Cryptography
Math 626, Spring 2003

Michael E. O'Sullivan

Suggestions for Projects

Projects may be an oral report to the class, a written report, a computer program or a combination of these.

You may work with another person. Larger teams are ok if there is a clear division of tasks and you discuss it with me.

Please discuss your idea for a project with me before getting to deeply involved.

Here are some possible subjects for a project.

1. Ancient history: the attack on Enigma, or the attack on Purple.
2. One of the industry protocols, for security: e.g. PGP, SSL, SSH.
3. Hash functions.
4. Random number generators.
5. One of the industry standards, see the links at the bottom of the home page for the course, or talk to me or Flip.
   (a) Give an overview of the whole standard.
   (b) Dig into the details of one aspect, such as generation of a prime or encrypting exponent.
6. Other cryptographic protocols: e.g. secret sharing, zero knowledge proofs.
7. P versus NP, or other NP problems.
8. Other cryptosystems (NTRU at `http://www.ntru.com/cryptolab/algorithms.htm`, or Cayley-Purser code and Sarah Flannery's work, see `http://www.profilebooks.co.uk/procat/2000/flannery_01.htm`)
9. An educational module on cryptography for high school students. See `http://www.zeal.com/category/preview.jhtml?cid=10098424`.
10. Advanced versions of what we have done (e.g. the quadratic sieve or number field sieve, or more work on elliptic curves).
11. The paper "Primes is in P."
12. Attacks on DES, or similar cryptosystems.
13. Attack on the knapsack cryptosystem.
14. Quantuum cryptography.
15. Shor's quantuum factoring algorithm.