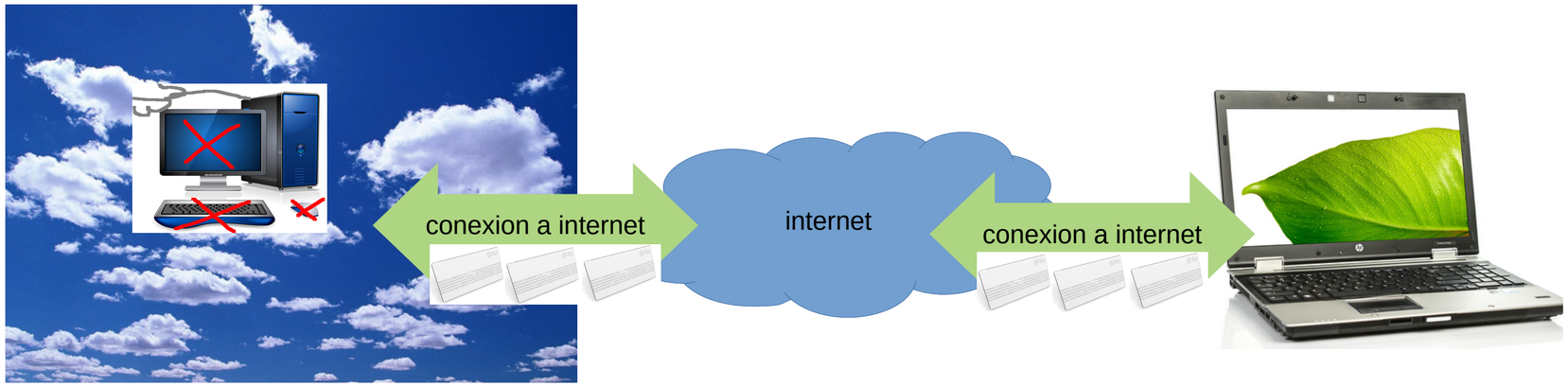
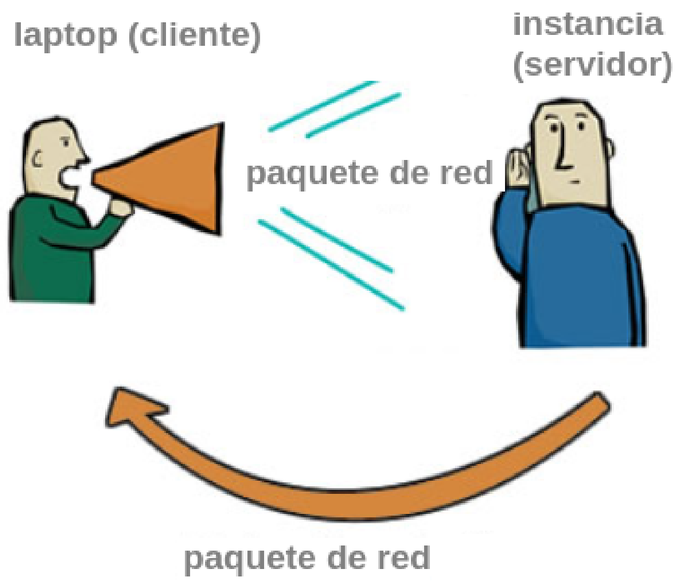
#1 tienes una instancia (un computador) en la nube, y tu laptop en la casa y quieres comunicarlos con un canal privado.



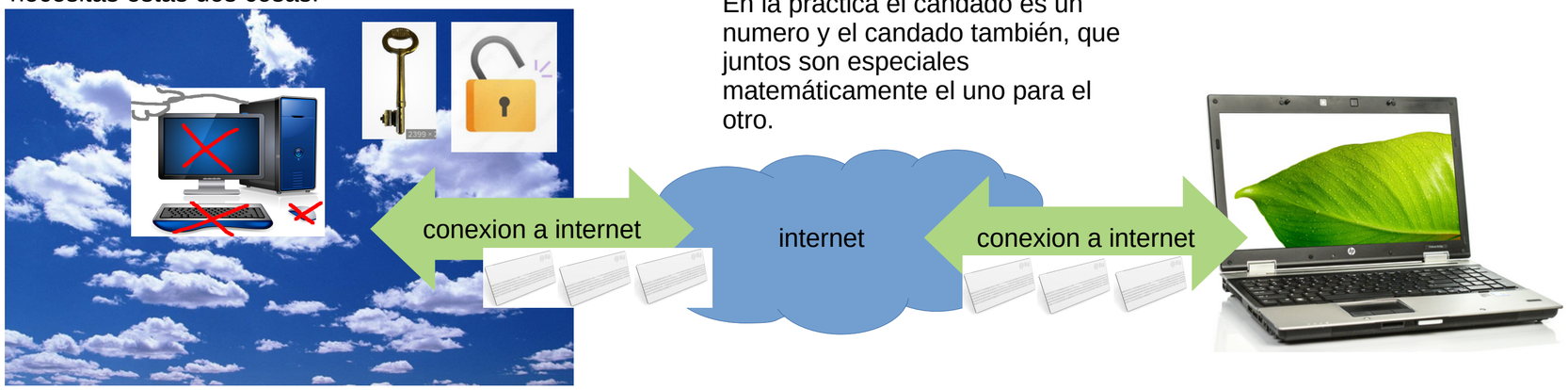


#2: Generas unas llaves (publica y privada), para esto necesitas un computador, que puede ser culaquiera de los dos u otro computador, el caso es que necesitas estas dos cosas.

En nuestro caso las generamos en el computador que esta en la nube, porque es el unico que tiene debian y está funcionando en el momento.

Estas llaves se generaron con un software que se llama OpenSSH, que tambien está en windows. Pero es más facil hacerlo en Linux.

En la práctica el candado es un numero y el candado también, que juntos son especiales matemáticamente el uno para el otro.



#3 Dejas la llave en el computador (llave publica) que está en la nube, y dejas el candado (llave privada) en la laptop.

Recuerda la analogia. La comunicacion entre el laptop y el pc de la nube deberá ser secreta, si no cualquier persona de internet podría interceptar la comunicacion y hacerse pasar por ti. Con este esquema el mensaje que se envie desde el laptop va estar asegurado con el candado cerrado (es decir cifrado, porque en la practica cada paquete de red se combina con uno de los numeros que generaste en el paso anterior, es decir la llave privada); así que mientras llegue a la nube, podrá ser interceptado pero nunca se podrá decifrar. Para saber su contenido, el pc de la nube combinara su numero (la llave publica) con el mensaje que esta sellado (cifrado) y matematicamente el mensaje se revela.