MATH 75: MATHEMATICAL CRYPTOGRAPHY
HOMEWORK #8

Problems

Problem 1.

(a) Let $p = 101$. Compute $\log_2 11$ (using complete enumeration by hand).

(b) Let $p = 27781703927$ and $g = 5$. Suppose Alice and Bob engage in a Diffie-Hellman key exhange; Alice chooses the secret key $a = 1002883876$ and Bob chooses $b = 21790753397$. Describe the key exchange: what do Alice and Bob exchange, and what is their common (secret) key? *[You may use a computer!]*

Problem 2. Let $p = 1021$. Compute $\log_{10} 228$ using the baby step-giant step method.

Problem 3. In a modified Diffie-Hellman key exchange protocol, Alice and Bob choose a large prime p which they make public, but when they choose a primitive root g for p they decide for safety to keep it secret. Alice sends $x \equiv g^a \pmod{p}$ to Bob and Bob sends $y \equiv g^b \pmod{p}$ to Alice. Suppose Eve bribes Bob to tell her the values of b and y. Suppose that $\gcd(b, p-1) = 1$. Show how Eve can determine g from the knowledge of p, y and b.

Problem 4. Suppose the ElGamal system is used with $p = 71$, $g \equiv 7 \pmod{p}$, public key $g^b \equiv 3 \pmod{p}$ and random integer $a = 2$. What is the ciphertext for the message $x \equiv 30 \pmod{p}$?

Problem 5. Let E be the elliptic curve given by the equation $y^2 = x^3 + x^2 + 1$ over $\mathbb{F}_3$.

(a) Determine all points of $E(\mathbb{F}_3)$.

(b) Make an addition table for $E(\mathbb{F}_3)$.

Date: Due Wednesday, 25 May 2016.