Math 5405/Cryptography/Spring 2013
Review for the First Midterm

Stuff you should be able to define.

(1) A public key.
(2) Carmichael Numbers.
(3) Korselt's Criterion for Carmichael Numbers.
(4) The circle group (in fields with p^2 elements).
(5) A hash function.

Cryptography-related procedures you should know.

(1) The Diffie-Hellman Key Exchange
(2) The RSA Cipher
(3) The El-Gamal Cipher
(4) The Miller-Rabin primality test.
(5) How to check an element (mod p) for primitivity.

Hacks you should be able to describe.

(1) The $p-1$ method for factoring.
(2) The $p+1$ method for factoring.
(3) The Quadratic Sieve for factoring.
(4) The baby step/giant step method for finding discrete logs.
(5) The Pohlig-Hellman method for finding discrete logs.
(6) The Index Calculus for finding discrete logs.