# Introduction to Cryptography

Review Midterm 1

October 16, 2006

Here's what you need to know:

- The background from elementary number theory (Euler-Fermat, Chinese Remainder, Euclidean algorithm; Bezout; computation of inverses modulo $n$; existence of primitive roots etc.)
- Solving simple cryptograms; what is frequency analysis?
- complexity: explain how to find the complexity of the most basic arithmetic operations (addition, multiplication, powering; similarly for polynomials with bounded coefficients).
- RSA: how and why it works; "stupid things to do"; attacks
- primality tests (Fermat, Miller-Rabin)
- primality proofs (via $p-1$ or AKS); only the basic ideas, no details.
- factorization methods: trial division, Fermat, Pollard's $p-1$ and $\rho$ method; birthday paradox

Diffie-Hellman and discrete logs will be on midterm 2.