# Llaves públicas y privadas

## Introducción

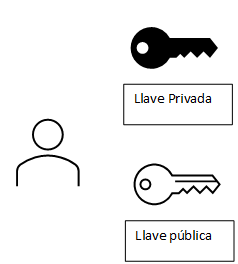
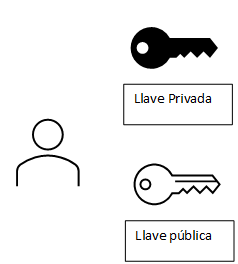
Cifrado asimétrico de un solo camino.

Se vinculan matemáticamente una con la otra, se requiere la llave pública para poder ver lo de la privada.

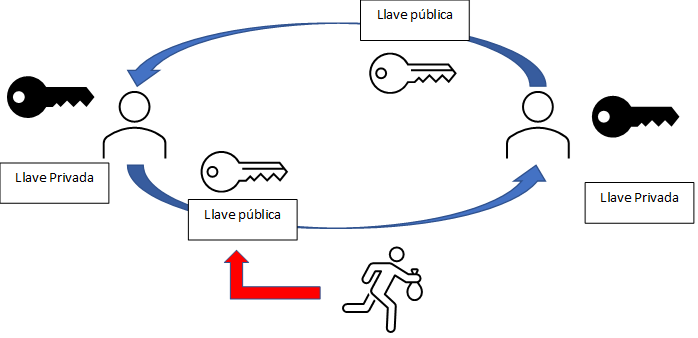
Las llaves públicas y privadas nos ayudan a cifrar y descifrar nuestros archivos de forma que los podamos compartir sin correr el riesgo de que sean interceptados por personas con malas intenciones.

La forma de hacerlo es la siguiente:

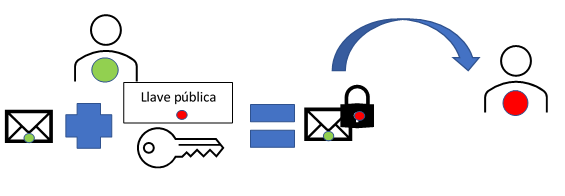
Ambas personas deben crear su llave pública y privada.

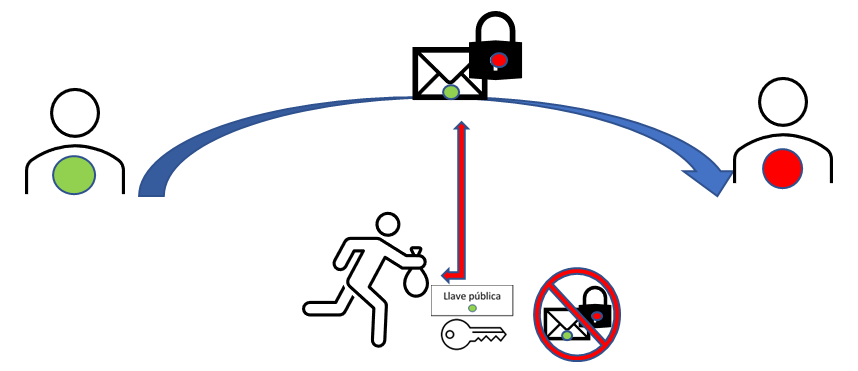


Ambas personas pueden compartir su llave pública a las otras partes (recuerda que esta llave es pública, no hay problema si la “interceptan”).

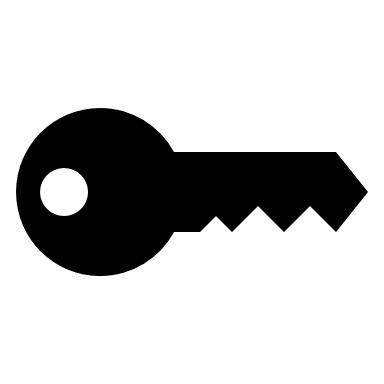
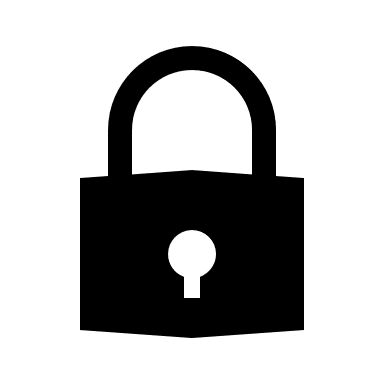


La persona que quiere compartir un mensaje puede usar la llave pública de la otra persona para cifrar los archivos y asegurarse que solo puedan ser descifrados con la llave privada de la persona con la que queremos compartir el mensaje.

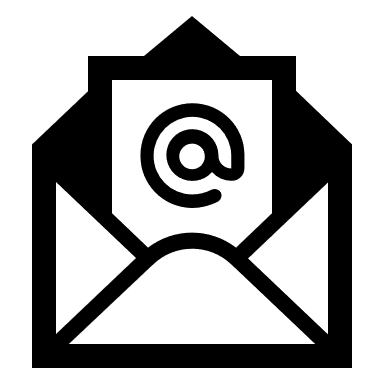
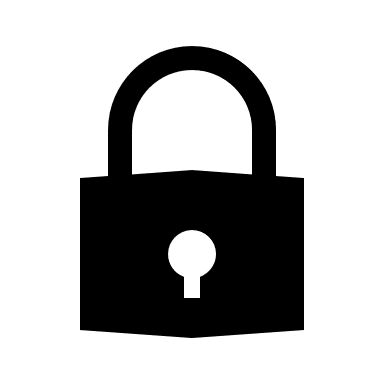


El mensaje está cifrado y puede ser enviado a la otra persona sin problemas en caso de que los archivos sean interceptados.

La persona a la que enviamos el mensaje cifrado puede usar su llave privada para descifrar el mensaje y ver los archivos.



Llave Privada



## Configuración de llave SSH en local

SSH o Secure Shell: Es un protocolo de red que permite acceso remoto seguro a través de una conexión encriptada. Este método de autenticación requiere un passphrase (contraseña) o tambien puede funcionar sin passphrase sobre la clave.

$ git config -l: Muestra la configuración dentro de Git(user y email), Este comando funciona por que Git esta instalado en todo el equipo local.

$ git config --global user.email “nombre\_email\_cambiado” : Se puede utilizar este mismo comando para cambiar el email.

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza baja

ssh-keygen -t rsa -b 4096 -C “[correo@ausar.com](mailto:correo@ausar.com)”

ssh-keygen: Generar llave ssh

-t : especifica el algoritmo para la llave.

Rsa : el algoritmo a utilizar.

-b : Que tan compleja es la llave.

4096: nivel de complejidad solicitado.

-C : correo electrónico al que estará conectada la llave.

Se ejecuta el comando:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Se deja por defecto la ruta mostrada en pantalla, se selecciona contraseña y se escribe la confirmación de esta.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Se realiza la verificaciòn de lo generado: Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Se verifica la ruta en la que se generò :   
Captura de pantalla de computadora

Descripción generada automáticamente

Se requiere adicionar la llave privada a git, para esto se requiere iniciar el agente ssh para poder realizar al validación de estas llaves, utiliza el comando:

eval $(ssh-agent -s)

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Luego se utiliza el símbolo ~ , este es el usado para poder ingresar nuevamente a HOME (donde está la ruta .ssh).

Se debe adicionar ahora la llave privada, por lo que se va a utilizar lo siguiente comando:

ssh-add ruta-donde-guardaste-tu-llave-privada

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente