Diffie-Hellman Key Exchange

Motivation for Key Exchange Algorithm

The fastest encryption schemes are symmetric encryption schemes. In order to use these, the two communicators (Alice & Bob) would have to meet in a secure location. BUT, this sort of defeats the purpose, because their whole goal is to communicate when securely when they aren't in the same place. A modern day example of why it would be useful to exchange a key without meeting deals with an online purchase. You are making the purchase online so that you DON'T have to go to the store to meet with the vendor. So, you don't really want to go to the store to just exchange a secret key either. You want to be able to do that from the comfort of your own home.

Thus, that is the underlying problem: how do two users exchange a secret key without a secure communication channel?

The first solution to this problem was the Diffie-Hellman Key Exchange. What's interesting about this algorithm is that neither user actually gets to choose the key. But, at the end of the algorithm, both users have calculated the same key, which is not easy for an eavesdropper to calculate.

The security of the Diffie-Hellman Key Exchange is based on the difficulty of the Discrete Logarithm Problem which we previously discussed. For clarity, a summary of the Discrete Log Problem is included below.

Discrete Log Problem

The (discrete) exponentiation problem is as follows: Given a base a, an exponent b and a modulus p, calculate c such that $a^b \equiv c \pmod{p}$ and $0 \leq c < p$.

It turns out that this problem is fairly easy and can be calculated "quickly" using fast-exponentiation.

The discrete log problem is the inverse problem:

Given a base a, a result c ($0 \leq c < p$) and a modulus p, calculate the exponent b such that

$a^b \equiv c \pmod{p}$.

It turns out that no one has found a quick way to solve this problem. To get an intuition as to why this is the case, try picking different values of a and p, and listing out each successive power of a mod p. What you will find is that there is no discernable pattern for the list of numbers created. Thus, given a number on the list, it's very difficult to predict where it appears on the list.

Here's a concrete example:

Given a = 2, b = 7 and p = 37, calculate c: $2^7 = 128$, and $128 \equiv 17 \pmod{37}$

Given a = 2, c = 17, and p = 37, calculate b: Try each value of b until you find one that works! (For large prime numbers, this is too slow.)

Diffie Hellman Key Exchange

Alice and Bob agree on two values: a large prime number p, and a generator g, $1 < g < p$. (It's better if g is an actual generator, meaning that when you raise it to the 1st, 2nd, 3rd, …, p-1 powers, you get all different answers. Technically, as long as the order of g is very large, then it should be okay to use.)

These values are known to everyone.

In secret, Alice picks a value a, with $1 < a < p$.
In secret, Bob picks a value b, with $1 < b < p$.

Alice calculates $g^a \pmod p$, call this f(a) and sends it to Bob.
Bob calculates $g^b \pmod p$, call this f(b) and sends it to Alice.

Note that f(a) and f(b) are also known by everyone.

In secret, Alice computes $f(b)^a \pmod p$ – this is the exchanged key.
In secret, Bob computes $f(a)^b \pmod p$ – this is again, the exchanged key.

Why does this work?

$f(b)^a \equiv (g^b)^a \equiv g^{ab} \pmod p$. Similarly,
$f(a)^b \equiv (g^a)^b \equiv g^{ab} \pmod p$.

Here's a concrete example:

Let p = 37 and g = 13.

Let Alice pick a = 10. Alice calculates $13^{10} \pmod{37}$ which is 4 and sends that to Bob.
Let Bob pick b = 7. Bob calculates $13^7 \pmod{27}$ which is 32 and sends that to Alice.
(Note: 6 and 7 are secret to Alice and Bob, respectively, but both 4 and 32 are known by all.)

Alice receives 32 and calculates $32^{10} \pmod{37}$ which is 30, the secret key.
Bob receives 4 and calculates $4^7 \pmod{37}$ which is 30, the same secret key.

Note that neither Alice nor Bob chose 30, but that they ended up with that secret key anyway. Furthermore, note that even with knowing p = 37, g = 13, f(a) = 4 and f(b) = 32, it is difficult to ascertain the secret key, 30 without doing a brute force check.

In particular, if the discrete log problem were easy, this scheme could be broken. Consider the following:
If an adversary saw that f(a) = 4, p = 37 and g = 13 and could solve the discrete log problem, then they could calculate that $13^{10} \equiv 4 \pmod{37}$. Once they had this value, 10, then they could take f(b) = 32 and then calculate $32^{10} \pmod{37}$ to arrive at 30.

Thus, the Diffie-Hellman Key Exchange is only as secure as the Discrete Log problem.