CRYPTOGRAPHY HANDOUT 17

DISCRETE LOG

1. First Explorations and Definition

Suppose p is a prime number. Let α and β be nonzero integers. Consider the congruence $\beta \equiv \alpha^x \mod p$. Solving for x is the **discrete log problem**.

Notation: We write $x = L_\alpha(\beta)$ for the **discrete log of β with respect to α** and assume all computations are $\mod p$.

Example. $p = 11$, $\alpha = 2$, $\beta = 9$. Since $2^6 \equiv 9 \mod 11$, then $L_2(9) = 6$.

1. Find an appropriate value of x given the following, and write it as $x = L_\alpha(\beta)$.
   a. $p = 11$, $\alpha = 3$, $\beta = 5$

   b. $p = 7$, $\alpha = 4$, $\beta = 5$

   c. $p = 13$, $\alpha = -7$, $\beta = 3$

2. In the discrete log problem, is x unique? Justify.

2. Computing Discrete Logs

You should have concluded that we can find multiple values of x, so we tend to choose the smallest nonnegative value. Oftentimes, α is a primitive root $\mod p$.

Recall the following:

- The smallest natural number k such that $\alpha^k \equiv 1 \mod p$ is the **order**.
- If the order is $p-1$, then α is a **primitive root** $\mod p$**.**
- Every prime p has $\varphi(p-1)$ primitive roots.

Suppose $p = 7$.

1. How many primitive roots are there?

2. Primitive Root Case:

   a. Verify that $\alpha = 3$ is a primitive root.

   b. Compute $\beta \equiv \alpha^x \bmod p$ for all values $x \in \{1, 2, 3, 4, 5, 6\}$.

   c. List any observations about the values of β.

3. Not a Primitive Root Case:

   a. Verify that $\alpha = 2$ is not a primitive root.

   b. Compute $\beta \equiv \alpha^x \bmod p$ for all values $x \in \{1, 2, 3, 4, 5, 6\}$.

   c. List any observations about the values of β.

It turns out that when α is a primitive root $\mod p$, then every power β is a power of $\alpha \bmod p$. If α is not a primitive root, then the discrete log problem will not be defined for some values of β.

Property: The discrete log is like the usual log function. If α is a primitive root $\mod p$, then we have

$$L_\alpha(\beta_1\beta_2) \equiv L_\alpha(\beta_1) + L_\alpha(\beta_2) \bmod (p-1).$$

Convince yourself that the above is true using an example.

3. One-Way Functions

Example. Let $p = 41, \alpha = 7, \beta = 12$. We want to solve $7^x \equiv 12 \bmod 41$.

1. Discuss strategies that you would use to solve this, and find a value of x.

2. What are the challenges of such a problem? Are there any situations in which your strategies would be unreasonable to use?

In general, the discrete log is difficult to compute. It is an example of a **one-way function**, which means $f(x)$ is easy to find, but given y, it is much too computationally slow to find x such that $f(x) = y$. These functions are useful for cryptography.