SAMS 2023 WEEK 5: DIFFIE-HELLMAN KEY EXCHANGE

Please keep this packet and bring it with you to class every day this week to work on. This packet will not be collected, but I encourage you to use our google group (linked on our course webpage) to post questions and solutions.

Definitions and Theorems

The following definitions and theorems will be introduced during lecture, and will be needed for this week's problem set. Note that a *definition* is some explanation of the meaning of a word. A *theorem* is some statement which has been demonstrated to be true.

Definition 1. Let p be prime and g, h be integers in between 1 and $p-1$. Then, the DISCRETE LOGARITHM of h with base g modulo p is any integer value x satisfying

$$g^x \equiv h (\mathrm{mod}\, p).$$

In this case, we write $x = \log_g(h)$.

Theorem 1 (Fermat's Little Theorem)**.** Suppose that p is prime. Then, for any integer a we have

$$a^p \equiv a (\mathrm{mod}\, p).$$

Diffie-Hellman Key Exchange.

STEP 1: PUBLIC PARAMETER CREATION

Bob and/or Alice decide on a large prime p and primitive root g. The parameters (g, p) are shared publicly.

STEP 2: PRIVATE COMPUTATIONS

Alice chooses and computes

$$A \equiv g^a (\mathrm{mod}\, p).$$

Bob then chooses a secret integer b with $1 \leq b \leq p-2$ and computes

$$B \equiv g^b (\mathrm{mod}\, p).$$

STEP 3: PUBLIC EXCHANGE

Alice sends A to Bob, and Bob sends B to Alice.

STEP 4: KEY CREATION

Alice computes $B^a (\mathrm{mod}\, p)$ and Bob computes $A^b (\mathrm{mod}\, p)$. Observe that Bob and Alice now share the secret key $k \equiv g^{ab} (\mathrm{mod}\, p)$.

Problem Set

Complete as many problems from the list below as you have time and interest for. Feel free to skip around as you'd like, and to work on your own or with your group as you prefer. If you generally prefer to work on your own, I encourage you to discuss at least two problems together with your group. I suggest you keep a notebook or binder for this course to store your solutions. There is also scratch paper available at the front of the class for you to use at any time.

P1. Verify Fermat's Little Theorem holds for the following integers a and primes p.

a) $a = 5$, $p = 23$

b) $a = 45, p = 37$

c) $a = 4, p = 61$

d) $a = 46, p = 23$

P2. Do you think that Fermat's Little Theorem holds when p is not prime? That is, if n is *any integer* do we always get $a^n \equiv a (\mathrm{mod}\, n)$?

P3. Compute the following discrete logs. I suggest using Wolfram Alpha to help in some of your computations.

a) $\log_3(4)$ modulo 7

b) $\log_7(2)$ modulo 11

c) $\log_2(13)$ modulo 23

d) $\log_{12}(22)$ modulo 47

e) $\log_{627}(608)$ modulo 941

P4. Find the shared secret key Alice and Bob created from the following public information by solving a discrete log problem.

a) $p = 11, g = 7, A = 2$ and $B = 10$

b) $p = 23, g = 2, A = 13$ and $B = 6$

P5. In pairs of two, create shared secret keys using the prime $p = 941$ and primitive root $g = 627$.

a) Did you run into any difficulties in your implementation?

b) See if your other groupmates can find your shared private key using only your public information by solving a discrete log problem.

c) Discuss the differences and similarities between Diffie-Hellman and RSA. Was one easier to implement than the other? Does one seem more useful than the other?

Additional Problems

The problem set below requires methods and background we won't necessarily cover in our course. If you've seen proof methods before, or want some extra challenge, feel free to play with these!a secret integer a with $1 \leq a \leq p - 2$

A1. Prove Fermat's Little Theorem. *(Hint: one method is to use mathematical induction and the binomial theorem).*

A2. Fermat's little theorem says that *if* p is prime, then $a^p \equiv a (\mathrm{mod}\, p)$. Use the converse of this theorem to show that the following numbers are composite.

a) $n = 341$

b) $n = 1105$

c) $n = 561$ *(you should run into trouble here...)*

A3. Show that

$$\log_g(h_1 h_2) = \log_g(h_1) + \log_g(h_2)$$

modulo p.

A4. Show that for any integers n and h we have

$$\log_g(h^n) = n \log_g(h)$$

modulo p.

Debrief Questions.

We'll spend the last part of class on Wednesday debriefing on our time together. I would love to hear from you all, so please think about the following questions, and consider sharing some of your thoughts with the group during our discussion.

1. Has your time in this course, or more generally in this program, changed your perspective of mathematics?
2. Reflecting on your time here at CMU, how are you thinking about your upcoming college careers? What was different about this program than what you experience in highschool?
3. How have you struggled in this course? What do you think could have been helpful, both from your community of classmates and from me as a teacher, for you to succeed in a course like this?
4. How can you show up for yourself and your classmates in college to help you meet the needs discussed in the previous question?
5. Ask me anything! I am happy to answer any questions about my life and path in academia, and am happy to answer at least most of the personal question you might have.
6. What can I do to further support you after you leave CMU?