



# Protocolo Diffie-Hellman

Ing. Max Alejandro Antonio Cerna Flores

# Agenda

## Protocolo Diffie-Hellman

Historia

Descripción básica

Complejidad de Logaritmo Discreto

¿Cómo funciona?

Ataques de hombre en medio (MiTM)

Solución a ataques MiTM

# Historia

El intercambio de claves Diffie-Hellman debe su nombre a sus creadores Whitfield Diffie y Martin Hellman, publicaron su artículo **New Directions in Cryptography** en 1976.

Permite acordar una clave secreta entre dos máquinas, a través de un canal inseguro y enviando únicamente dos mensajes.

Actualmente se conoce que es vulnerable a ataques de hombre en medio.

Whitfield Diffie y Martin Hellman recibieron el premio A.M. Turing de 2015 de la Association for Computer Machinery en 2016.

<https://awards.acm.org/about/2015-turing>

# Descripción Básica



# Descripción Básica



# Descripción Básica



Alice



Bob y Alice escogen  
un nuevo segundo  
color el cual solo  
ellos conocen



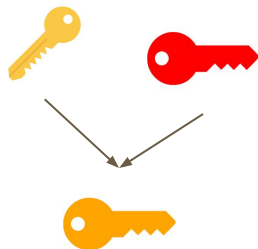
Bob



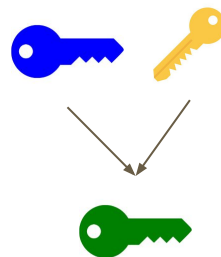
# Descripción Básica



Alice



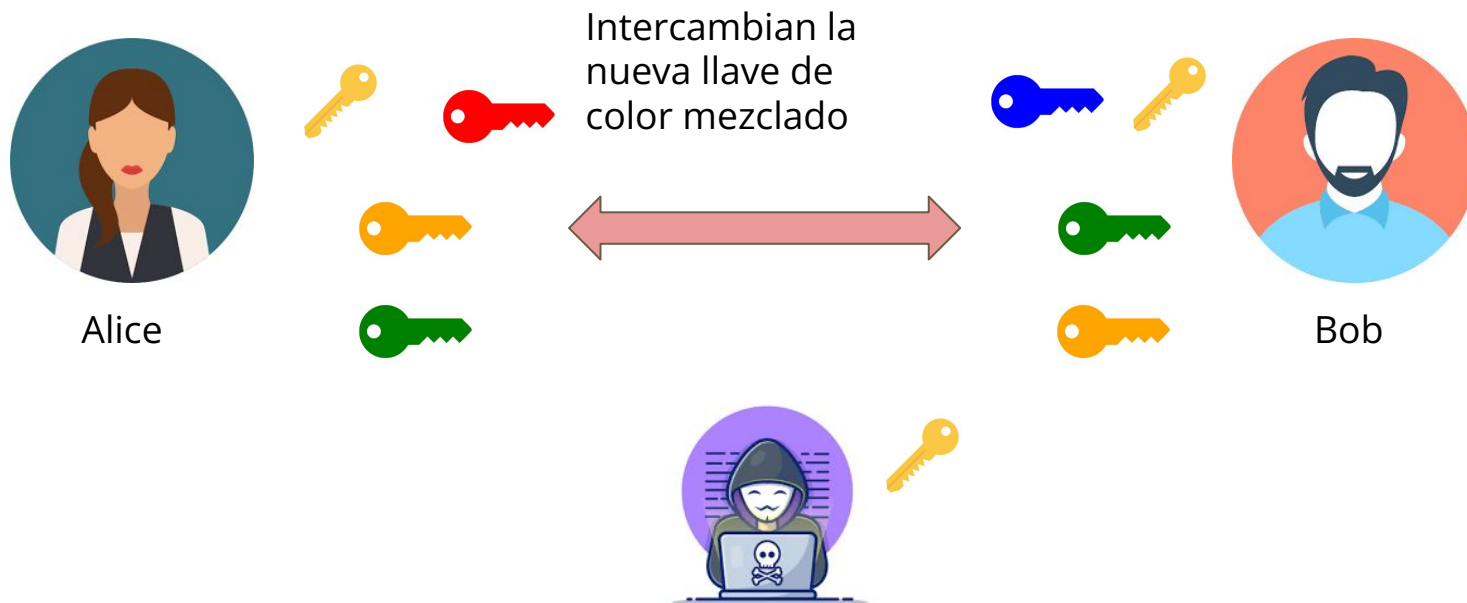
Mezclan la común  
con la secreta  
generando un  
nuevo color



Bob

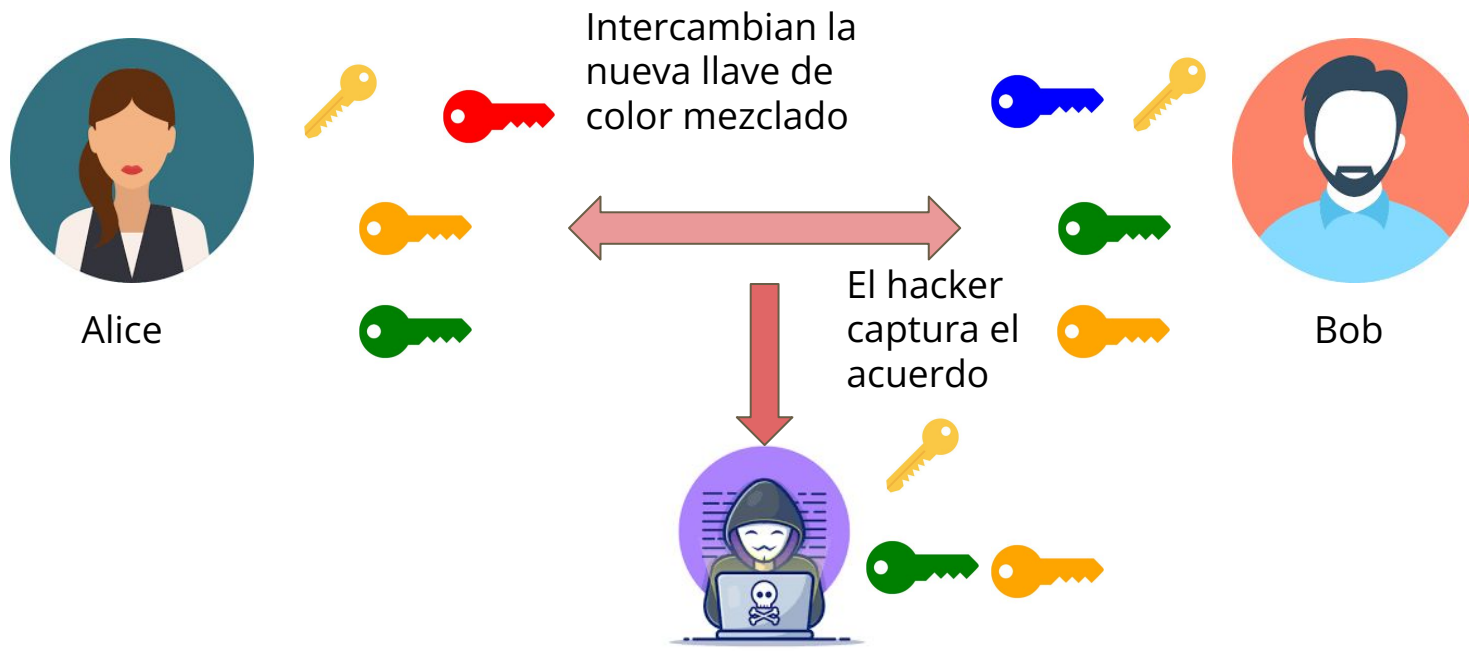


# Descripción Básica

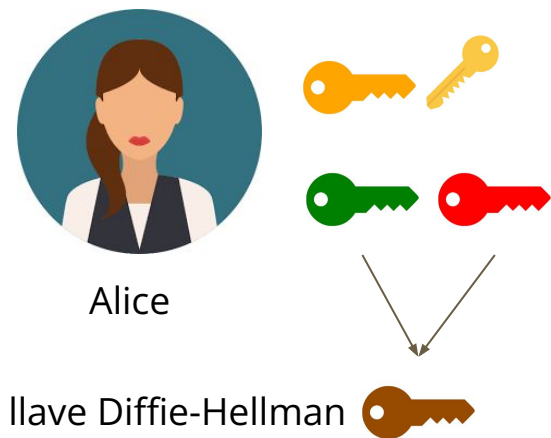




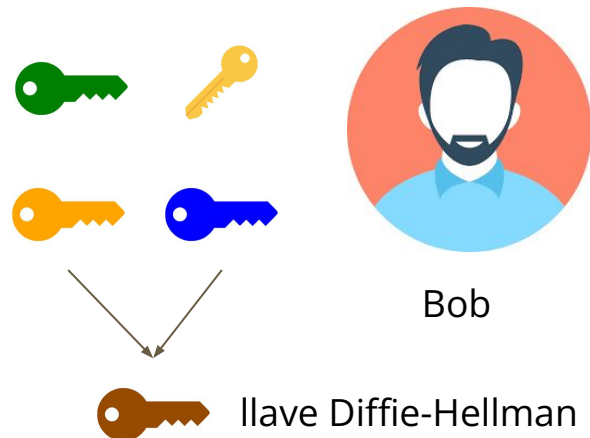
# Descripción Básica



# Descripción Básica



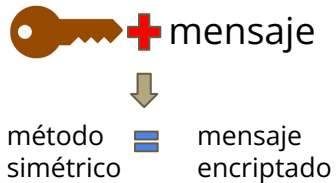
se mezclan la última llave compartida entre ellos con la llave privada de cada uno y se genera una llave igual para ambas partes



# Descripción Básica



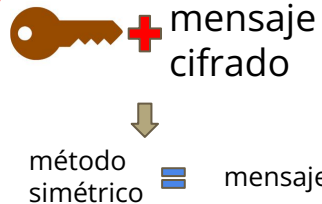
Alice



llaves públicas



llave privada



Bob

llaves públicas



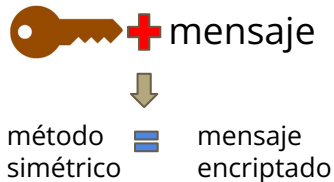
llave privada



# Descripción Básica



Alice



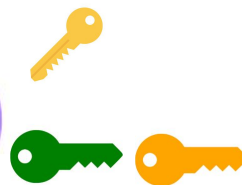
llaves públicas



llave privada



Hacker captura el mensaje cifrado e intenta descifrar usando las llaves.



Bob

llaves públicas



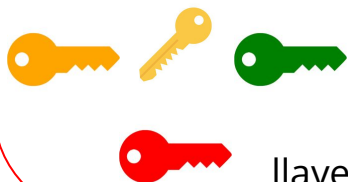
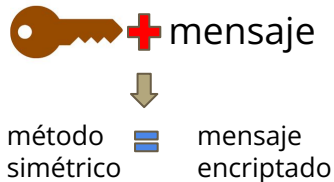
llave privada



# Descripción Básica



Alice

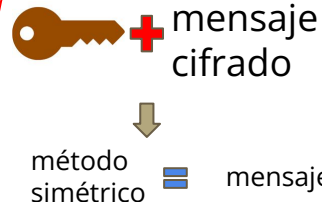


llaves públicas

llave privada



Sin las llaves privadas no puede generar la clave Diffie-Hellman



Bob



llaves públicas

llave privada

# Complejidad de Logaritmo Discreto

La seguridad del algoritmo creado por Whitfield Diffie y Martin Hellman se basa en la dificultad de solucionar el problema del **logaritmo discreto**.

El algoritmo se basa en las propiedades de la **exponenciación modular**.

La exponenciación modular es un tipo de exponenciación realizada sobre un módulo.

$$A = k^a \bmod p$$

# Complejidad de Logaritmo Discreto

**¿Cual es el problema del logaritmo discreto?**

Conociendo  $k, a$  y  $p$  (este último siendo un número primo) y realizando exponenciación modular:

$$A = k^a \bmod p$$

es muy fácil calcular  $A$ , supongamos  $k=3, a=2$  y  $p = 11$  entonces:

$$A = 3^2 \bmod 11 = 9$$

# Complejidad de Logaritmo Discreto

¿Cual es el problema del logaritmo discreto?

Pero, qué pasaría si conocemos  $A$ ,  $k$  y  $p$  pero desconocemos  $a$ :

$$A = k^a \bmod p$$

entonces:

$$a = \log_k A \bmod p$$



# Complejidad de Logaritmo Discreto

¿Cual es el problema del logaritmo discreto?

Calcular  $\log_k A$  **SIMPLE**

Al resultado anterior aplicarle  $\text{mod } p$  **MUY COMPLEJO**

Esto se puede notar a mayor grado conforme los números utilizados son más grandes.

# ¿Cómo funciona?



Alice



Bob

acuerdan clave pública  
( $k, p$ ) en común

$p$  es un número primo  
muy grande.

$k$  es un número menor  
que  $p$  ( $0 < k < p$ )

Supongamos  $p=17$  y  $k=4$

$$A = k^a \bmod p$$

# ¿Cómo funciona?

Alice calcula su llave privada  $a$



$a$  es un número menor que  $p$   
( $0 < a < p$ )



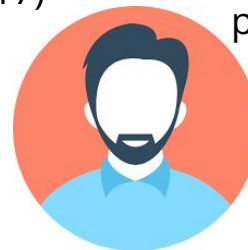
Alice

(4,17)

$$A = k^a \bmod p$$

Supongamos  $a=3$  y  $b=6$

(4,17)



Bob

Bob calcula su llave privada  $b$



$b$  es un número menor que  $p$   
( $0 < b < p$ )

$$B = k^b \bmod p$$

# ¿Cómo funciona?

Calculamos A  
sabiendo

$a=3$   
 $k=4$   
 $p=17$



Alice

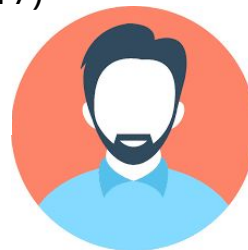
$(4,17)$



$$A = 4^3 \bmod 17$$

$$A = 13$$
 

$(4,17)$



Bob

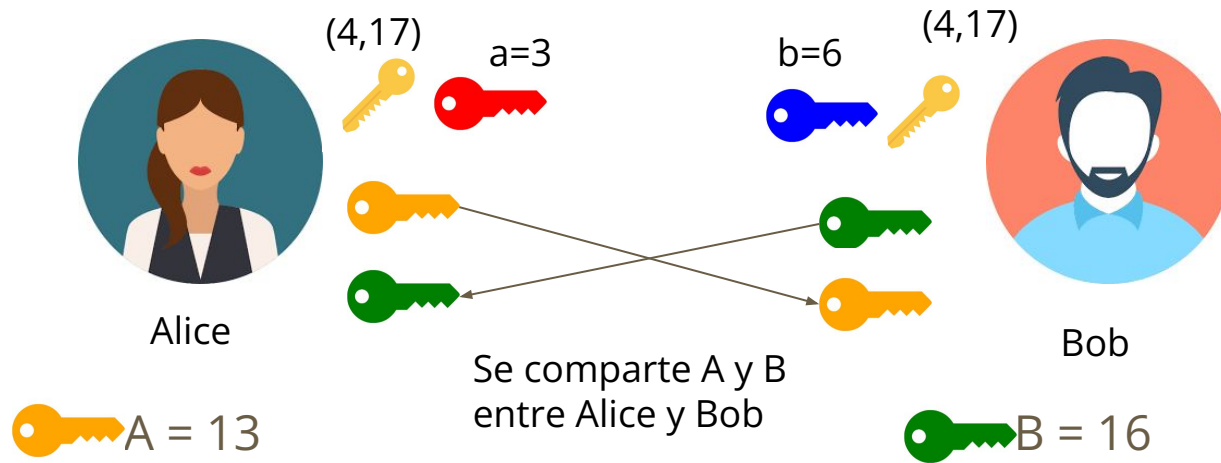
Calculamos B  
sabiendo

$b=6$   
 $k=4$   
 $p=17$

$$B = 4^6 \bmod 17$$


$$B = 16$$
 

# ¿Cómo funciona?



# ¿Cómo funciona?

(4,17)  $a=3$



Alice

Alice is represented by a circular icon of a woman with brown hair. To her right are four keys: a yellow key, a red key, an orange key, and a green key. The text '(4,17)' and 'a=3' is positioned above the keys.

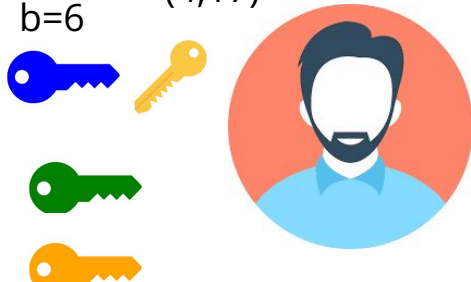
  $B = 16$    $a=3$

$K = B^a \bmod p$



$K = 16^3 \bmod 17 = 16$

(4,17)  $b=6$



Bob is represented by a circular icon of a man with a beard. To his left are four keys: a blue key, a yellow key, a green key, and an orange key. The text '(4,17)' and 'b=6' is positioned above the keys.

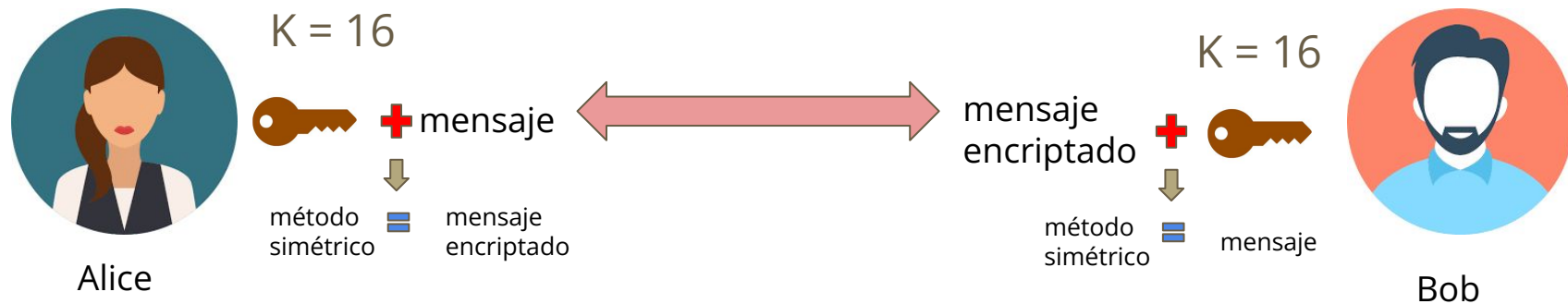
  $A = 13$    $b=6$

$K = A^b \bmod p$



$K = 13^6 \bmod 17 = 16$

# ¿Cómo funciona?



# Ataques de Hombre en Medio (MiTM)

El atacante puede ser un oyente pasivo en tu conversación robando los mensajes mientras escucha, o un participante activo, alterando el mensaje.

En el protocolo Diffie-Hellman un atacante podría situarse entre ambas máquinas y acordar una clave simétrica con cada una de las partes.

Una vez establecidas las 2 claves simétricas, el atacante haría de puente entre los 2 hosts, descifrando toda la comunicación y volviéndola a cifrar para enviársela al otro host.



# Solución a los ataques MiTM

Diffie-Hellman no proporciona autenticación, no tiene forma de verificar si la otra parte en una conexión es realmente quien dice ser.

La autenticación del mensaje es necesaria para evitar que intermediarios utilicen un ataque hombre en medio.

Generalmente se implementa junto con algunos medios de autenticación. Esto a menudo implica el uso de certificados digitales y un algoritmo de clave pública.