Clave pública y privada

¿Cómo funciona la encriptación por SSL?

Para entender el funcionamiento de la encriptación, hay que tener presente que existen dos claves: una para cifrar y otra descifrar. Explicaremos esto con un ejempĺo.

Supongamos por un momento que la comunicación es entre dos personas, Alice y Bob. Para cifrar el mensaje, Alice tiene una clave y para descifrarlo tiene otra. Previo a comunicarse, Alice se junta con Bob y le traspasa la clave para descifrar.

Esto permite que Alice cifre su mensaje con su clave, le envía el mensaje a Bob, y Bob la descifra con la clave que la pasó previamente Alice. Esto tiene dos ventajas; Primero, el mensaje pasa cifrado por lo que nadie mas puede leerlo a menos que tenga la clave para descifrar. Pero además, la llave para descifrar solo sirve para descifrar mensajes de Alice, por lo que sabremos que el mensaje viene realmente de Alice y no de otra persona.

Clave pública, clave privada

Las dos claves son distintas; Una clave es para cifrar el mensaje, y la otra para descifrarlo. Por eso se dice que este sistema de cifrado es asimétrico.

La clave que firma el mensaje, pero jamás se comparte, recibe el nombre de clave privada, mientras que la clave que se comparte recibe el nombre de clave pública.

Ventajas de SSL

El sistema de juego entonces tiene dos ventajas.

- Cifra el mensaje impidiendo que terceros puedan leerlo.
- Asegura que el emisor es quien dice ser, porque si alguien mas cifró el mensaje con una llave distinao, el mensaje no tendrá sentido al desifrarlo.