Math 5405/Cryptography/Spring 2013
Review for the Final Exam

Definitions.

(1) A public key.
(2) A hash function.
(3) The order of an element of a group.
(4) Lagrange's Theorem.
(5) An (n, M, d) q-ary code.
(6) A code that error detects vs error corrects to t places.
(7) A Hamming code.
(8) A primitive element of a cyclic group.
(9) The discrete logarithm with respect to a primitive element.
(10) A Carmichael Number and Korselt's Criterion.
(11) The circle group (in fields with p^2 elements).
(12) An elliptic curve in Weierstrass form and its discriminant.
(13) The group law on an elliptic curve.
(14) Cuspidal vs nodal degenerate elliptic curves.
(15) The group $E(p)$ associated to an elliptic curve (and a prime p).
(16) Hasse's bound on the number of points of an $E(p)$.
(17) The fields $\mathrm{GF}(2^d)$.

Cryptostuff.

(1) The Diffie-Hellman Key Exchange
(2) The RSA Cipher
(3) The El-Gamal Cipher
(4) Formulate each of the above on an elliptic curve $E(p)$.

More of a Number Theory Flavor

(1) The Miller-Rabin primality test.
(2) Various factoring methods (there are four).
(3) Various methods for computing discrete logs (there are three).
(4) How to check an element of a group for primitivity.
(5) Computations in $\mathrm{GF}(2^d)^\times$.

Elliptic Curves in Particular

(1) Be able to add and double points on an elliptic curve (or $E(p)$).
(2) Be able to compute the order of a point on $E(p)$.
(3) Use Savin's two propositions to find $E(p)$'s with $p+1$ elements.
(4) Contrast $E(p)$ with the cyclic groups $\mathbb{Z}/p\mathbb{Z}^\times$ and $\mathrm{GF}(2^d)^\times$.