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

Elliptic Curves.

(1) What is the Weierstrass form of a cubic equation?
(2) What alternative form is required in characteristic two?
(3) What is the group law (for either form)?
(4) What are the formulas for adding and doubling points on an elliptic curve (Weierstrass form)?
(5) What is Hasse's estimate for elliptic curves mod p?
(6) When is an elliptic curve mod p degenerate?
(7) When is an elliptic curve (in Weierstrass form) degenerate?
(8) What are the three types of degenerate real elliptic curves?
(9) Describe the group law on a cuspidal curve.
(10) Explain Lenstra's elliptic curve factoring method.
(11) Formulate Diffie-Hellman on an elliptic curve mod p.
(12) Explain why baby-step, giant-step works fine on $E(p)$, but index calculus doesn't.

Related stuff.

(1) Explain how to find fields with 2^d elements.
(2) Be prepared to do arithmetic in such fields.
(3) Add and double points on elliptic curves over such fields.
(4) Contrast the groups $(\mathbb{Z}/p\mathbb{Z})^\times$, $GF(2^d)^\times$ and $E(p)$.

A Couple of Proofs.

(1) Prove that an elliptic curve of the form $y^2 = x^3 + c$ satisfies $|E(p)| = p + 1$ when p does not divide c and $p \equiv 2 \pmod 3$.
(2) Prove that an elliptic curve of the form $y^2 = x^3 + bx$ satisfies $|E(p)| = p + 1$ when p does not divide b and $p \equiv 3 \pmod 4$.