EL ALGORITMO DIFFIE-HELLMAN

Angel Hesse Caracena

¿QUE ES?

El algoritmo Diffie-Hellman es un algoritmo creado por Whitfield Diffie y Martin Hellman publicado en 1976. Consiste en acordar una clave secreta entre dos maquinas, a través de un canal inseguro. Con esto se busca conseguir una clave simétrica con la que después se podrán cifrar las comunicaciones entre dichas maquinas.

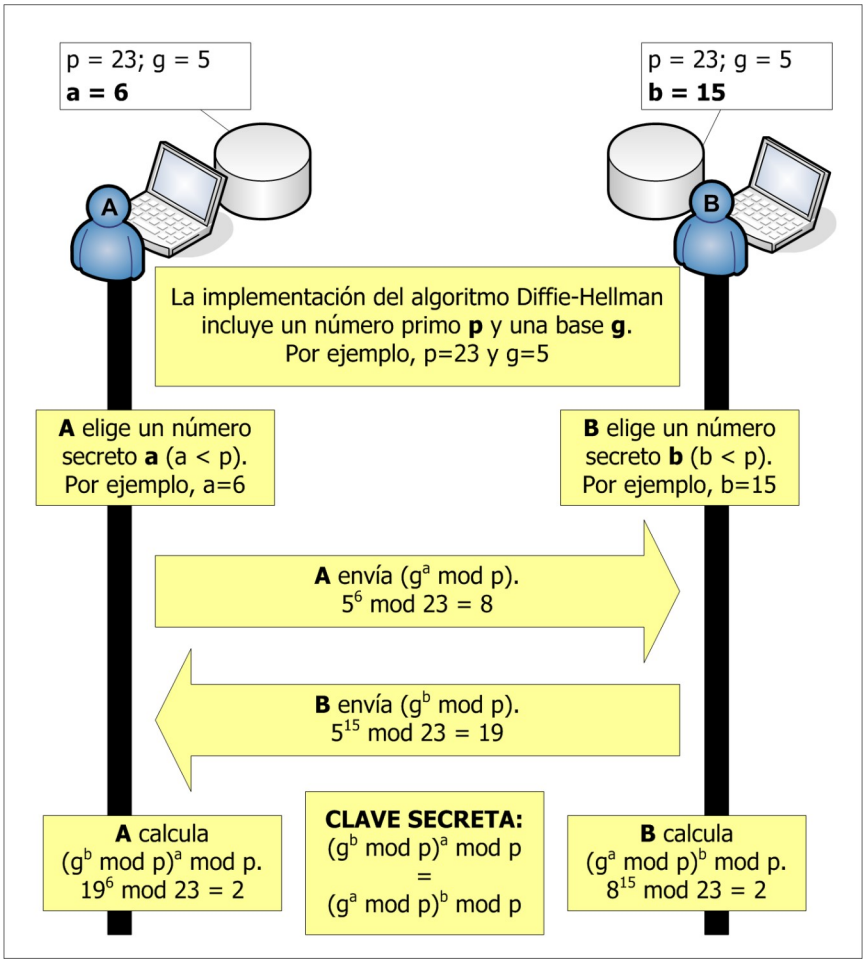
FUNCIONAMIENTO

Se basa en la idea de que dos interlocutores pueden generar conjuntamente una clave compartida sin que un intruso, que esté escuchando las comunicaciones, pueda llegar a obtenerla.

Para ello se eligen dos números públicos (p g) y cada interlocutor su propio número secreto (a b).

Mediante una formula matemática, cada interlocutor hace una serie de operaciones con los dos números públicos y su número secreto. A continuación los interlocutores se intercambian los resultados de forma pública (adquieren llaves públicas). Y por último ambos interlocutores utilizan por separado una fórmula matemática que combina los dos números transformados con su número secreto y al final los dos llegan al mismo número resultado (clave compartida).

Con dicha clave compartida, las comunicaciones podrán ser cifradas y descifradas únicamente por quienes tengan la clave (los interlocutores).



BIBLIOGRAFÍA

https://www.youtube.com/watch?v=bMO59atm8yc

https://es.wikipedia.org/wiki/Diffie-Hellman

https://javiercampos.es/blog/2011/07/22/el-algoritmo-de-diffie-hellman/