topics: conventional encryption techniques, the Hill cipher, DES and SDES, RSA, the Rijndael cipher, discrete logarithms and the Diffie-Hellman key exchange, and elliptic curve cryptography.

All mathematical objects will be defined, so the prerequisites are minimal: Math 52 or 124, or permission should suffice. The course will be offered at a 295 level intended for undergraduates with a minimal background and at a 395 level for graduate students or others who are seeking a challenge. Computationally-minded individuals are especially welcome! The class will be driven by applications and examples.

- **Lectures**: MWF 1:25–2:15 p.m.
- **Instructor**: John Voight
- **Web Page**: `http://www.cems.uvm.edu/~voight/`
- **Prerequisites**: Math 52, 124 or permission.