Diffie-Hellman key exchange

So we have a problem ... to be honest, a lot of problems. But today we will talk about secure message exchange!

Let`s watch at Alice and Bob. They are happy enough, but they want to send messages each other. So they do. But they have a problem I talked earlier. The evil Eve wants to read all of their messages. And now our Alice and Bob become sad. How can we help them? Ciphers you can say. Yea that is a good way. Not now, a little bit later. Why? We for all ciphers we must generate keys for it. But keys should be equal on both sides or have something in common. This means we need to send them. And at this point we are back at our problem.

Two great cryptographists (Obi-Van, sorry) Whitfield Diffie on the left and Martin Hellman on the right saved us creating method called (obviously) Diffie-Hellman key exchange. We need one key for two persons? Not a problem! Let`s generate some awesomely big numbers **g** and **p**. For example, Alice did it so she has to send them to Bob. The next step is to generate secret keys Alice generates **a**, Bob generates **b**. Ha! Great, now we should calculate some value **A** for Alice and **B** for Bob, you see them on the screen. Next one step is to send **A** to Bob and **B** to Alice. And now we can calculate our common secret key named **K** by the formula on the screen. So let`s assume we sent **g** and **p** – our generators, **A** and **B** – public keys, but the **a** and **b** secret keys are still secret and nobody can calculate the common key **K** because of discrete logarithm problem. Now we can use ciphers!

Didn`t understand? That is normal. I have simplified explanation! Alice and Bob have some common color and one secret color each. That is our generators and secret keys. They mix common paint with their secret color and send exchange it. They are the public keys. Now both of them again add personal secret color to mixed and get new common secret color or as we called it earlier key. Yea, it is not very beautiful. Nobody can get it because secret colors were not sent.

Hope I helped you a bit. Let`s check!

* What is the problem?
* Who are the solution authors?
* Why it works?

Words:

Exchange – обмен

Cipher – шифр

Public key – публичный ключ

Secret key – секретный ключ

Simplified – упрощенное

Discrete logarithm – дискретное логарифмирование