1. Cifrado de información



2. Cifrado simétrico y asimétrico (o de llave pública y privada)





# 3. Protocolo de línea de comandos seguro :: Secure SHell (SSH)



### Llave privada: id\_rsa

Llave pública: id\_rsa.pub

# 4. Generación de llaves (Windows $\rightarrow$ Powershell; Linux y Mac $\rightarrow$ Shell)

C:\Windows\system32>ssh-keygen -b 2048 -t rsa

Y presionar tres veces la tecla Enter.

Generating public/private rsa key pair. Enter file in which to save the key (C:\Users\Sergio/.ssh/id_rsa Enter passphrase (empty for no passphrase): Enter same passphrase again: Your identification has been saved in C:\Users\Sergio/.ssh/id_rsa.pu Your public key has been saved in C:\Users\Sergio/.ssh/id_rsa.pu The key fingerprint is: SHA256:5bGGGVZG8nYQMu03q7mnEHaqcD4khTjrVLL04qPtmc sergio@Sergio The key's randomart image is: +[RSA 2048]+   .+B   +o+*   * oo   o . B.o   .+ S =   +o. + +   +=o . + .   +=se   +*+o= +[SHA256]+ PS C:\Users\Sergio> dir C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh		rgio> ssh-key	<b>ygen</b> -b 2048	-t rsa	
<pre>Enter file in which to save the key (C:\Users\Sergio/.ssh/id_rsa Enter passphrase (empty for no passphrase): Enter same passphrase again: Your identification has been saved in C:\Users\Sergio/.ssh/id_rsa Your public key has been saved in C:\Users\Sergio/.ssh/id_rsa.pu The key fingerprint is: SHA256:5bGGGVZYG8nYQMu03q7mnEHaqcD4khTjrVLL04qPtmc sergio@Sergio The key's randomart image is: +[RSA 2048]+   .+B   + tot+*   + t</pre>	ating pub.	lic/private r	rsa key pair.		
Enter passphrase (empty for no passphrase): Enter same passphrase again: Your identification has been saved in C:\Users\Sergio/.ssh/id_rsa.pu The key fingerprint is: SHA256:5bGGGVZYG8nYQMu03q7mnEHaqcD4khTjrVLL04qPtmc sergio@Sergid The key's randomart image is: +[RSA 2048]+   .+B   +o+*   * oo   0 . B.0   .+ S =   +o. + +   +.=o. + .   .+BE o.+ ++*+o= +[SHA256]+ PS C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh	file in u	which to save	e the key (C:	:\Users\Ser	gio/.ssh/id_rsa):
Enter same passphrase again: Your identification has been saved in C:\Users\Sergio/.ssh/id_rs Your public key has been saved in C:\Users\Sergio/.ssh/id_rsa.pu The key fingerprint is: SHA256:5bGGGVZYG8nYQMu03q7mnEHaqcD4khTjrVLL04qPtmc sergio@Sergio The key's randomart image is: +[RSA 2048]+   .+B   +o+*   +o+*   * oo   0 . B.o   1.+ S =   +o. + +   +.=o. + .   1.+BE o.+ H+**+o= +[SHA256]+ PS C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh	passphra	se (empty for	r no passphra	ase):	
<pre>Your identification has been saved in C:\Users\Sergio/.ssh/id_rs Your public key has been saved in C:\Users\Sergio/.ssh/id_rsa.pu The key fingerprint is: SHA256:5bGGGVzYG8nYQMu03q7mnEHaqcD4khTjrVLL04qPtmc sergio@Sergic The key's randomart image is: +[RSA 2048]+   .+B   +oo+*     * oo     o . B.o     .+ S =     +o. + +     +.=o. + .    .+BE o.+   ++*+o= +[SHA256]+ PS C:\Users\Sergio&gt; dir C:\Users\Sergio\.ssh</pre>	same pas	sphrase agair	n:		
<pre>Your public key has been saved in C:\Users\Sergio/.ssh/id_rsa.pu The key fingerprint is: SHA256:5bGGGVzYG8nYQMu03q7mnEHaqcD4khTjrVLL04qPtmc sergio@Sergic The key's randomart image is: +[RSA 2048]+   .+B   +-o+*   + * oo  </pre>	identific	ation has bee	en saved in (	C:\Users\Se	rgio/.ssh/id_rsa.
The key fingerprint is: SHA256:5bGGGVzYG8nYQMu03q7mnEHaqcD4khTjrVLL04qPtmc sergio@Sergio The key's randomart image is: +[RSA 2048]+   .+B   .+B   .+b   * oo   o . B.o   .+ S =   +o. + +   +.=o. + .  .+BE o.+ +[SHA256]+ PS C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh	public ke	y has been sa	aved in C:\Us	sers\Sergio,	/.ssh/id_rsa.pub.
SHA256:5bGGGVzYG8nYQMu03q7mnEHaqcD4khTjrVLL04qPtmc sergio@Sergic The key's randomart image is: +[RSA 2048]+   .+B   +o+*   * * * * *   * * * *   * * *   * * * + * * * + * * + * * + * * - * S C:\Users\Sergio> dir C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh	ey finger	print is:			
The key's randomart image is: +[RSA 2048]+   .+B   +o+*   * oo   o . B.o   . + S =   +o. + +   +.=o. + .   .+BE o.+   .+BE o.+   ++*+o= +[SHA256]+ PS C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh	6:5bGGGVz	YG8nYQMu03q7n	nnEHaqcD4khT	jrVLL04qPtmo	c sergio@SergioOptiplex70
<pre>+[RSA 2048]+   .+B   +-0+*   * 00   0 . B.0   .+ S =   +0. ++    +.=0. +.    .+BE 0.+    ++*+0= ++[SHA256]+ PS C:\Users\Sergio&gt; dir C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh</pre>	ey's rand	omart image i	is:		
<pre>.+B +o+* * oo 0 . B.o .+ S = ++o. + + +.=o. + . !+BE o.+ !+**o= +[SHA256]+ PS C:\Users\Sergio&gt; dir C:\Users\Sergio\.ssh</pre>	RSA 2048]	+			
+o+* * oo 0 . B.o . + S = +o. + + +.=o. + . .+BE o.+ ++*+o= +[SHA256]+ PS C:\Users\Sergio> dir C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh	.+B				
* oo   o . B.o   . + S =   +o. + +   +.=o. + .  .+BE o.+  ++*+o= +[SHA256]+ PS C:\Users\Sergio> dir C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh	+0+*	i ļ			
o . B.o   . + S =   +o. + +   +.=o. + .  .+BE o.+ ++*+o= +[SHA256]+ PS C:\Users\Sergio> dir C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh	* 00	i ļ			
. + S =     +0. + +     +.=0. + .    .+BE 0.+    ++*+. 0=   +[SHA256]+ PS C:\Users\Sergio> dir C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh	. B.o	i ļ			
+o. + +   +.=o. + .  .+BE o.+  ++*+o= +[SHA256]+ PS C:\Users\Sergio> dir C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh	- S =				
+.=o . + .    .+BE o.+   ++*+o= +[SHA256]+ PS C:\Users\Sergio> dir C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh	. + +				
.+BE o.+    ++*+o=   +[SHA256]+ PS C:\Users\Sergio> dir C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh	0.+.				
++*+o=   +[SHA256]+ PS C:\Users\Sergio> dir C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh	0.+				
+[SHA256]+ PS C:\Users\Sergio> dir C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh	<u> </u>				
PS C:\Users\Sergio> dir C:\Users\Sergio\.ssh Directorio: C:\Users\Sergio\.ssh	0=	+			
Directorio: C:\Users\Sergio\.ssh	[SHA256]-				
Mada LastWaitaTima Langth Nama	[SHA256]- \Users\Se	rgio> dir C:\	\Users\Sergio	o∖.ssh	
	[SHA256]- \Users\Se	rgio> dir C:\ : C:\Users\Se	\Users\Sergio ergio\.ssh	o∖.ssh	Namo
-a 04/04/2024 16:23 1831 id_rsa	[SHA256]- \Users\Se	rgio> dir C:\ : C:\Users\Se LastWr 	\Users\Sergio ergio\.ssh riteTime	o\.ssh Length <u></u>	Name 
-a 04/04/2024 16:23 408 id_rsa.pub	u- [SHA256]- \Users\Se	rgio> dir C:\ : C:\Users\Se LastWr  04/04/2024	\Users\Sergio ergio\.ssh riteTime  16:23	⊳\.ssh Length  18 <u>31</u>	Name  id_rsa
	SHA256]- \Users\Se Pirectorio	rgio> dir C:\ : C:\Users\Se LastWr 94/04/2024 94/04/2024	\Users\Sergio ergio\.ssh riteTime 16:23 16:23	Length  1831 408	Name  id_rsa id_rsa.pub

5. Conexión al servidor y creación del directorio de llaves:

PS C:\Users\Sergio>ssh stinoco@132.248.172.201 -p10022
stinoco@nodo1:~\$mkdir .ssh
stinoco@nodo1:~\$exit

## Copiar llave pública al servidor

```
PS C:\Users\Sergio>scp -P 10022 C:\Users\Sergio\.ssh\id_rsa.pub
stinoco@132.248.172.201:/home/stinoco/.ssh/
```

🜌 stinoco@nodo1: ~	
PS C:\Users\Sergio> <mark>scp</mark> -P 10022 C:\Users\Sergio\.ssh\id_rsa.pub	<pre>stinoco@132.248.172.201:/home/stinoco/.ssh/</pre>
stinoco@132.248.172.201's password:	
id_rsa.pub	100% 408
PS C:\Users\Sergio> ssh stinoco@132.248.172.201 -p10022	

### 6. Anexar la llave pública al archivo **authorized keys** en el servidor

PS C:\Users\Sergio>ssh stinoco@132.248.172.201 -p10022

stinoco@nodo1:~\$ls .ssh

stinoco@nodo1:~\$cd .ssh

stinoco@nodo1:~/.ssh\$cat id rsa.pub >> authorized keys

stinoco@nodo1:~/.ssh\$cat authorized keys

stinoco@nodo1:~/.ssh\$exit

# stinoco@nodol:-/.sh stinoco@nodol:-/s ls .ssh id\_rsa.pub stinoco@nodol:-/ cd .ssh stinoco@nodol:-/.ssh\$ cat id\_rsa.pub >> authorized\_keys stinoco@nodol:-/.ssh\$ cat authorized\_keys ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDH7NscofDtRYSXbx5KCN1fzTzxFoy8WjdeFdcfhqcDjVkLy2bdDoI11oJSFnv4gURUJZ8rddU8bvdCdKyietWNZ PoESPo6d03GzcnNqZ+ejG3voeWv6w9F2YKxaaqZ1Mvh0euDpoBIFwaMfNGJD6ZUOhsQjtTzZ0Z1IzsjjSCfCIF19Le90AaA7IViNaM8c5bNOWVOPwdWwY/Rp0mY/o jLY1BJxfpzg3znPbmX/eGMHtd7s1ybMz85qo+0J63xRXZdgnfX9bzuBV7WeWZxBCEw+TDsjMUxrBG2chmZX+JeLRA+YHGXTZWABUskyuvRGS4/PjqDqD/zLHxdIXj 6Pomj sergio@SergioOptiplex7050 stinoco@nodo1:-/.ssh\$ exit\_

MUY IMPORTANTE: No se les olvide <u>cambiar</u> las instrucciones para escribir su propio nombre de usuario (tanto en Powershell como en la terminal del servidor).

# 7. Descargar el instalador de Anaconda Python

PS C:\Users\Sergio>ssh stinoco@132.248.172.201 -p10022

stinoco@nodo1:~\$wget https://repo.anaconda.com/archive/Anaconda3-2024.02-1-Linuxx86 64.sh

stinoco@nodo1:~\$chmod +x Anaconda3-2024.02-1-Linux-x86\_64.sh

stinoco@nodo1:~\$ls

stinoco@nodo1:~\$ ./Anaconda3-2024.02-1-Linux-x86\_64.sh

🔎 stinoco@nodo1: ~ 🚽		×
<pre>stinoco@nodo1:~/.ssh\$ cd stinoco@nodo1:~\$ wget https://repo.anaconda.com/archive/Anaconda3-2024.02-1-Linux-x86_64. 2024-04-04 23:26:35 https://repo.anaconda.com/archive/Anaconda3-2024.02-1-Linux-x86_ Resolving repo.anaconda.com (repo.anaconda.com) 104.16.130.3, 104.16.131.3, 2606:4700: :8303, Connecting to repo.anaconda.com (repo.anaconda.com) 104.16.130.3 :443 connected. HTTP request sent, awaiting response 200 OK</pre>	sh _64.s :681	h .0
Length: 1045673900 (997M) [application/octet-stream]		
Saving to: 'Anaconda3-2024.02-1-Linux-x86_64.sh' Anaconda3-2024.02-1-Lin 100%[=======================>] 997.23M 29.7MB/s in 30s		
2024-04-04 23:27:06 (32.9 MB/s) - 'Anaconda3-2024.02-1-Linux-x86_64.sh' saved [1045673900 673900]	)/104	5
stinoco@nodo1:~\$ chmod +x Anaconda3-2024.02-1-Linux-x86_64.sh stinoco@nodo1:~\$ ls		
Anaconda3-2024.02-1-Linux-x86_64.sh		
stinoco@nodo1:~\$ ./Anaconda3-2024.02-1-Linux-x86_64.sh		

⇒ **Nota.-** El último comando ejecuta el instalador de Anaconda Python.