A simple explanation of the Diffie-Hellman-Merkle Key Exchange Protocol

Note: the general one-way function used in this protocol is $Y^x \pmod P$. Alice and Bob have chosen values for Y (7) and P (11), and hence have agreed on a one-way hash function of $7^x \pmod{11}$. The values are exchanged in the clear. Both numbers need to be prime.

Alice	Bob
Alice chooses a number, say 3, and keeps it secret. Alice labels her number *A*.	Bob chooses a number, say 6, and keeps it secret. Bob labels his number *B*.
Alice puts 3 into the one-way function and works out the result of $7^A \pmod{11}$: $7^3 \pmod{11} = 343 \pmod{11} = 2$	Bob puts 6 into the one-way function and works out the result of $7^B \pmod{11}$: $7^6 \pmod{11} = 117{,}649 \pmod{11} = 4$
Alice calls the result of here calculation *alpha*, and Alice sends her result, 2, to Bob	Bob calls the result of his calculation *beta*, and Bob sends his result, 4, to Alice
The Swap: ordinarily, this would be a **crucial moment**, because Alice and Bob are exchanging information in the clear, and therefore this is an opportunity for Eve to eavesdrop and find out the details of the information. However, it turns out that Eve can listen in without it affecting the ultimate security of the system. Alice and Bob could use the same telephone line (or network connection) that they used to agree the numbers for Y and P, and Eve could intercept the two numbers that are now being exchanged, that is, 2 and 4. However, *these numbers are not the key*, which is why it does not matter if Eve knows them.	
Alice takes Bob's result and works out the result of: $Beta^A \pmod{11}$: $4^3 \pmod{11} = 64 \pmod{11} = 9$	Bob takes Alice's result and works out the result of: $Alpha^B \pmod{11}$: $2^6 \pmod{11} = 64 \pmod{11} = 9$
Miraculously, Alice and Bob have ended up with the same number, 9. **This is the key!**	

For more details, see Chapter 6 of "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography" (page 265) by Simon Singh. Published by Fourth Estate.