Diffie-Hellman Key Exchange and the Discrete Log Problem

R. C. Daileda

Trinity University

Number Theory

Introduction

Suppose two individuals, Eliza (E) and Zoey (Z), want to communicate using a classical (non-public-key) cryptosystem, but they must share their key via insecure (unencrypted) means.

In the presence of eavesdroppers, is there any way E and Z can securely agree upon a secret key (without using encryption)?

The *Diffie-Hellman Key Exchange* provides one way to accomplish this.

Its security is based on the difficulty in solving the *discrete log problem*.

The Set-up

E and Z do the following:

- (publicly) agree on a prime p and a generator g of $(\mathbb{Z}/p\mathbb{Z})^\times$;
- E secretly chooses an integer $1 \leq m \leq p-1$; she (publicly) transmits g^m to Z;
- Z secretly chooses an integer $1 \leq n \leq p-1$; she (publicly) transmits g^n to E;
- compute $g^{mn} = (g^n)^m = (g^m)^n$ and agree to use it as their secret key.

Example

Suppose E and Z have agreed on $p = 5754853343$ and $g = 5 + p\mathbb{Z}$.

E has chosen $m = 581869302$ and used repeated squaring to compute

$$g^m = 5^{581869302} + p\mathbb{Z} = 4434769206 + p\mathbb{Z},$$

which she sends to Z.

Z has chosen $n = 3586334585$ and used repeated squaring to compute

$$g^n = 5^{3586334585} + p\mathbb{Z} = 1689959166 + p\mathbb{Z},$$

which she sends to E.

Because she knows m, E can use Z's message to compute g^{mn}:

$$\begin{aligned} g^{mn} &= (g^n)^m \\ &= (1689959166 + p\mathbb{Z})^m \\ &= 1689959166^{581869302} + p\mathbb{Z} \\ &= 2372777492 + p\mathbb{Z}. \end{aligned}$$

Likewise, Z can compute g^{mn} from n and E's message:

$$\begin{aligned} g^{mn} &= (g^m)^n \\ &= (4434769206 + p\mathbb{Z})^n \\ &= 4434769206^{3586334585} + p\mathbb{Z} \\ &= 2372777492 + p\mathbb{Z}. \end{aligned}$$

So their "shared secret" is $2372777492 + p\mathbb{Z}$.

Security

The quantities p, g, g^m, g^n are public knowledge.

To determine the secret key g^{mn} an eavesdropper must determine either m or n.

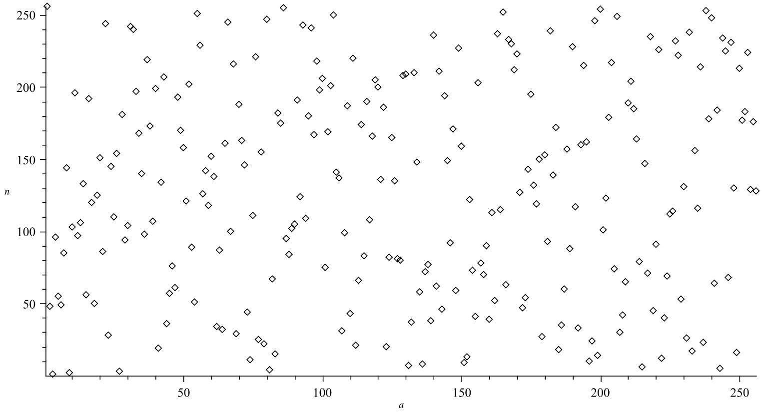
That is, the eavesdropper must solve

The Discrete Log Problem. Given a cyclic group $G = \langle g \rangle$ and $a \in G$, find an $n \in \mathbb{Z}$ so that $g^n = a$.

For $G = (\mathbb{Z}/pZ)^\times$ this is a "very difficult" problem to solve, as the following graph illustrates.

Log plot

Plot of the discrete logarithm $n = \log_g a$ (i.e. $g^n = a$) for $G = (\mathbb{Z}/p\mathbb{Z})^\times$, $p = 257$ and $g = 3 + p\mathbb{Z}$.



Remarks

Because of its random behavior, $\log_g a$ is "hard" to compute.

A naïve way to find $\log_g a$ is to simply compute

$$g, g^2, g^3, g^4, \ldots$$

until one lands on a.

Based on the "random" behavior we have seen, this is extremely inefficient.

However, there is no known algorithm that is more efficient than this approach.

In the "toy" example above ($p = 5754853343$, $g = 5 + p\mathbb{Z}$, $g^m = 4434769206 + p\mathbb{Z}$) this process took nearly 17 minutes on a 2.53 GHz processor to compute m.