

Assignment #4

CAS 705

Computability and Complexity

Jason Jaskolka

0546444

Dr. Michael Soltys

November 24, 2009

Question 1

Let G be a group, and suppose that we have an algorithm to solve the discrete logarithm problem in G for any element whose order is a power of a prime. To be concrete, if $g \in G$ has order q^e , then we can solve $g^x = h$ in $O(S_{q^e})$ steps.

Now let $g \in G$ be an element of order n , and suppose that n factors into a product of prime powers as follows $n = q_1^{e_1} \cdots q_t^{e_t}$. Then show that the discrete logarithm problem $g^x = h$ can be solved in

$$O\left(\sum_{i=1}^t S_{q_i^{e_i}} + \log n\right)$$

steps, using the following procedure:

(a) For each $i \in \{1, 2, \dots, t\}$ let $g_i = g^{n/q_i^{e_i}}$ and $h_i = h^{n/q_i^{e_i}}$. Notice that g_i has prime power order $q_i^{e_i}$, so use the given algorithm to solve the discrete logarithm problem $g_i^y = h_i$; let $y = y_i$ be a solution to this.

(b) Use the Chinese remainder theorem to solve

$$\begin{aligned} x &\equiv y_1 \pmod{q_1^{e_1}} \\ x &\equiv y_2 \pmod{q_2^{e_2}} \\ &\vdots \\ x &\equiv y_t \pmod{q_t^{e_t}} \end{aligned}$$

In order to show that the discrete logarithm problem $g^x = h$ can be solved in $O\left(\sum_{i=1}^t S_{q_i^{e_i}} + \log n\right)$ we must show that the above algorithm, steps a) and b), solves the discrete logarithm problem and that it can be done in $O\left(\sum_{i=1}^t S_{q_i^{e_i}} + \log n\right)$ steps.

We will begin by showing that the above algorithm, steps a) and b), solves the discrete logarithm problem, in particular provides a solution for $g^x = h$. Let x be the solution found by solving the congruences in step b) by the Chinese Remainder Theorem. By the Remainder Theorem, we can write for each i that $x = q_i^{e_i} a_i + y_i$ for some a_i . Using this we are able to compute the following by step a)

$$\begin{aligned} &(g^x)^{n/q_i^{e_i}} \\ &= \langle \text{Definition of } x \rangle \\ &\quad (g^{q_i^{e_i} a_i + y_i})^{n/q_i^{e_i}} \\ &= \langle \text{Exponent Laws} \rangle \\ &\quad g^{na_i} \cdot (g^{n/q_i^{e_i}})^{y_i} \\ &= \langle \text{Identity Element } g^n \rangle \\ &\quad (g^{n/q_i^{e_i}})^{y_i} \\ &= \langle \text{Definition of } g_i \rangle \\ &\quad g_i^{y_i} \\ &= \langle g_i^y = h_i \text{ from step a)} \rangle \\ &\quad h_i \\ &= \langle \text{Definition of } h_i \rangle \\ &\quad h^{n/q_i^{e_i}} \end{aligned}$$

We can now rewrite this in terms of discrete logarithms of base g as

$$n/q_i^{e_i} \cdot \log_g h \equiv_n n/q_i^{e_i} \cdot x \quad (1)$$

This leads us to consider the numbers $n/q_1^{e_1}, n/q_2^{e_2}, \dots, n/q_t^{e_t}$ for which we can see that their greatest common divisor is 1. By applying the Extended Euclidean Algorithm we have integers u_i such that

$$\sum_{i=1}^n n/q_i^{e_i} \cdot u_i = 1 \quad (2)$$

Now, we are able to rewrite Equation (1) and get our result as follows

$$\begin{aligned} & n/q_i^{e_i} \cdot \log_g h \equiv_n n/q_i^{e_i} \cdot x \\ \Leftrightarrow & \langle \text{Sum } n/q_i^{e_i} \text{ over } i = 1, 2, \dots, t \rangle \\ & \sum_{i=1}^n n/q_i^{e_i} \cdot \log_g h \equiv_n \sum_{i=1}^n n/q_i^{e_i} \cdot x \\ \Leftrightarrow & \langle \text{Multiply both sides by } u_i \rangle \\ & \sum_{i=1}^n n/q_i^{e_i} \cdot u_i \cdot \log_g h \equiv_n \sum_{i=1}^n n/q_i^{e_i} \cdot u_i \cdot x \\ \Leftrightarrow & \langle \text{Equation (2)} \rangle \\ & \log_g h \equiv_n x \\ \Leftrightarrow & \langle \text{Definition of Discrete Logarithm} \rangle \\ & g^x = h \end{aligned}$$

Therefore, we have shown that the algorithm, steps a) and b), compute an x that satisfies $g^x = h$.

Now that we know that the algorithm will correctly compute an x which satisfies $g^x = h$, it remains to show that it can be done in $O\left(\sum_{i=1}^t S_{q_i^{e_i}} + \log n\right)$ steps. Since g has order q^e , we can solve $g^x = h$ in $O(S_{q^e})$ steps. So, we can see that in step a), we need $O\left(\sum_{i=1}^t S_{q_i^{e_i}}\right)$ many steps since we need to sum over the prime power order $q_i^{e_i}$ to solve the discrete logarithm problem $g_i^y = h_i$ for each i . For step b), we can see by the use of the Chinese Remainder Theorem to solve the system of equations that we can do it in $O(\log n)$ steps. Thus, the discrete logarithm problem $g^x = h$ can be solved in $O\left(\sum_{i=1}^t S_{q_i^{e_i}} + \log n\right)$ steps.

Question 2

Let G be a group and suppose that q is prime, and that we know an algorithm that takes S_q steps to solve the discrete logarithm problem $g^x = h$ in G whenever g has order q . Now let $g \in G$ be an element of order q^e with $e \geq 1$. Then show that we can solve the discrete logarithm problem $g^x = h$ in $O(eS_q)$ steps.

We need to show that we can solve the discrete logarithm problem $g^x = h$ in $O(eS_q)$ steps. We begin by coming up with a definition of x as follows

$$x = \sum_{i=0}^{e-1} x_i q^i \quad \text{such that } 0 \leq x_i < q \quad (3)$$

Using this definition we can inductively determine each x_i by first taking note that the element $g^{q^{e-1}}$ is of order q and can be used to compute the following

$$\begin{aligned}
& h^{q^{e-1}} \\
= & \langle \text{Raising to } q^{e-1} \rangle \\
& (g^x)^{q^{e-1}} \\
= & \langle \text{Equation (3) and expansion} \rangle \\
& (g^{x_0+x_1q+x_2q^2+\dots+x_{e-1}q^{e-1}})^{q^{e-1}} \\
= & \langle \text{Exponent Laws} \rangle \\
& g^{x_0q^{e-1}} \cdot (g^{q^e})^{x_1+x_2q+\dots+x_{e-1}q^{e-2}} \\
= & \langle \text{Identity Element } g^{q^e} \rangle \\
& (g^{q^{e-1}})^{x_0}
\end{aligned}$$

So, since $g^{q^{e-1}}$ is of order q in G we have that $(g^{q^{e-1}})^{x_0} = h^{q^{e-1}}$ is a DLP with a base that is an element of order q . By the assumption, we are able to compute this problem in S_q steps and thus we would know x_0 . We can now do a similar computation by taking note that the element $g^{q^{e-2}}$ is of order q , so

$$\begin{aligned}
& h^{q^{e-2}} \\
= & \langle \text{Raising to } q^{e-2} \rangle \\
& (g^x)^{q^{e-2}} \\
= & \langle \text{Equation (3) and expansion} \rangle \\
& (g^{x_0+x_1q+x_2q^2+\dots+x_{e-1}q^{e-1}})^{q^{e-2}} \\
= & \langle \text{Exponent Laws} \rangle \\
& g^{x_0q^{e-2}} \cdot g^{x_1q^{e-1}} \cdot (g^{q^e})^{x_2+x_3q+\dots+x_{e-1}q^{e-3}} \\
= & \langle \text{Identity Element } g^{q^e} \rangle \\
& g^{x_0q^{e-2}} \cdot g^{x_1q^{e-1}}
\end{aligned}$$

Now, since we have already computed x_0 and $g^{q^{e-1}}$ is of order q , we need solve $(g^{q^{e-1}})^{x_1} = (h \cdot (g^{x_0})^{-1})^{q^{e-2}}$ to find x_1 . Again, by the assumption, we are able to compute this problem in S_q steps and thus we would know x_1 . So we have now taken $O(2S_q)$ steps to compute both x_0 and x_1 .

We can continue in the same fashion to compute the rest of the x_i and after we have computed x_0, x_1, \dots, x_{i-1} (the induction hypothesis), we can compute x_i by solving the the DLP $(g^{q^{e-1}})^{x_i} = (h \cdot (g^{x_0+x_1q+x_2q^2+\dots+x_{i-1}q^{i-1}})^{-1})^{q^{e-i-1}}$.

So, as we have seen, we need to solve a DLP in order to find each x_i and since each DLP has a base that is an element of order q , each of them can be found in S_q steps. So after $O(eS_q)$ steps (the e comes from the fact that we need to perform the algorithm e times, for the number of x_i such that $0 \leq i \leq e-1$), we can find x as defined by Equation (3) which satisfies $g^x = h$.

Question 3

Conclude that the discrete logarithm problem in a group G is not secure if the order of the group is a product of powers of small primes.

If the order of the group is a product of powers of small primes, then the discrete logarithm problem in a group G is not secure. Restated, this says that $g^x = h$ is easy to solve if the order of $g \in G$ is a product of powers of small primes. As seen above by Question 2, we are able to reduce the DLP for elements of prime power order to the DLP for elements of prime order. Thus, for elements of order q^e , we can reduce the number of steps from S_{q^e} to $O(eS_q)$. Thus, since we can reduce the number of steps in this way, we can see that the $g^x = h$ becomes much easier to solve and thus the DLP in a group G is not secure.

References

1. Menezes, A., Van Oorschot P., and Vanstone, S. *Handbook of Applied Cryptography*. pp. 107-109. CRC Press. 1997.
2. Mollin, R. *An Introduction to Cryptography*. pp. 344-349. Chapman & Hall/CRC. 2006.