Memoria Algoritmo Diffie-Hellman

A continuación describiré como funciona el código aportado tanto en este fichero zip como en un enlace a mi Github por si hubiera algún problema con alguno de los dos. Dentro del ejecutable cada función y cada bloque de código está explicado más detalladamente.

Para empezar en el ejecutable nos encontraremos un encabezado donde se explica que práctica es, asignatura, nombre y apellidos.

A continuación, nos encontramos con una función llamada "mod_exp". Esta función la definimos para poder realizar el calculo del algoritmo mucho más rápido computacionalmente y le pasamos como parámetros de entrada la base, el exponente generado aleatoriamente y el número primo.

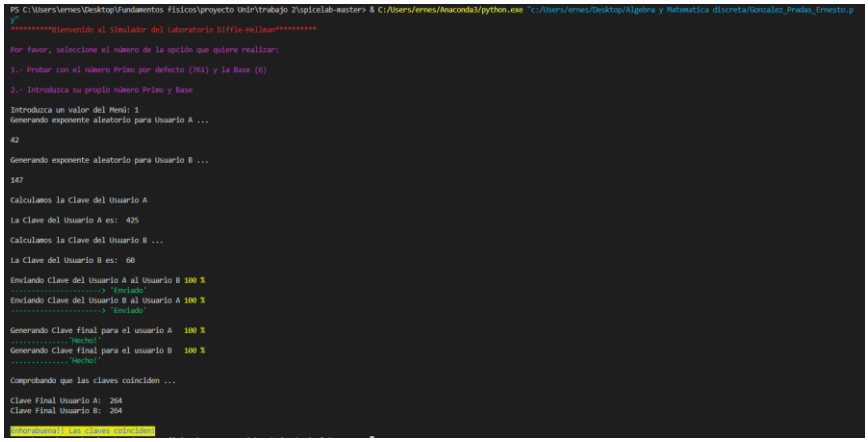
La siguiente función que nos encontramos es una función que no tiene que ver con la práctica en sí, pero que la he querido realizar para darle un toque más personal a la práctica ya que me dedico profesionalmente a programar (Desarrollo software de defensa para el ministerio de defensa) y bueno soy un poco friki para estas cosas. Básicamente lo que hace es simular tanto para el envío de claves como para la generación un loading de 0-100% diferenciado con colores para que se vea el loading por un lado de color amarillo y el 'enviado' o 'hecho!' con verde.

Siguiendo el código, nos encontramos un menú interactivo donde nos dará a elegir entre la opción número 1 que será realizar las pruebas con el primo y la base marcados por la práctica (p = 761 y g = 6) o la número 2 que introduciremos nuestro número primo y nuestra base.

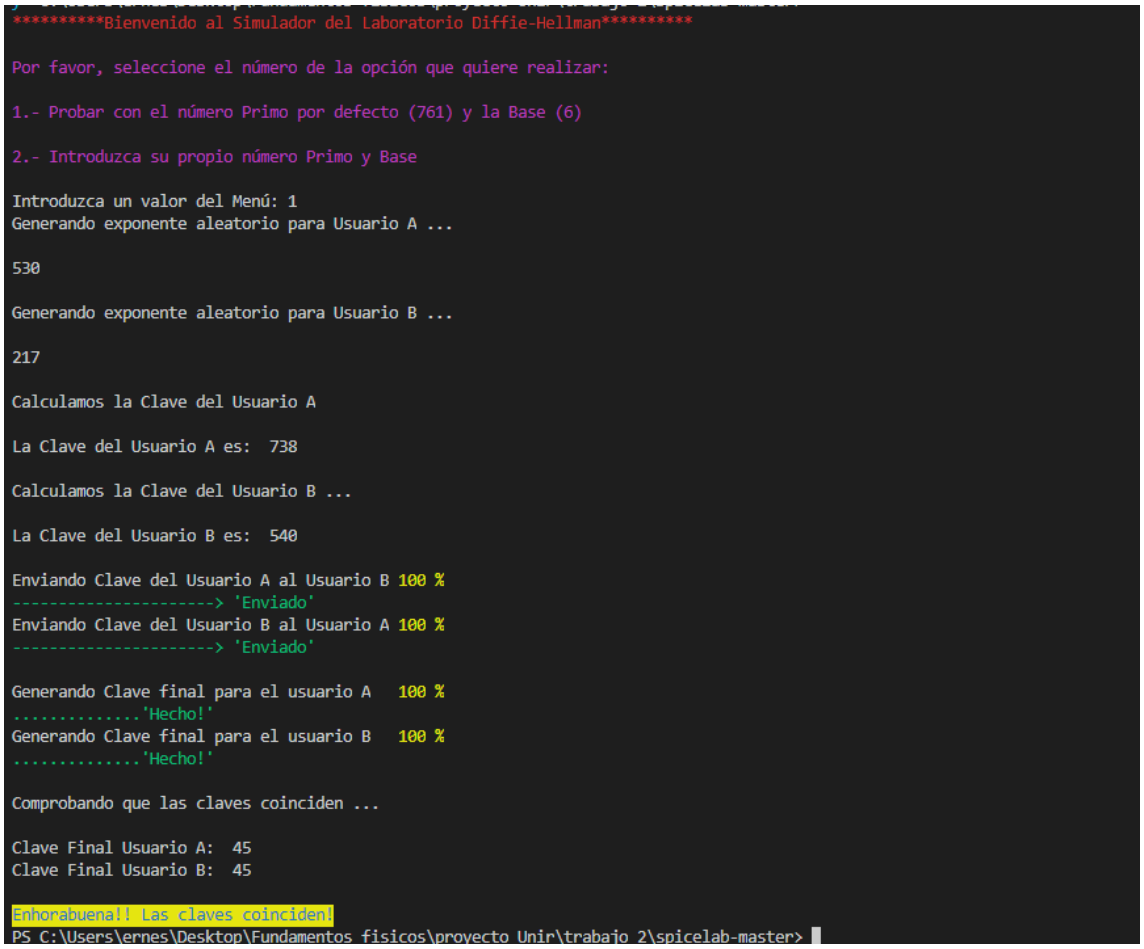
En el propio código dejo comentado cada paso que se va realizando para que quede claro todas las partes del programa, por lo que a continuación paso a exponer las pruebas y los resultados que he obtenido.

Con este programa tenemos dos modalidades a las que podemos acceder a partir de un menú interactivo descrito ya más arriba:

1.- Usando la opción del menú número 1 estos son algunos resultados que he obtenido (las capturas se ven pequeñas pero si se amplía el Word se pueden leer perfectamente las líneas (más o menos sobre un 180% - 200%)):

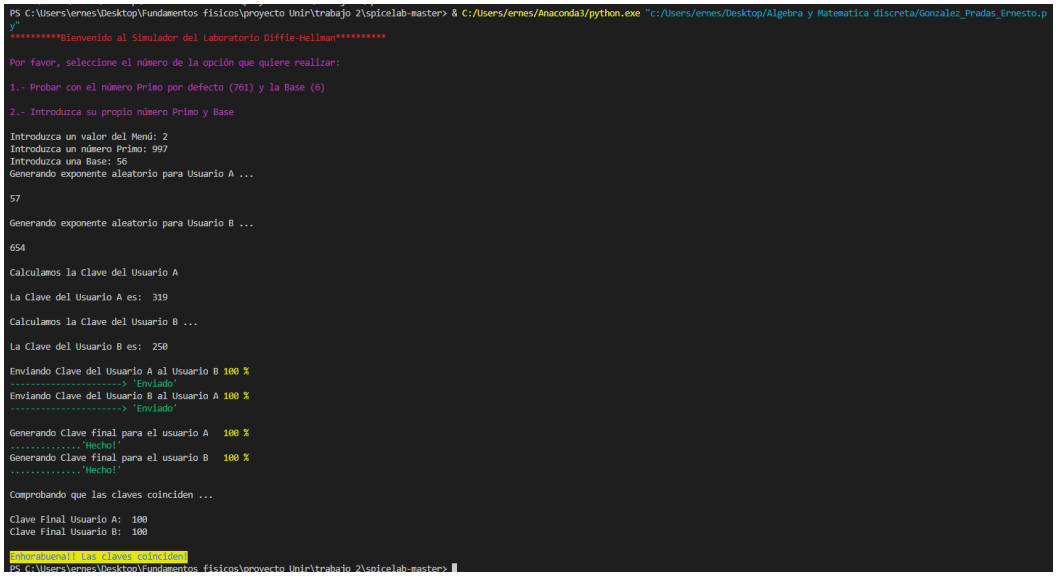


Otra prueba:



En general, con la primera opción del menú he realizado unas 15 simulaciones y siempre me han salido bien las claves.

2.- Usando la opción del menú número 2 estos son algunos resultados, primero usando mis propios números primos (primer caso p = 997 segundo caso p = 10007):



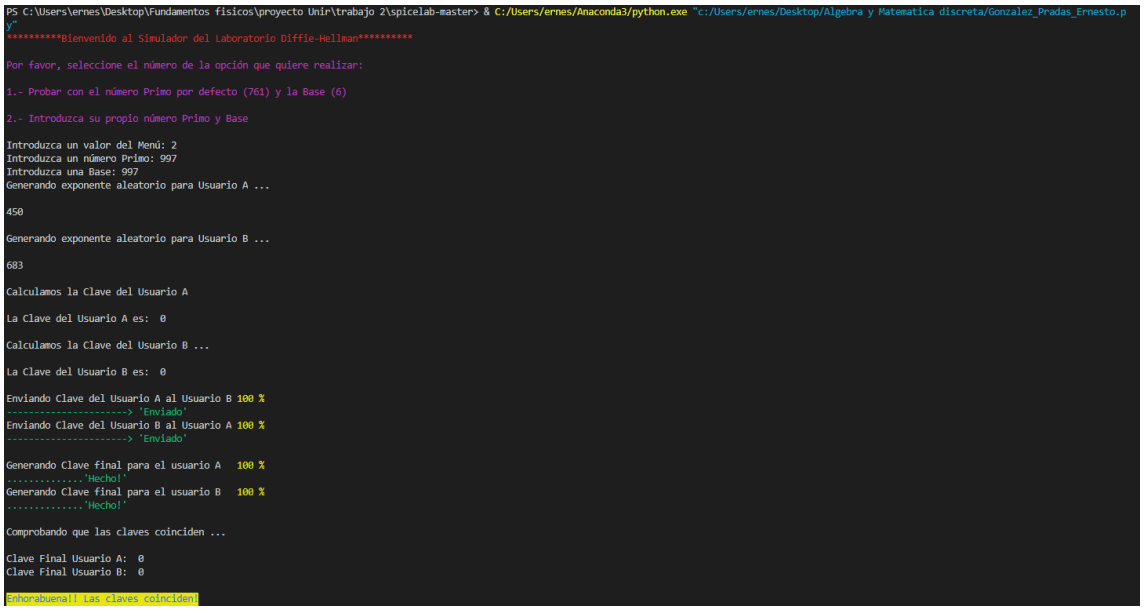
```
PS C:\Users\ernes\Desktop\Fundamentos fisicos\proyecto Unir\trabajo 2\spicelab-master> & C:/Users/ernes/Anaconda3/python.exe "c:/Users/ernes/Desktop/Algebra y Matematica discreta/Gonzalez_Pradas_Ernesto.p
y"
*********Bienvenido al Simulador del Laboratorio Diffie-Hellman*********

Por favor, seleccione el número de la opción que quiere realizar:

1.- Probar con el número Primo por defecto (761) y la Base (6)

2.- Introduzca su propio número Primo y Base

Introduzca un valor del Menú: 2
Introduzca un número Primo: 10007
Introduzca una Base: 89
Generando exponente aleatorio para Usuario A ...

6884

Generando exponente aleatorio para Usuario B ...

4738

Calculamos la Clave del Usuario A

La Clave del Usuario A es:  9063

Calculamos la Clave del Usuario B ...

La Clave del Usuario B es:  1579

Enviando Clave del Usuario A al Usuario B 100 %
----------------------> 'Enviado'
Enviando Clave del Usuario B al Usuario A 100 %
----------------------> 'Enviado'

Generando Clave final para el usuario A   100 %
..............'Hecho!'
Generando Clave final para el usuario B   100 %
..............'Hecho!'

Comprobando que las claves coinciden ...

Clave Final Usuario A:  1894
Clave Final Usuario B:  1894

Enhorabuena!! Las claves coinciden!
PS C:\Users\ernes\Desktop\Fundamentos fisicos\proyecto Unir\trabajo 2\spicelab-master>
```

A continuación algunos ejemplos en los que no se han introducido números primos(primer caso p = 888 segundo caso p = 666242862):

```
PS C:\Users\ernes\Desktop\Fundamentos fisicos\proyecto Unir\trabajo 2\spicelab-master> & C:/Users/ernes/Anaconda3/python.exe "c:/Users/ernes/Desktop/Algebra y Matematica discreta/Gonzalez_Pradas_Ernesto.p
y"
*********Bienvenido al Simulador del Laboratorio Diffie-Hellman*********

Por favor, seleccione el número de la opción que quiere realizar:

1.- Probar con el número Primo por defecto (761) y la Base (6)

2.- Introduzca su propio número Primo y Base

Introduzca un valor del Menú: 2
Introduzca un número Primo: 888
Introduzca una Base: 5
Generando exponente aleatorio para Usuario A ...

385

Generando exponente aleatorio para Usuario B ...

549

Calculamos la Clave del Usuario A

La Clave del Usuario A es:  389

Calculamos la Clave del Usuario B ...

La Clave del Usuario B es:  413

Enviando Clave del Usuario A al Usuario B 100 %
----------------------> 'Enviado'
Enviando Clave del Usuario B al Usuario A 100 %
----------------------> 'Enviado'

Generando Clave final para el usuario A   100 %
..............'Hecho!'
Generando Clave final para el usuario B   100 %
..............'Hecho!'

Comprobando que las claves coinciden ...

Clave Final Usuario A:  413
Clave Final Usuario B:  413

Enhorabuena!! Las claves coinciden!
```

```
PS C:\Users\ernes\Desktop\Fundamentos fisicos\proyecto Unir\trabajo 2\spicelab-master> & C:/Users/ernes/Anaconda3/python.exe "c:/Users/ernes/Desktop/Algebra y Matematica discreta/Gonzalez_Pradas_Ernesto.p
y"
*********Bienvenido al Simulador del Laboratorio Diffie-Hellman*********

Por favor, seleccione el número de la opción que quiere realizar:

1.- Probar con el número Primo por defecto (761) y la Base (6)

2.- Introduzca su propio número Primo y Base

Introduzca un valor del Menú: 2
Introduzca un número Primo: 666242862
Introduzca una Base: 8947
Generando exponente aleatorio para Usuario A ...

138687034

Generando exponente aleatorio para Usuario B ...

624754904

Calculamos la Clave del Usuario A

La Clave del Usuario A es:  620020075

Calculamos la Clave del Usuario B ...

La Clave del Usuario B es:  429530467

Enviando Clave del Usuario A al Usuario B 100 %
----------------------> 'Enviado'
Enviando Clave del Usuario B al Usuario A 100 %
----------------------> 'Enviado'

Generando Clave final para el usuario A   100 %
..............'Hecho!'
Generando Clave final para el usuario B   100 %
..............'Hecho!'

Comprobando que las claves coinciden ...

Clave Final Usuario A:  637666585
Clave Final Usuario B:  637666585

Enhorabuena!! Las claves coinciden!
```

Los únicos casos un poco distintos que he encontrado es cuando usamos de primo y de base el mismo número que nos genera todas las claves a 0:



Conclusión

He realizado numerosas pruebas, y no he encontrado ningún caso en el que el programa no devolviera las claves finales bien, ya sea con los p y b del enunciado o con los míos propios siendo estos, p primos y no primos, mayores y menos que la base. Lo único un poco más raro es el último caso expuesto donde p=b. Es posible que se me haya escapado alguna casuística.