Diffie Hellman

Overview

This key exchange was one of the significant advancements in public-key cryptography and is still widely implemented in several different security protocols. It allows two parties who have not yet met to create a vital key that they can use to protect their communication. This article explains what it is used for, how it works step by step, its different variations, and the security aspects that must be considered for secure implementation.

This key exchange also called an exponential key exchange, is a digital encryption method that uses numbers of certain powers to generate decryption keys based on components that are never transmitted directly, making the task of potential decryption of codes are mathematically overwhelming. It is a method for the secure exchange of cryptographic keys through a public communication channel. In reality, the keys are not exchanged but are derived together. It is named after its inventors Whitfield Diffie and Martin Hellman. It is a key exchange protocol that allows two parties to communicate through a public channel to create a shared secret without being transmitted over the Internet. DH allows both of you to use a public key to encrypt and decrypt your conversation or data using symmetric cryptography.

Working of Diffie-Hellman key exchange

It is complex and it can be challenging to become familiar with how it works. Let's first explain the Diffie-Hellman essential discussion with an analogy to make things a little more understandable. The best analogy is to imagine two people mixing colors. Let's use the crypto standard and say their names are Alice and Bob. They both initially agree on a random color. Let's say they message each other and choose yellow as their standard color.

They set their color. It does not tell the other party of its choice. Let's say Alice chooses red while Bob chooses a slightly greenish-blue. The next step is for Alice and Bob to mix their secret color (red for Alice, green-blue for Bob) with the mutually agreed yellow. Alice gets an orange blend, while Bob's result is a deeper blue, according to the diagram. Once they have finished shuffling, they send the result to the other party. Alice gets a deeper blue while Bob gets the color orange. After you get the mixed result from

your partner, add her secret color to it. Alice takes the deepest blue and adds her unique red color, while Bob adds her secret green-blue to the orange mix she just received. The result? They both come out the same color, which in this case is a disgusting brown. It may not be the type of color you want to paint your living room with, but it is a standard color nonetheless. This traditional color is known as the shared secret. The critical part of the Diffie-Hellman key exchange is that both parties achieve the same result without having to send the entire shared secret over the communication channel. Picking a standard color, your secret colors, swapping the mix, and then adding your color back gives both parties a chance to come up with the same shared secret without having to submit everything.

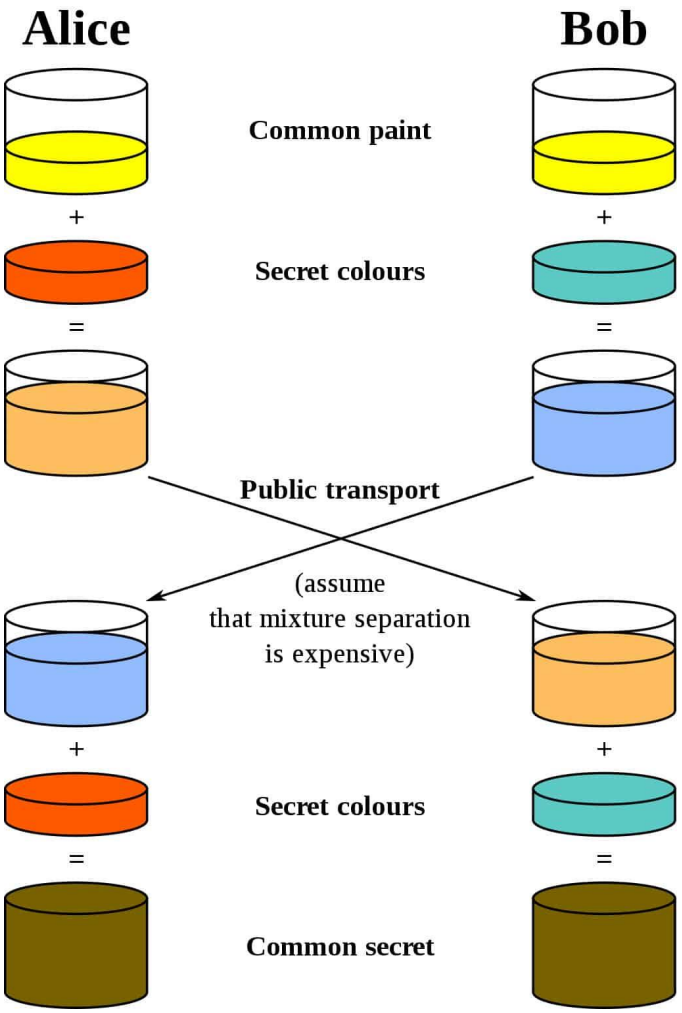

Figure 1: Diffie Hellman