Exemplo 4. Conexión SSH sen contrasinal

Exemplo 4. Conexión SSH sen contrasinal

ESCENARIO: Servidor SSH configurado do seguinte xeito (ver a seguinte ligazón: Exemplo1 para configurar un Servidor SSH):

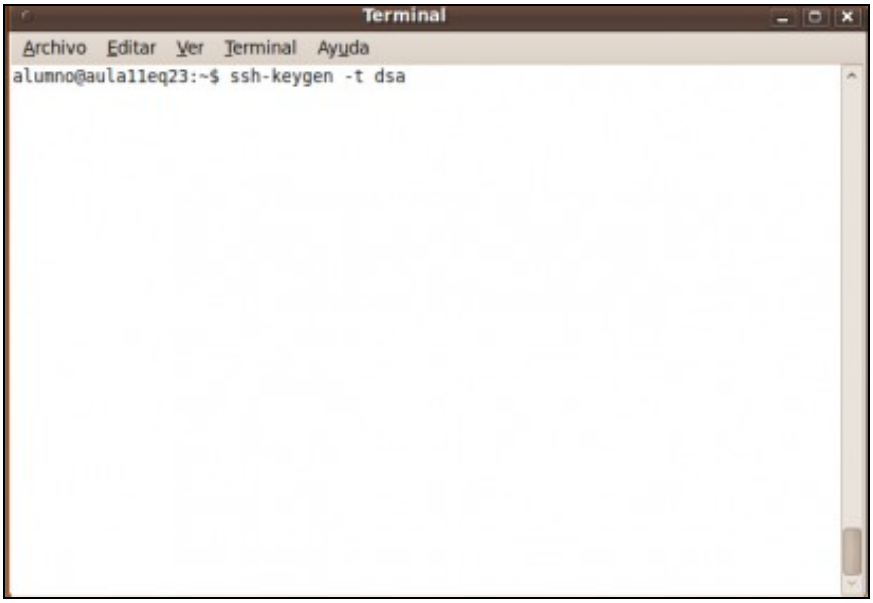
1. **IP/MS: 192.168.120.100/24**
2. **Porto conexión: 22**
3. **Usuario/Contrasinal da conexión: root/toor**

Configuración do Cliente da Conexión SSH

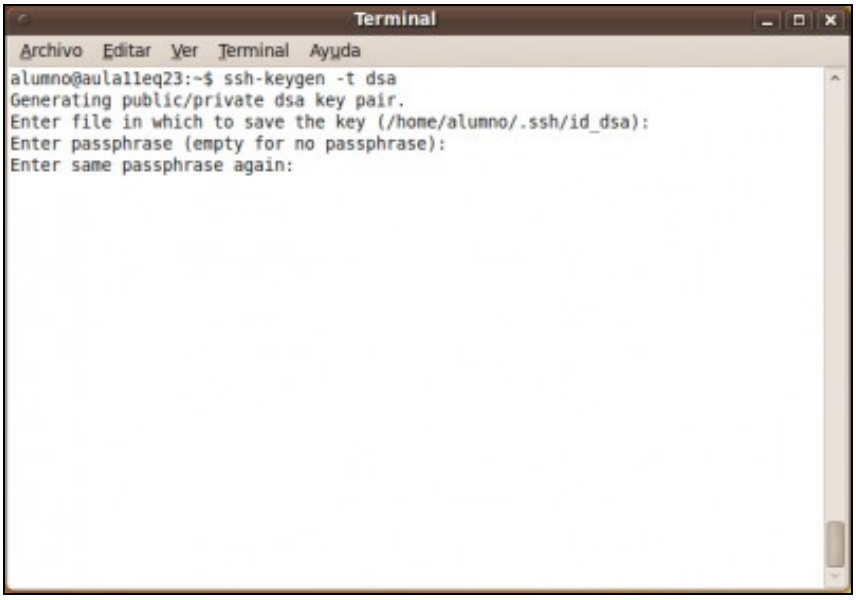
Para poder conectar mediante SSH sen contrasinal debemos crear certificados: chave pública e chave privada. Así:

1. O certificado de **chave pública** é o que debe posuir o **Servidor SSH**
2. O certificado de **chave privada** é o que debe posuir o **Cliente da conexión SSH**.

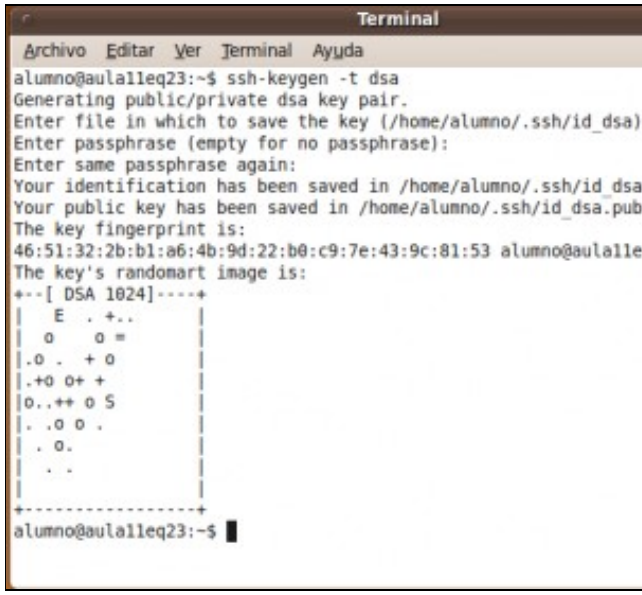
Proceder do seguinte xeito:



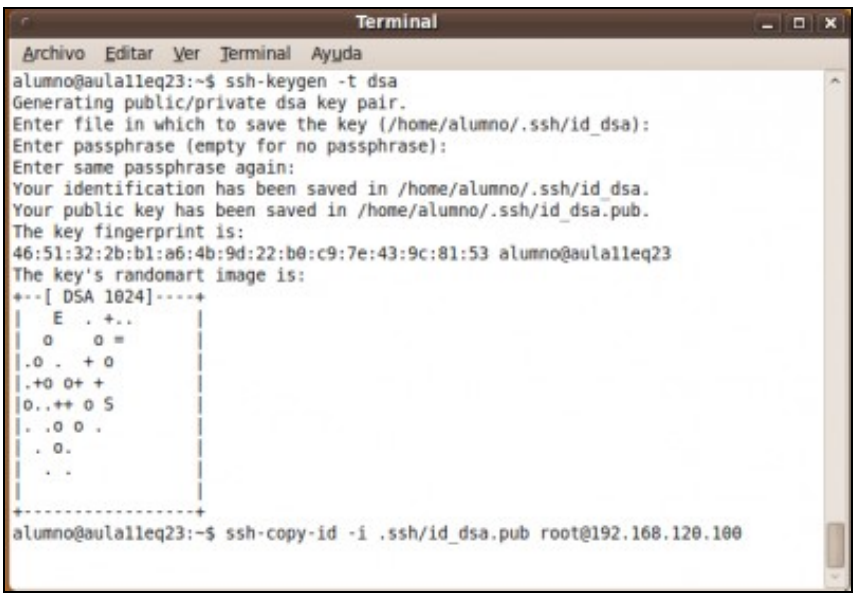
a. Crear un par de chaves: pública e privada.
No comando emprégase o algoritmo de cifrado **dsa (Digital Signature Algorithm)**, que por defecto a non ser que o modifiquemos co parámetro **-b nº_bits** é de **1024bits**.



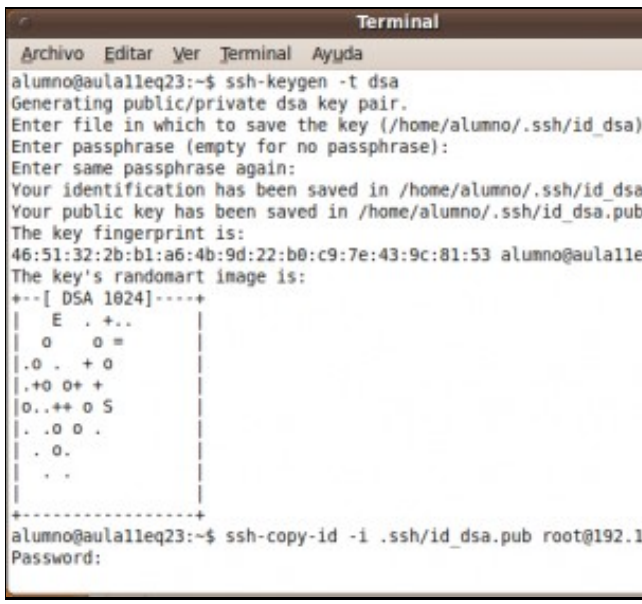
b. Elixir o cartafol onde gardar as chaves.
Pulsamos **Enter** para deixar por defecto o cartafol **.ssh/id_sda** den
usuario: **/home/alumno**



c. Passphrase nulo. Se aquí pomos un contrasinal, frase ou similar, cando queiramos conectarnos ao **Servidor SSH** en vez de pedir o contrasinal do usuario da conexión pedirá iste **passphrase**, mais como cando queremos conectarnos queremos facelo de forma directa sen petición de contrasinal ou passphrase, entón **pulsamos 2 veces Enter** para que a conexión se faga sen contrasinal.



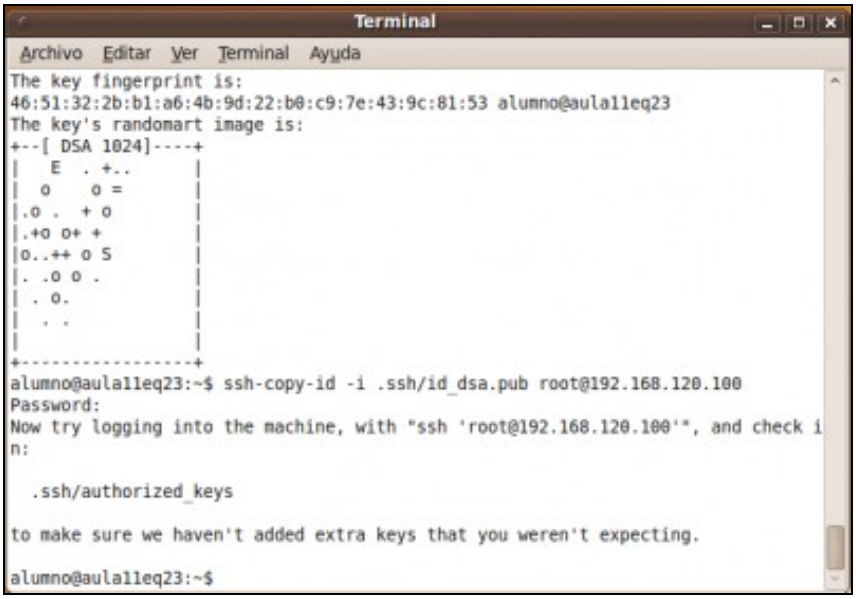
d. Chave pública e privada creadas. Fingerprint. Creáronse no c
indicado (ver imaxe **b.**) a **chave privada id_dsa** e a **chave pública**
Tamén creouse o **fingerprint da chave pública**, e dicir, a **identific**
chave pública correspondente ao usuario alumno do equipo cl



e. Copia da chave pública ao Servidor SSH. Para poder establecer a conexión sen contrasinal enviamos unha copia da chave pública ao Servidor SSH. Soamente será posible establecer unha conexión sen contrasinal se posuimos a parella desa chave pública, que non é outra que a chave privada, polo cal, nunca deberiamos desprendernos da chave privada, xa que sen ela a conexión non sería posible ou outro usuario podería suplantarnos no caso de facerse coa chave privada.

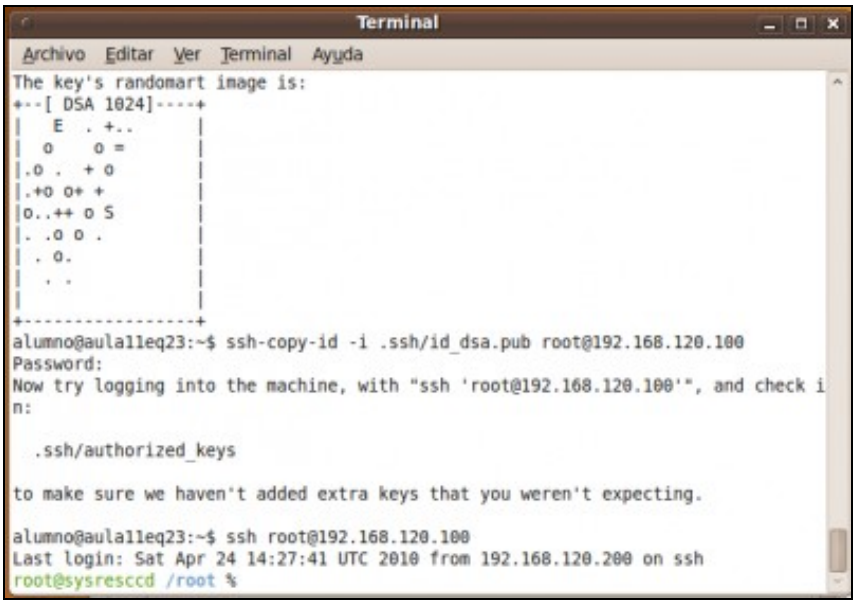
f. Password usuario root: toor. Como aínda non temos copiada a conexión pídese o contrasinal do usuario co cal queremos conectar root. A password de root é toor.

Agora a conexión sen contrasinal será posible por alumno na r sendo unha vez establecida o usuario root, con todos os permi na máquina Servidor SSH.



g. Chave pública copiada.

h. Conectando ao Servidor SSH.



i. Conexión establecida sen contrasinal

--ricardofc [26/04/10]