MAT 4930, Fall 2013

Cryptography and Coding

Topics for the first test

Classical Cryptosystems:

- Shift cipher
- Affine cipher
- Vigenere cipher
- Hill cipher
- LFSR sequences

Basic Number Theory

- Solving congruences
- Modular Exponentiation
- Fermat and Euler theorems
- Inverting matrices mod n
- Continued fractions

The RSA algorithm

- The RSA algorithm (encoding/decoding)
- Attacks on RSA (low-exponent, short plaintext, cycling)
- Primality testing (Fermat, Miller-Rabin)
- Factoring ((p-1)-factoring, quadratic sieve