

vamos a ver como conectar a otro usuario sin necesidad de contraseña, nos podemos conectar con criptografía asimétrica

clave pública y clave privada, esto sirve para crear un script que se conecte y haga todo lo que nosotros necesitamos, copiar, leer, mover, borrar, editar, ejecutar, etc

Clave simétrica: se abre con misma clave, usuario envía archivo a usuario 2 y este debe utilizar misma contraseña

En la asimétrica existen 2 claves, 1 por cada interviniente.. La clave pública que la podemos compartir con todo el mundo y la clave privada que jamás la debemos compartir con nadie, esta es la llave para descifrar

esto sirve también para identificarnos en los sistemas

para crear las claves: desde la terminal con el comando ssh-keygen  
luego pregunta dónde guardar las claves, lo tiene en un lugar por defecto o podemos cambiar la ubicación, además podemos poner una contraseña para que si alguien me roba la clave privada necesita esa contraseña para poder utilizarlas.

crea 2 archivos id\_rsa.pub que es el archivo público y el archivo de clave privada

usaremos un hosting en este caso digitalocean, ahí también podremos ver todo esto de ssh y el fichero de autorice keys.

en el server introducimos nuestra clave pública para que yo me pueda conectar desde mi pc sin tener la contraseña

conexión método tradicional ej:

ssh usuario@server@192.168.1.149  
y pide contraseña y listo estoy en máquina remota

ahora ssh-keygen

vamos a home/home/usuario.ssh/ y vemos los ficheros

el fichero está vacío y podemos abrir con nano y metemos todas las claves publicas ssh que queramos que se conecten al servidor