MATH 295A/395A: CRYPTOGRAPHY
HOMEWORK #11

Problems for all

Problem 1.

(a) Let $p = 101$. Compute $\log_2 11$ (using complete enumeration).
(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 choose 21790753397. Describe the key exchange: what do Alice and Bob exchange, and what is their common (secret) key?

Problem 2.

(a) Let g be a primitive root modulo the prime p. Prove that

$$\log_g(h_1 h_2) \equiv \log_g h_1 + \log_g h_2 \pmod{p-1}$$

and

$$\log_g(h^n) \equiv n \log_g h \pmod{p-1}.$$

(b) Given $3^6 \equiv 44 \pmod{137}$ and $3^{10} \equiv 2 \pmod{137}$, compute $\log_3 11$.

Problem 3. Let $p = 1021$. Compute $\log_{10} 228$ using the baby step-giant step method.

Problem 4. In the Diffie-Hellman key exchange protocol, Alice and Bob choose a large prime p which they make public and choose a primitive root g for p which they keep secret. Alice sends $x = g^a \pmod{p}$ to Bob and Bob sends $y = g^b \pmod{p}$ to Alice. Suppose Eve bribes Bob to tell her the values of b and y, but Eve cannot find out g. Suppose that $\gcd(b, p-1) = 1$. Show how Eve can determine g from the knowledge of p, y and b.

Problem 5. Suppose the ElGamal system is used with $p = 71$, $g = 7$, public key $g^b = 3$ and random integer $a = 2$. What is the ciphertext for the message $x = 30$?

Additional problems for 395A

Problem 6. Let $G = \langle g \rangle$ be a cyclic group generated by the element $g \in G$. For an element $h \in G$, define $\log_g h$ to be the smallest positive integer i such that $g^i = h$.

(a) Let $\sigma = (1\ 2\ 3)(4\ 5)(6\ 7\ 8\ 9\ 10)$ and $\tau = (1\ 3\ 2)(4\ 5)(6\ 9\ 7\ 10\ 8)$. Show that $\tau \in \langle \sigma \rangle$ and compute $\log_\sigma \tau$.
(b) Let $k = \mathbb{F}_5[X]/(X^2 + X + 1)$ and $G = k^*$. Show that $\langle X - 1 \rangle = k^*$ and compute $\log_{X-1}(3(X+1))$.
(c) Let $G = \mathbb{Z}/101\mathbb{Z}$. Compute $\log_5 13$. *[Hint: This is not $G = (\mathbb{Z}/p\mathbb{Z})^*$.]*
(d) If $\#G = m$, show that the map

$$G \to \mathbb{Z}/m\mathbb{Z}$$
$$h \mapsto \log_g h$$

is an (well-defined) isomorphism of groups.

Date: Due Wednesday, 19 November 2008.

Problem 7. Let G be a group with $\#G = n$ and let $g \in G$.

(a) Show that if $hg \neq gh$ for some $h \in H$ then $\log_g h$ is not defined.

(b) Show that $G = \langle g \rangle$ if and only if $g^{n/\ell} \neq 1$ for every prime $\ell \mid n$.

(c) Conclude that $g \in (\mathbb{Z}/p\mathbb{Z})^*$ is a primitive root if and only if $g^{(p-1)/\ell} \not\equiv 1 \pmod{p}$ for every prime $\ell \mid (p-1)$, and use this to show that 2 is *not* a primitive root modulo $p = 65537$.

(d) Let p be a prime number for which $2^p - 1$ is prime ($q = 2^p - 1$ is called a *Mersenne prime*), and let $f \in \mathbb{F}_2[X]$ be irreducible of degree p. Let $\mathbb{F}_{2^p}$ be the field $\mathbb{F}_2[X]/(f)$. Prove that $\langle X \rangle = \mathbb{F}_{2^p}^*$.