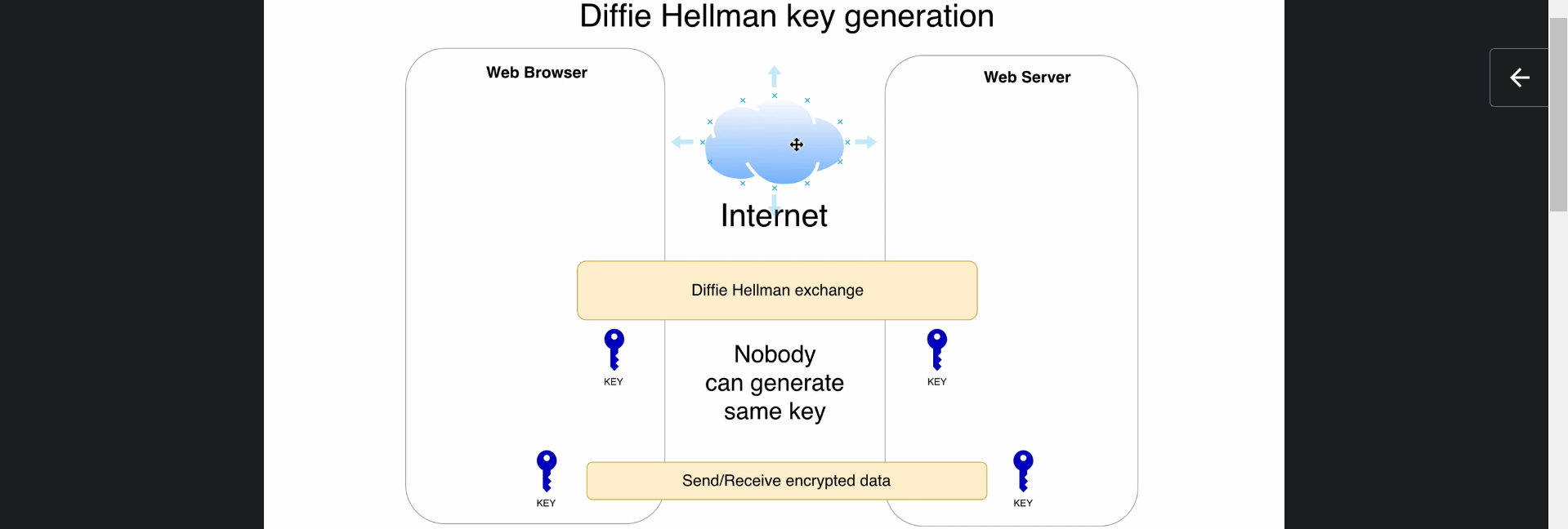
1. From ChatGPT:
   1. It was invented by Whitfield Diffie and Martin Hellman in 1976
   2. DH enables both parties to generate identical encryption keys without transmitting the key itself.
   3. DH allows both parties to independently compute a shared secret without ever transmitting it directly.
2. 
3. It was developed by two people and its name was named after their names.
4. This algo is used to generate Symmetric key over unencrypted public connection (unsecure connection).
   1. Let’s see how it happens in this and next lecture.
5. This algo can be used b/w any two computers. **They don’t need to be browser and webserver**.
6. Diffie-Hellman Algo generates same key on both sides in such a way that nobody can generate same key on both sides.  
   Of course there a sequence of packets which are sent b/w both sides on during phase but the generated key itself (symmetric key) is not sent rather generated by both side but same.
7. **Valid Question**: how same key can be generated both sides still no one can generate the same key.
8. **Answer**: A one-way function is used with parameters. Even though if someone knows the result of the function, they are not able to retrieve the parameters used inside the function.
9. There is a Standard Diffie-Hellman algo that uses mod(modulus) operation and mod is considered as one-way function.   
    **Diffie-Hellman that uses Elliptic** Curve Cryptography (Jatin Inspired by Diffie-Hellman Algo).
10. Next lecture we will talk about both variants.