UNIVERSIDAD DE GUDALAJARA
CENTRO UNIVERSITARIO: CUTonalá
CRIPTOGRAFÍA

PROYECTO FINAL
Algoritmo de intercambio de llaves de Diffie Hellman

Alumno:
Edwin Michael Rodríguez Cervantes
Maestro:
Carlos Ramon Patiño Ruvalcaba

ÍNDICE

INTRODUCCIÓN

El intercambio de claves Diffie-Hellman fue el primer método ampliamente utilizado para desarrollar e intercambiar claves de forma segura a través de un canal inseguro.

El protocolo criptográfico Diffie-Hellman es un protocolo de establecimiento de claves entre partes que no han tenido contacto previo, utilizado un canal inseguro y de manera anónima, no autenticada.

Se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión, establecer clave de sesión. Siendo no autentificado, sin embargo, provee las bases para varios protocolos autenticos.

Su seguridad radica en la extrema dificultad conjeturada, no demostrada, de calcular logaritmos discretos en un cuerpo finito.

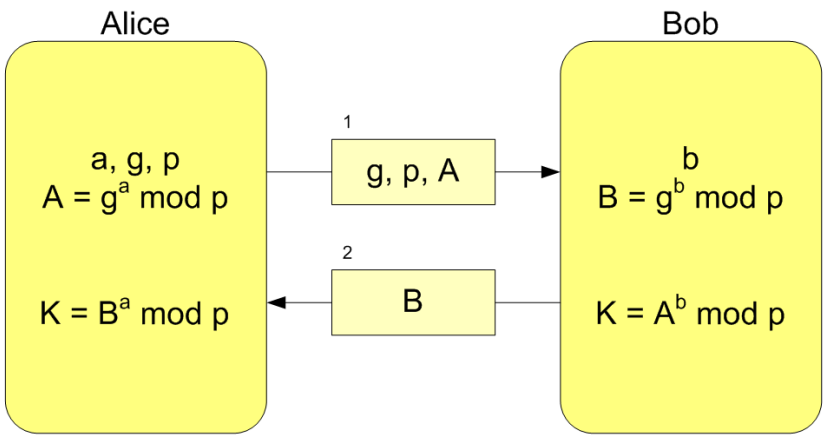
En este reporte de proyecto analizaremos y realizaremos el algoritmo como ejemplo y visualización de el mismo.

DESCRIPCIÓN DE ALGORITMO.

El sistema 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 y, cada interlocutor, un número secreto. Usando una fórmula matemática, que incluye la exponenciación, 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. En teoría revertir esta función es tan difícil como calcular un logaritmo discreto, un sextillón de veces más costosa que la exponenciación usada para transformar los números.

Por eso se dice que este número es el resultado de aplicar una función unidireccional al número secreto.
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, que será la clave compartida.



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Para dos partes Alice y Bob, que intentan establecer una clave secreta, y un adversario Mallory, la versión básica es como sigue:

- Se establecen un primo p y un generador $g \in \mathbf{Z}_p^*$ ([3]). Estos son públicos, conocidos no solo por las partes *Alice* y *Bob* sino también por el adversario *Mallory*.
- *Alice* escoge $a \in \mathbf{Z}_{p-1}$ al azar, calcula $A = g^a \mod p$, y envía A a *Bob*
- *Bob* escoge $b \in \mathbf{Z}_{p-1}$ al azar, calcula $B = g^b \mod p$, y envía B a *Alice*

Nótese que tanto A como B pueden calcular el valor $K = g^{a \cdot b} \mod p$. En efecto, lo podemos demostrar usando las propiedades del grupo $\mathbf{Z}_p^*$:

Para Alice: $B^a \mod p = (g^b \mod p)^a \mod p = (\overbrace{(g^b \mod p)(g^b \mod p) \cdots (g^b \mod p)}^{a}) \mod p = g^{b \cdot a} \mod p = g^{a \cdot b} \mod p = K$

Para Bob: $A^b \mod p = (g^a \mod p)^b \mod p = (\overbrace{(g^a \mod p)(g^a \mod p) \cdots (g^a \mod p)}^{b}) \mod p = g^{a \cdot b} \mod p = K$

Como *ambas* partes pueden calcular K, entonces la podemos usar como clave compartida.

El intercambio de claves Diffie-Hellman tiene sus raíces en la década de 1970. Si bien el campo de la criptografía se había desarrollado significativamente a principios del siglo XX, estos avances se centraron principalmente en el área de la criptografía de clave simétrica.No fue hasta 1976 que los algoritmos de clave pública surgieron en la esfera pública, cuando Whitfield Diffie y Martin Hellman publicaron su artículo, New Directions in Cryptography.

La colaboración describió los mecanismos detrás de un nuevo sistema, que se conocería como el intercambio de claves Diffie-Hellman.

El trabajo se inspiró en parte en desarrollos anteriores realizados por Ralph Merkle. Los llamados rompecabezas de Merkle involucran a una parte que crea y envía una serie de rompecabezas criptográficos a la otra. Estos acertijos requerirían una cantidad moderada de recursos computacionales para resolverlos.

El destinatario elegiría al azar un rompecabezas para resolver y luego haría el esfuerzo necesario para completarlo. Una vez que se resuelve el rompecabezas, se revela al destinatario un identificador y una clave de sesión. Luego, el destinatario transmite el identificador al remitente original, lo que le permite saber qué acertijo se ha resuelto.

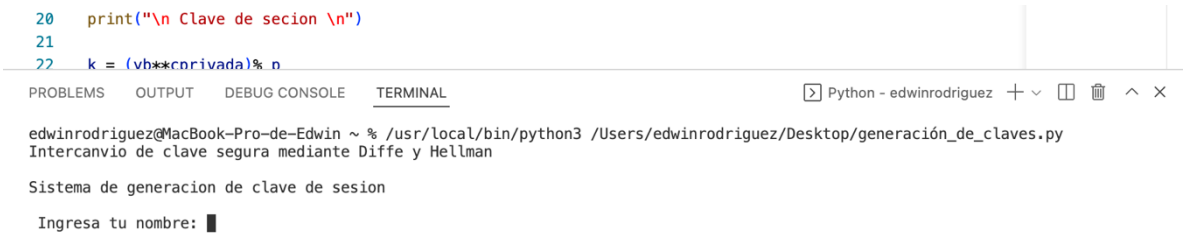
Dado que el remitente original creó los acertijos, el identificador les permite saber qué clave de sesión descubrió el destinatario, y las dos partes pueden usar esta clave para comunicarse de manera más segura. Si un atacante está escuchando la interacción, tendrá acceso a todos los acertijos, así como al identificador que el destinatario transmite al remitente original.

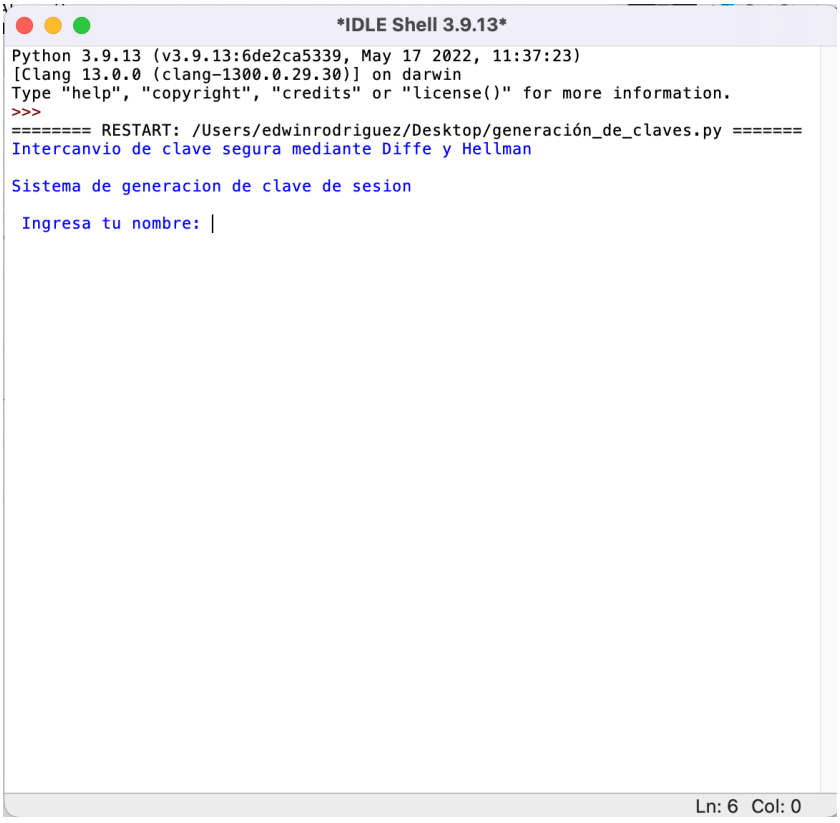
El identificador no le dice al atacante qué clave de sesión se está utilizando, por lo que el mejor enfoque para descifrar la información es resolver todos los acertijos para descubrir la clave de sesión correcta. Dado que el atacante tendrá que resolver la mitad de los acertijos en promedio, termina siendo mucho más difícil para él descubrir la clave que para el destinatario. Este enfoque proporciona más seguridad, pero

está lejos de ser una solución perfecta. El intercambio de claves Diffie-Hellman tomó algunas de estas ideas y las hizo más complejas para crear un método seguro de criptografía de clave pública.

PRUEBAS

Corremos el programa en diferentes terminales para así autentificar la conexión entre ambas, (Terminal en CPU y VScode).





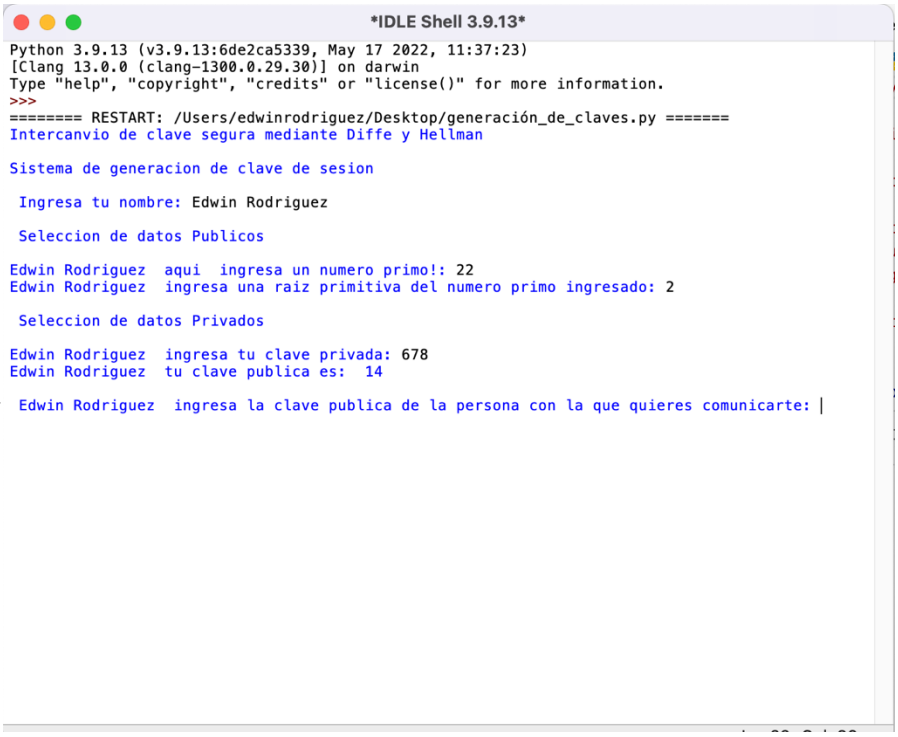
Ingresamos un nombre en cada sistema de generación de claves.

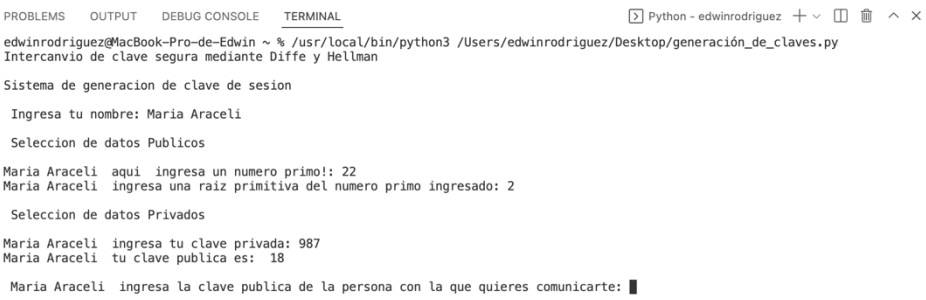
Numero entre los dos usuarios.

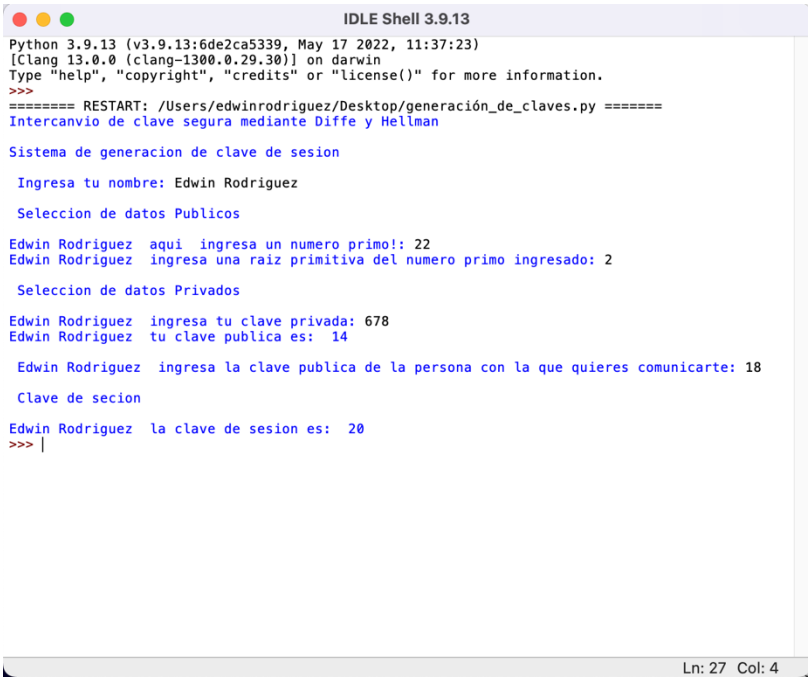
Raíz del número primo en este caso es (2).

Clave única de usuario privada para un reconocimiento único.

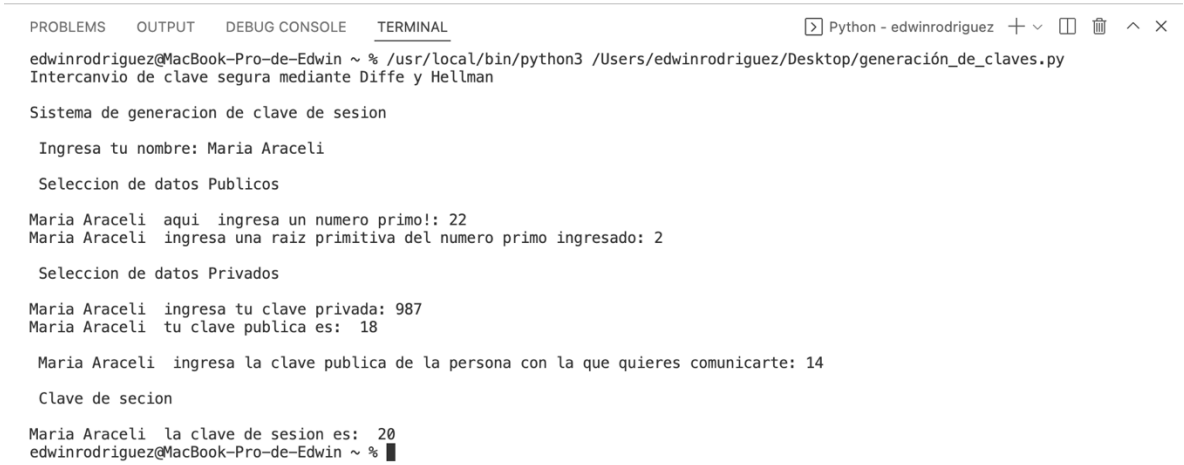
Ingresamos la clave para podernos comunicar con el usuario que deseemos. En este caso la clave de María Araceli (18).







Ya conectados los dos usuarios nos arroja una clave de sesión (20).



Entramos a nuestro programa de cálculo de clave privada, llenamos los datos que nos pide, en este caso la clave publica, el numero primo y la raíz primitiva.
Aquí podemos comprobar la funcionalidad de nuestro programa que gracias al cifrado programable nos arroja la clave publica para así poder interactuar con el otro usuario (María Araceli 18).

```
>>>
======== RESTART: /Users/edwinrodriguez/Desktop/generación_de_claves.py =======
Intercanvio de clave segura mediante Diffe y Hellman

Sistema de generacion de clave de sesion

 Ingresa tu nombre: Edwin Rodriguez

 Seleccion de datos Publicos

Edwin Rodriguez  aqui  ingresa un numero primo!: 22
Edwin Rodriguez  ingresa una raiz primitiva del numero primo ingresado: 2

 Seleccion de datos Privados

Edwin Rodriguez  ingresa tu clave privada: 678
Edwin Rodriguez  tu clave publica es:  14

 Edwin Rodriguez  ingresa la clave publica de la persona con la que quieres comunicarte:
18

 Clave de secion

Edwin Rodriguez  la clave de sesion es:  20
>>>
```

```
Maria Araceli  la clave de sesion es:  20
edwinrodriguez@MacBook-Pro-de-Edwin ~ % /usr/local/bin/python3 /Users/edwinrodriguez/Desktop/calculo_de_clave.py
--------------
Programa para calcular la clave secreta
--------------

Ingresa la clave Publica: 14
Ingresa el numero primo : 22
Ingresa el valor de la raiz primitiva: 20

 La clave privada es:  18

 El tiempo de computo es:  46.93022394180298
edwinrodriguez@MacBook-Pro-de-Edwin ~ %
```

CÓDIGO.
(Python)

Generación de claves.

```
print("Intercanvio de clave segura mediante Diffe y Hellman
\n")

print("Sistema de generacion de clave de sesion")

nombre=input("\n Ingresa tu nombre: ")

print("\n Seleccion de datos Publicos \n")
p=int(input( nombre +" aqui " +" ingresa un numero primo!:
"))
a=int(input( nombre +" ingresa una raiz primitiva del numero
primo ingresado: "))

print("\n Seleccion de datos Privados \n")
cprivada=int(input(nombre + " ingresa tu clave privada: "))

cpublica= (a**cprivada)% p
print(nombre + " tu clave publica es: ",cpublica)


yb=int(input("\n "+ nombre + " ingresa la clave publica de la
persona con la que quieres comunicarte: "))

print("\n Clave de secion \n")

k = (yb**cprivada)% p
print(nombre+ " la clave de sesion es: ", k)
```

Cálculo de clave secreta.

```
from time import time

inicio = time()

print("--------------")
print("Programa para calcular la clave secreta")
print("--------------\n")
clave = int(input("Ingresa la clave Publica: "))
q= int(input("Ingresa el numero primo : "))
a= int(input("Ingresa el valor de la raiz primitiva: "))

for i in range(q):
    ck = (a**i)%q
    if clave==ck:
        resultado=i
        i=q

print(" \n La clave privada es: ", resultado)

final= time()

tiempo=(final-inicio)

print("\n El tiempo de computo es: ",tiempo)
```

CONCLUSIÓN.

El algoritmo de encriptación Diffie-Hellman constituye la base de la criptografía moderna. Permite el desarrollo de varias herramientas y tecnologías. Adicionalmente, hace que la seguridad esté en el proceso de encriptación y no en la llave.

Cabe recalcar que gracias a su implementación la comunicación que es uno de los pilares fundamentales de la humanidad desde su inicio inherente a ella encontramos que tasmbién es un requerimeinto fundamental la necesidad de proteger nuestros mensajes de terceras personas.

Donde este algoritmo permite a dos partes producir un secreto compartido a pesar de que no se hayan nunca antes comunicado. Deffie-Hellman es apliamente usado en varias aplicaciones para encriptar datos, por ejemplo: SSL secure socket layer, TLS transport layer security, SSH secure shell, VPN virtual private network.

REFRENCIAS.

Bibliografía

CRYPTOGRAPHY PIONEERS RECEIVE ACM A.M. (s.f.). TURING AWARD .

Diffie, W. y. (1976). *New directions in cryptography.* IEEE Transactions on Information Theory 22.

Gordon, D. M. (s.f.). *Designing and Detecting Trapdoors for Discrete Log.* Berlin:Springer Verlag: Cryptosystems.

https://ciberseguridad.com/guias/recursos/intercambio-claves-diffie-hellman/