HENSEL LIFTING AND THE DISCRETE LOGARITHM PROBLEM

ARCHISHMAN SRAVANKUMAR

1. The Discrete Logarithm Problem

The discrete logarithm problem is used in many areas of cryptography like ElGamal encryption, Diffie-Hellman Key Exchange, and the Digital Signature Problem. Although the problem can be defined for any group, here we will only look at the specific case where the group is $\mathbb{F}_p$.

Definition 1.1. The discrete logarithm problem. Given a prime p and $g, h \in \mathbb{F}_p$ find an x such that

$$g^x = h \mod p.$$

2. Hensel Lifting and the Discrete Logarithm Problem

For a full discussion of this problem, see [1]. We define a new function called the **Hensel-Dlog** function and show that computing it is as hard as the Discrete Logarithm problem. The **Hensel-Dlog** is defined as

$$\textbf{Hensel-Dlog}[p, g, l](g^x \mod p) = g^x \mod p^l.$$

Theorem 2.1. *Let ω be a k-bit random prime and p, such that $\omega | p-1$, be a prime whose size is polynomially related with k. Given g of order ω in $\mathbb{Z}_p^*$, p and ω, $Hensel - Dlog[p, g, l]$ is hard if and only if the discrete logarithm in the subgroup spanned by g in $\mathbb{Z}_p*$ is a one way function, where l is defined as the unique positive integer such that $g^\omega \not\equiv 1 \mod p^l$ and $g^\omega \equiv 1 \mod p^{l-1}$*

Sketch of Proof. First we see that if the discrete logarithm problem is not hard, then, trivially, neither is computing **Hensel-Dlog**. The proof of the "other way" still remains.
We assume the existence of an Oracle which efficiently calculates **Hensel-Dlog** with probability ϵ. First we pick a random a sampled uniformly from $\mathbb{Z}_w^*$. We call the oracle twice to evaluate **Hensel-Dlog**$[p, g, l](h \mod p)$ and **Hensel-Dlog**$[p, g, l](h^a \mod p)$. From this we get $g^x \mod p^l$ and $g^\mu \mod p^l$ where $\mu = ax \mod \omega$. Since $ax = \mu + r\omega$, we get

$$g^{ax} \equiv g^\mu g^{r\omega} \mod p^l.$$

Using our oracle calls, it is easy to compute $g^{r\omega} \mod p^l$. Because of the constraints on l, r can be computed as well. This gives the bounds x as

$$\frac{r\omega}{a} \leq x < \frac{(r+1)\omega}{a}.$$

It can be shown that with non trivial probability, this interval is small enough to search exhaustively to find x. ∎

Date: June 11, 2018.

References

[1] Dario Catalano, Phong Q. Nguyen, and Jacques Stern. The hardness of hensel lifting: The case of rsa and discrete logarithm. pages 299–310, 2002.

Euler Circle, Palo Alto, CA 94306
E-mail address: archishman.sravankumar@gmail.com