Choosing Secure Primes and Generators for Diffie-Hellman Key-Exchange

Jack Scacco

October 27, 2019

Introduction

Before using Diffie-Hellman key-exchange, a public prime value p and generator g must be shared by both parties. However, a poor choice of p and g can render the scheme vulnerable to brute-force attacks. Consider, for example, $p = 19$ and $g = 3$. If Alice chooses $a = 6$ and computes $g^a \mod p = 3^6 \mod 19 = 7$ as her shared value, an attacker could intercept 7 and realize that 7 only generates three values $\mod 19$ when raised to some $i < 19$. Thus, there would only be three possible secret keys that Alice and Bob could share! This is obviously insecure, and highlights the importance of choosing p and g.

Subgroups

We will define a **subgroup** as the set of all values $g^i \mod p$, $i < p$. Consider the example above. The set generated by Alice's shared value was small, so the scheme was insecure. (For our purposes, a small subgroup is one whose size is either constant or significantly smaller than the average subgroup size.) In other words, Alice's shared value had a small subgroup under their chosen p. So, secure choices of p and g guarantee that no g will have a small subgroup $\mod p$.

Safe Primes

Due to the cyclic nature of modulo arithmetic, all subgroups $\mod p$ have a size that is a factor of $p - 1$ (we will never have a subgroup of size 0) [Kar17]. Since all primes (except for 2, which would never be used for Diffie-Hellman) are odd, $p - 1$ will always be even. Thus, if $(p - 1)/2$ is also prime, then every subgroup will either be of size 1, 2, $(p - 1)/2$, or $p - 1$. Generators $g = 0, 1, (-1 \mod p)$ have subgroups of size $2, 1$, and 2. Since we want large subgroups, we define a prime p as a **safe prime** if $(p - 1)/2$ is also prime.

Computation in Practice

To select a secure p and g in practice, first choose an arbitrary safe prime p. There are several academic and government documents which provide large safe primes p [KK03]. It is also necessary that p if sufficiently long to render brute-force attacks useless, and the current accepted standard is 2048 bits. Then, choose any $g \in \{2, 3, \dots, p - 2\}$. This will ensure that the chosen generators does not have small subgroups.

References

[KK03] T. Kivinen and M. Kojo. *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*. May 2003. URL: `https://tools.ietf.org/html/rfc3526`.

[Kar17] Hubert Kario. *Safe primes in Diffie-Hellman*. May 2017. URL: `https://securitypitfalls.wordpress.com/2017/05/05/safe-primes-in-diffie-hellman/`.