PMAT 4282 – Cryptography Assignment #4
Winter 2012

Instructions

- Answer each question completely; justify your answers.

A *group* $(\mathcal{G}, \cdot)$ consists of a set $\mathcal{G}$ along with a binary operation $\cdot$, such that:

- $\mathcal{G}$ is closed under $\cdot$
- $\cdot$ is associative (i.e., $a \cdot (b \cdot c) = (a \cdot b) \cdot c$)
- there exists an identity with respect to $\cdot$
  (i.e., there exists an element $e \in \mathcal{G}$ such that $a \cdot e = e \cdot a = a$ for all $a \in \mathcal{G}$)
- each element has an inverse
  (i.e., for each $a \in \mathcal{G}$ there exists an element $b \in \mathcal{G}$ such that $a \cdot b = b \cdot a = e$)

Note that we often refer to the group as $\mathcal{G}$ rather than $(\mathcal{G}, \cdot)$. Notice also that $\cdot$ need not be commutative; a group in which $\cdot$ is commutative is called an *Abelian* group.

The notation a^n will be used to denote $\underbrace{a \cdot a \cdot a \cdots a}_{n\ a\text{'s}}$. The *order* of an element $a \in \mathcal{G}$ is the smallest positive integer t such that $a^t = e$. If a has order $|\mathcal{G}|$ then a is a *generator* of $\mathcal{G}$.

1. Find all generators of each of the following groups:
   (a) $\mathbb{Z}_{17}^*$
   (b) $\mathbb{Z}_{25}^*$

2. Prove the following statement:
   If the order of $a \in \mathbb{Z}_n^*$ is t and $a^s \equiv 1 \pmod{n}$, then t divides s.

3. (a) Suppose that α is a generator of $\mathbb{Z}_n^*$. Prove that α^k is a generator of $\mathbb{Z}_n^*$ if and only if $\text{GCD}(k, \phi(n)) = 1$, where ϕ is Euler's totient function.
   (b) Provided that $\mathbb{Z}_n^*$ has at least one generator, then how many generators does it have?
   (c) When p is prime, $\mathbb{Z}_p^*$ is known to have a generator. How many generators are there in:
      i. $\mathbb{Z}_{31}^*$
      ii. $\mathbb{Z}_{181}^*$
      iii. $\mathbb{Z}_{257}^*$
      iv. $\mathbb{Z}_{2^t+1}^*$, where $(2^t + 1)$ is prime
      v. $\mathbb{Z}_{2t+1}^*$, where t and $(2t + 1)$ are prime

4. Solve for x by using Shanks' Algorithm:
   (a) $13^x \equiv 12 \pmod{197}$
   (b) $14^x \equiv 519 \pmod{557}$
   (c) $7^x \equiv 922 \pmod{1433}$

(over)

5. Solve for x by using the Index Calculus Method:

   (a) $55^x \equiv 444 \pmod{569}$

   (b) $7^x \equiv 92 \pmod{1433}$

6. Show that the Diffie-Hellman Problem (DHP) and the El Gamal Problem (ELGAMAL) are computationally equivalent.

7. Suppose that Alice has published the key $(1237, 34, 383)$ for use in the El Gamal public-key cryptosystem.

   (a) You wish to send the message $m = 14$ to Alice. What do you actually transmit?

   (b) You have monitored the transmission $(94, 225)$ to Alice.

      i. Use the Index Calculus Method for solving the Discrete Log Problem to find Alice's secret key a.

      ii. What was the original message?