Demystifying Diffie-Hillman

The Diffie-Hillman protocol allows two actors to generate a secret key using only public communications. Imagine that Alice and Bob want to generate a key, but Eve is trying to listen to everything they say. The basic idea works like this:

1. Bob comes ups with two prime numbers $\boldsymbol{g}$ and $\boldsymbol{p}$ and tells Alice what they are. It's OK if Eve also hears what they are – in fact, it's OK if this communication is public.
2. Alice then picks a secret number (little $\boldsymbol{a}$) but doesn't tell anyone what it is. Instead, Alice computes $\boldsymbol{A = (g^a)\ mod\ p}$ and sends the result $\boldsymbol{A}$ back to Bob. If Eve hears this conversation, or if the whole world hears it, that's OK.
3. Bob does the same thing, which means that he picks a secret number little $\boldsymbol{b}$ and computes $\boldsymbol{B = \left(g^b\right)\ mod\ p}$. He sends the result $\boldsymbol{B}$ back to Alice. Eve can hear this conversation without gaining any useful information, just like the previous communications.
4. Now, Alice takes the number Bob sent her and computes $\boldsymbol{key = (B^a)\ mod\ p}$.
5. Bob does the same thing, using the result Alice sent him: $\boldsymbol{key = \left(A^b\right)\ mod\ p}$.

And because of some magic math, the numeric key Alice computes in step 4 is the same one that Bob gets in step 5. And in spite of the fact that they have communicated publicly to establish this key, Eve cannot use the information she has overheard to determine what that key is.

Why is that? Here is an end-game analysis:

Eve's point of view:

Here are the numbers Eve knows: $\boldsymbol{g}$, $\boldsymbol{p}$, $\boldsymbol{A}$, and $\boldsymbol{B}$. She does not know the secret numbers little $\boldsymbol{a}$ or little $\boldsymbol{b}$. She is not happy about this, as we will explain below.

Alice's point of view:

In order to calculate the key, Alice has computed first $\boldsymbol{A = (g^a)\ mod\ p}$. Eve can't compute this because Alice's little $\boldsymbol{a}$ is never sent in any communications. Once Bob sends $\boldsymbol{B}$ back to her, Alice computes the value of the key as $\boldsymbol{key = (B^a)\ mod\ p}$. Eve can't compute this because it also has little $\boldsymbol{a}$ in it, a value Eve does not know because it was never transmitted.

Bob's point of view:

In order to calculate the key, Bob first computes $\boldsymbol{B = \left(g^b\right)\ mod\ p}$. Eve can't compute this because Bob's little $\boldsymbol{b}$ is never sent in any communications. Once Alice sends $\boldsymbol{A}$ back to him, Bob computes the value of the key as $\boldsymbol{key = \left(A^b\right)\ mod\ p}$. Eve can't compute this because it also has little $\boldsymbol{a}$ in it, a value Eve does not know because it was never transmitted.

Optional: If you want to understand the math

Why do Alice and Bob get the same key value?

Let's start by rewriting what Alice and Bob calculated in their final steps.

Because $\boldsymbol{B = \left(g^b\right) \bmod p}$, when Alice computes $\boldsymbol{\left(B^a\right) \bmod p}$, she is actually computing this:

$$\boldsymbol{\left(\left(\left(g^b\right) \bmod p\right)^a\right) \bmod p = g^{b*a} \bmod p}$$

All I did was substitute for $\boldsymbol{B}$ to get this equation.

Similarly, because $\boldsymbol{A = \left(g^a\right) \bmod p}$, when Bob computes $\boldsymbol{\left(A^b\right) \bmod p}$, he is computing this:

$$\boldsymbol{\left(\left(\left(g^a\right) \bmod p\right)^b\right) \bmod p = g^{a*b} \bmod p}$$

The last terms can be written because of a special characteristic of exponents in modulus math. Regular math has similar rules. For example, math tells us that all of the following are equivalent:

$$\boldsymbol{X^{Y*Z} = X^{(Y*Z)} = X^{(Z*Y)} = X^{Z*Y}}$$

For example, $\boldsymbol{6^{10} = 6^{(2*5)} = 6^{(5*2)} = 6^{2*5} = 6^{10} = 60,466,176}$.

This make sense, because each of those expressions mean the same thing: raise 6 to the 10th power.

Similarly, for exponents with modulus calculations, these are equivalent

$$\boldsymbol{(g^a \bmod p)^b \bmod p = g^{a*b} \bmod p}$$

You should be able to see that this means that Alice's and Bob's final equations have the same value. If we have time, I will work this out on the whiteboard. As for why it's true, that is a harder question that we won't be able to answer during our class time.

However, it might help you *believe* it's true if you notice the following: if you strip out the modulus parts from the previous equation, you are left with the following equation, which fits in perfectly with our discussion above that used $\boldsymbol{10^6}$ as an example. That might make you wonder if the non-modulus version below is just a special case of the modulus version above (hint, hint).

$$\boldsymbol{(g^a)^b = g^{a*b}}$$

The final facts I will mention about the Diffie-Hellman algorithm are these:

- Once you have a secret, you typically use that as an initial key for an encrypted communication channel.
- Diffie-Hellman works for more than two parties to establish a shared secret.
- If you study college-level math or computer science, you will probably learn gobs about *mod p* operations.

Sources:
https://security.stackexchange.com/questions/45963/diffie-hellman-key-exchange-in-plain-english?newreg=0388fc48938f4da4bd87a09c4eaae1bc, especially the amazing Alice in Wonderland ←→ Sponge Bob graphic, which I will reproduce here: