

DISEÑO DE ALGORTIMOS

PRACTICA 2: ALGORITMO DIFFIE HELLMAN

PABLO LARIO GOMEZ

DIEGO MIGUEL LOPEZ GARCIA

INDICE

[INTRODUCCION 2](#_Toc100420331)

[FUNCIONAMIENTO 2](#_Toc100420332)

[CUESTIONES Y PRUEBAS 3](#_Toc100420333)

[EJERCICIO PRACTICA 3](#_Toc100420334)

[EJERCICIO FORO 4](#_Toc100420335)

# 

# INTRODUCCION

Hoy en día, la seguridad en las comunicaciones es de vital importancia, no sabemos quién es la persona al otro lado de nuestro teléfono, o si alguien lee nuestros correos electrónicos antes de que lleguen a su destino, por ello ser capaces de cifrar nuestras comunicaciones es muy importante, para solo nosotros y quien queramos podamos mantener una comulación segura.

Es por ello que el algoritmo de Diffie-Hellman permite acordar una clase secreta, entre dos máquinas, a través de un canal inseguro, y enviando tan solo dos mensajes. La principal aplicación de este protocolo es acordar una clave simétrica con la que poder cifrar las comunicaciones.

El protocolo fue publicado en 1976, pero actualmente se sabe que es vulnerable, ya que a ataques de tipo Man in the Middle (MitM), este tipo de ataque se centra en situar una maquina entre ambas máquinas, y esta tercera maquina se hace pasar por ambas, por lo que puede acordar una clave con cada extremo sin que estos sepan realmente si se están comunicando con la maquina adecuada, la misión de esta maquina situada en medio es recibir la información de ambas partes y cifrarla con la correspondiente clave de cada extremo, por lo que de cara a las maquinas que quieren comunicarse es invisible.

Para solucionar este gran problema de seguridad se puede usar en conjunto con otros sistemas de seguridad basados en autenticación de mensajes. En esta practica usaremos el protocolo básico.

# FUNCIONAMIENTO

Veamos el funcionamiento básico de este algoritmo, aunque parezca complejo es bastante sencillo y potente.

Imaginemos que dos compañeros de clase están pensando en hacer un trabajo para subir nota, pero estos tienen que comunicarse por el foro de la asignatura y no quieren que les quiten la idea.

Diego y Pablo van a ser nuestros compañeros, pero Pedro sabe que están pensando en hacer el trabajo y quiere copiarles la idea.

1. Diego publica un número primo *“p”* y un número generador *“n”* por el foro.
2. Pablo escoge un número *“x”* secreto y envía un nuevo número *“z1”* de la forma: .
3. Diego escoge un valor *“y”* secreto, calcula y envía un nuevo número *“z2”* de la forma: .
4. Pablo calcula la clave secreta *“z”* de la forma:
5. Diego calcula la clave secreta *“z”* de la forma:

Los valores de *p* y *n* son públicos y Pedro puede conocerlos, pero no supone una vulnerabilidad, ya que, aunque Pedro los conoce, no puede averiguar la clave de Pablo y Diego.

En el caso de usar valores pequeños, es fácil encontrar el valor de clave, pero si usamos números grandes, el tiempo de calcular la clave por fuerza bruta se dispara.

# CUESTIONES Y PRUEBAS

## EJERCICIO PRACTICA

En este apartado vamos a ver la prueba que se plantea en la practica y un caso particular en el foro de la asignatura.

Encontrar la clave común para estos datos:

n = 12345701.

p = 66666667.

z1 = 8049097.

z2 = 6438362.

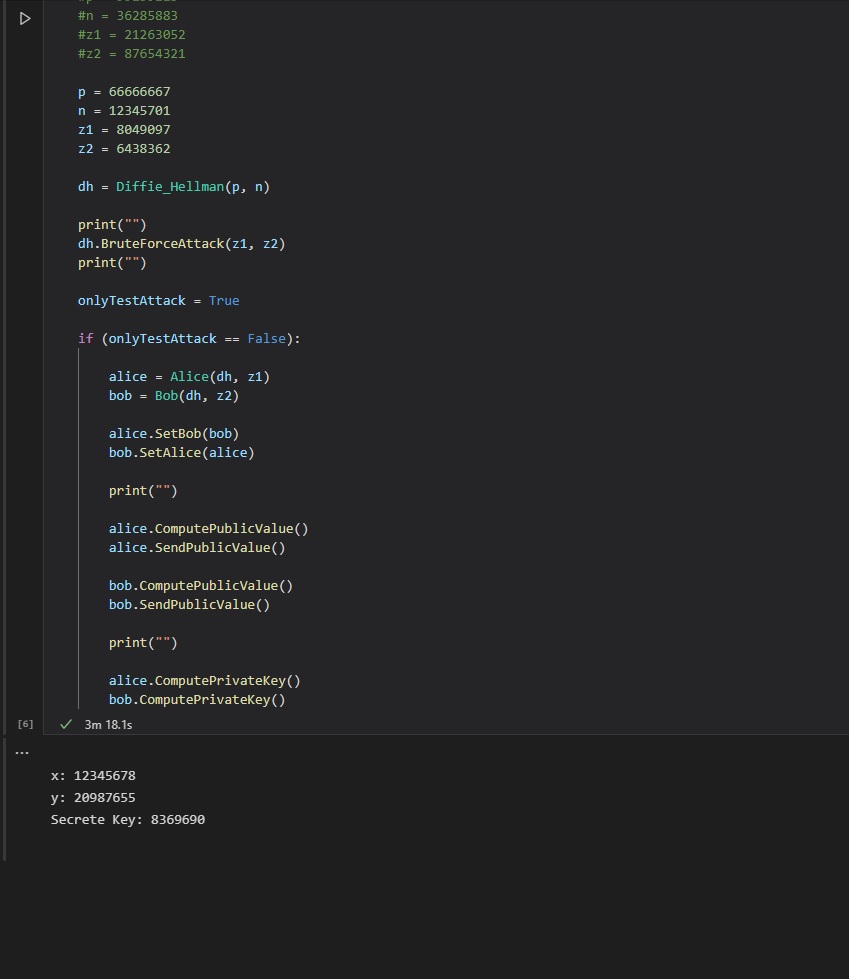
Valores obtenidos:

x: 12345678 (2m 11s).

y: 20987655.

Secrete Key: 8369690.

Tiempo empleado: 3m 18s.



## EJERCICIO FORO

Ahora pasamos a ver el ejercicio del foro, con estos mensajes:

p = 99239213

n = 36285883

z1 = 21263052

z2 = 87654321

