



Sistemas Operativos

Práctica

Lic. Exequiel Aramburu

aramburu.exequiel@uader.edu.ar



Agenda

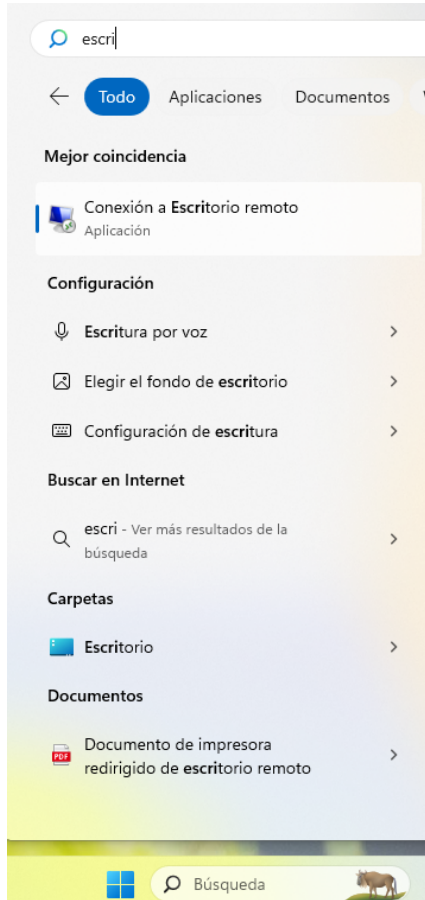
- **Presentación de la actividad extra aúlica clase anterior.**
- **Análisis de escritorio remoto Microsoft Windows – Cliente.**
- **Análisis de escritorio remoto Microsoft Windows - Servidor.**
- **Administración remota Telnet, SSH y SCP.**
- **Configuración SSH con usuario y contraseña.**
- **Configuración SSH con clave llaves.**
- **Prácticas de laboratorio.** Instalar OpenSsh y conectarse remotamente utilizando usuarios y contraseña

¿ Que herramientas de administración/acceso remoto existen?



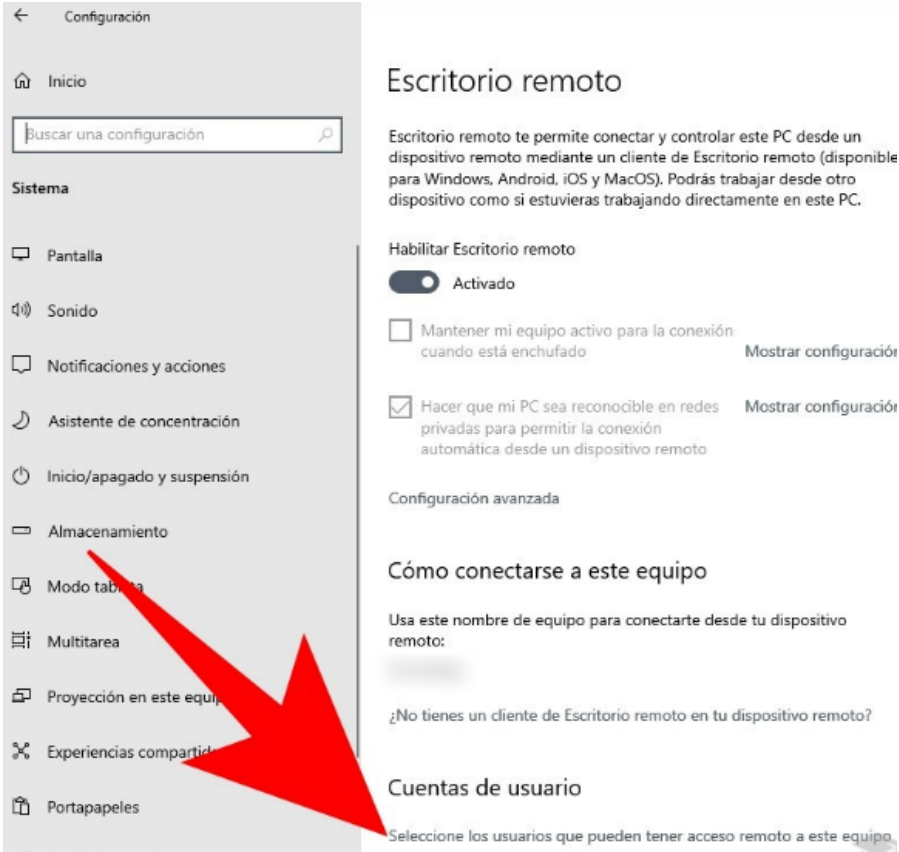
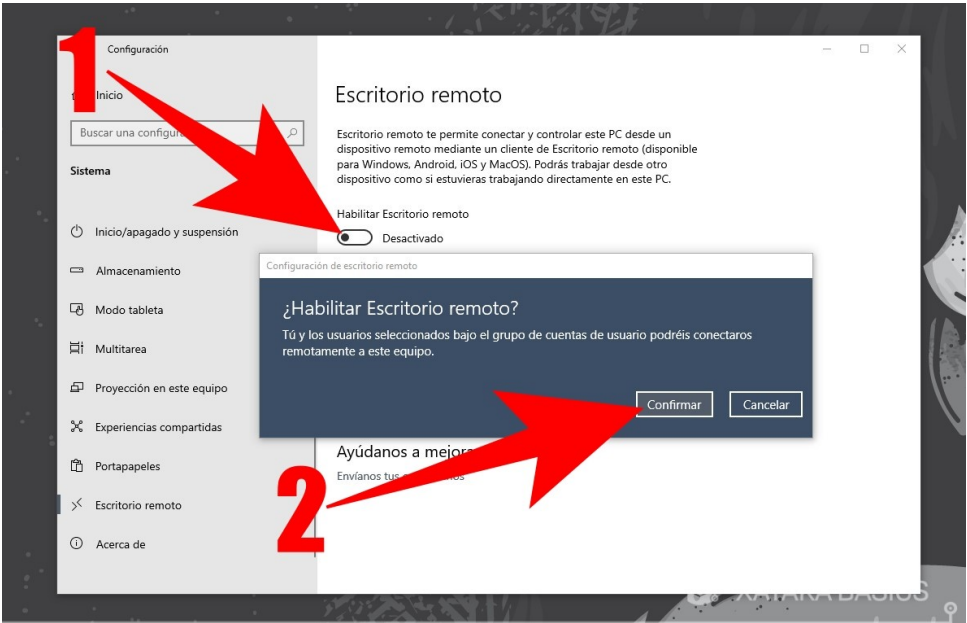
Escritorio Remoto – Microsoft Windows

CLIENTE



Escritorio Remoto – Microsoft Windows

SERVIDOR



Escritorio Remoto – Microsoft Windows

Administración de equipos

Archivo Acción Ver Ayuda

Administración del equipo (local)

- Herramientas del sistema
 - Programador de tareas
 - Visor de eventos
 - Carpetas compartidas
 - Usuarios y grupos locales
 - Usuarios
 - Grupos
 - Rendimiento
 - Administrador de dispositivos
- Almacenamiento
 - Administración de discos
- Servicios y Aplicaciones

Nombre	Descripción
Administradores	Los administradores tienen acces...
Administradores de Hyper-V	Los miembros de este grupo tiene...
Duplicadores	Pueden replicar archivos en un do...
IIS_IUSRS	Grupo integrado usado por Intern...
Invitados	De forma predeterminada, los invi...
Lectores del registro de eventos	Los miembros de este grupo pue...
Operadores criptográficos	Los miembros tienen autorización...
Operadores de asistencia de control de acceso	Los miembros de este grupo pue...
Operadores de configuración de red	Los miembros en este equipo pue...
Operadores de copia de seguridad	Los operadores de copia de seguri...
Propietarios del dispositivo	Los miembros de este grupo pue...
System Managed Accounts Group	Los miembros de este grupo los a...
Usuarios	Los usuarios no pueden hacer ca...
Usuarios avanzados	Los usuarios avanzados se incluye...
Usuarios COM distribuidos	Los miembros pueden iniciar, acti...
Usuarios de administración remota	Los miembros de este grupo pue...
Usuarios de escritorio remoto	A los miembros de este grupo se l...
Usuarios del monitor de sistema	Los miembros de este grupo tiene...
Usuarios del registro de rendimiento	Los miembros de este grupo pue...

Propiedades: Usuarios de escritorio remoto

General

Usuarios de escritorio remoto

Descripción: A los miembros de este grupo se les concede el derecho de

Miembros:

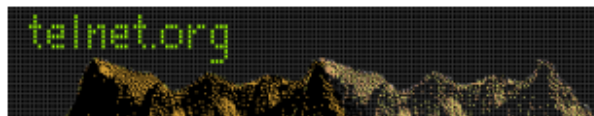
Agregar... Quitar

Cualquier cambio en la pertenencia a grupos de usuarios no surtirá efecto hasta que el usuario inicie sesión de nuevo.

Aceptar Cancelar Aplicar Ayuda

Debate

¿Cuántos usuarios se pueden conectar simultáneamente por escritorio remoto en Microsoft Windows?



→ **telnet**
1969



→ 1995



Cliente

Transmisión
Usuario: gugler
Password: uader



Servidor

Otras herramientas: rlogin, lsh , nsh , slush , etc ..

Instalación de OpenSSH:

SERVIDOR



`apt-get install openssh-server`

CLIENTE



`apt-get install openssh-client`

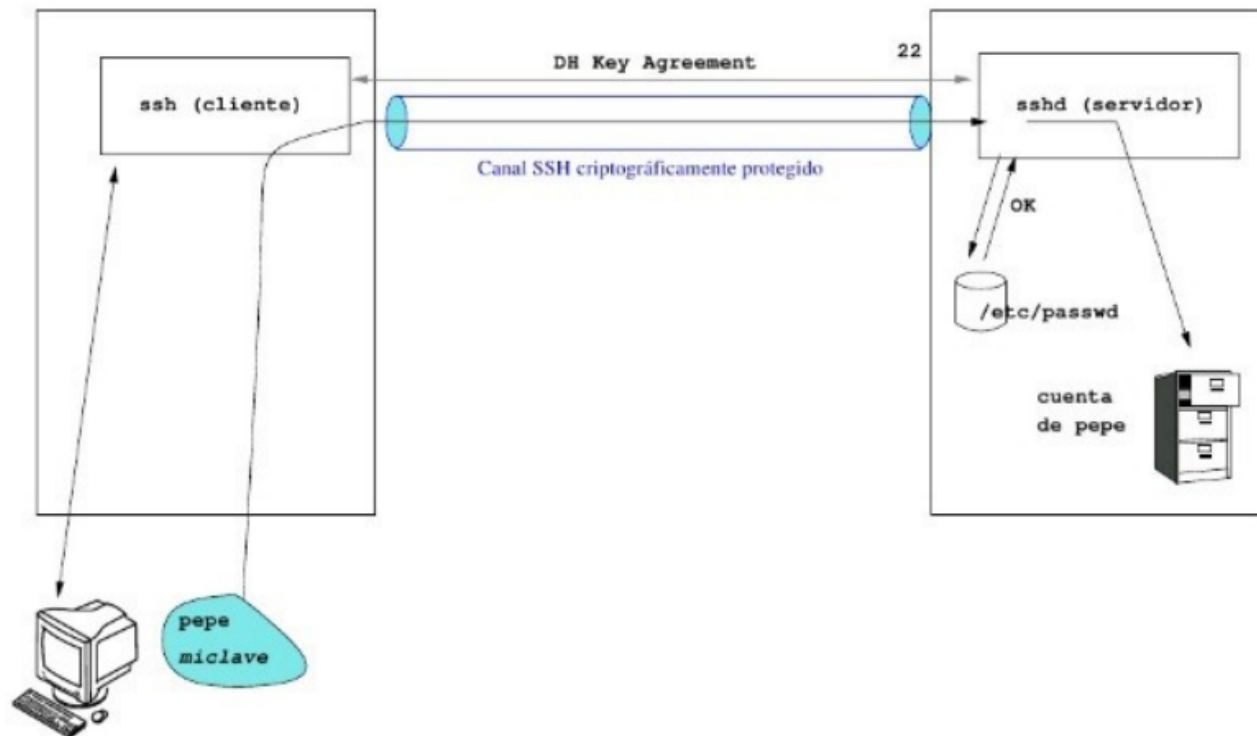
Configuración básica:



SERVIDOR

- Cambiar el puerto por defecto.
- Selección la versión 2 del protocolo.
- Autenticar mediante Login y Password.
- Permitir ciertos usuarios.
- Configurar las direcciones IP donde escucha el servicio.
- No permitir el acceso como root.
- Tiempo de espera del login.
- Cantidad de intentos erróneos permitidos.
- Máxima cantidad de conexiones.
- Introducir un banner

Autenticación por contraseña



Configuración de OpenSSH:

Archivo de configuración
del Servidor



/etc/ssh/sshd_config

Port 22
ListenAddress 0.0.0.0
Protocol 1,2
LoginGraceTime 120
PermitRootLogin yes
MaxAuthTries 10
MaxStartups 3
AllowUsers: gugler



Port 22000
ListenAddress 192.168.1.10
Protocol 2
LoginGraceTime 30
PermitRootLogin no
MaxAuthTries 2
MaxStartups 1
AllowUsers: gugler@IP
AllowUsers sergio@192.168.0.*

Banner /etc/ssh/mibanner

Herramientas:

ssh → Acceso remoto a otra máquina

scp → Transferencia segura de archivos en equipos

Trabajar con llaves:

ssh-keygen → Inspeccionar y generar claves RSA y DSA

ssh-agent
ssh-add } Herramientas para autenticarse de manera mas comoda

ssh-keyscan
ssh-vulnkey } Escanea una lista de clientes Y recolecta sus claves públicas

ssh (cliente OpenSSH):

Archivo de configuración
del Cliente



/etc/ssh/ssh_config

```
ssh (opciones) usuario@direccion
```

↑
-p *PORT*
-l *USUARIO*

↑
Usuario remoto

↑
Direccion IP o Nombre de Host
remota del servidor

scp (secure copy):

Copiar un archivo a un host remoto

```
scp (opciones) archivolocal usuario@direccion:/directorio/archivo_destino
```

↑
-P PORT

↑
remoto

Enviar

Copiar un archivo de un host remoto

```
scp (opciones) usuario@direccion:/directorio/archivo_destino archivo_local
```

↑
remoto

Traer

ssh (secure shell):

ssh gugler@192.168.56.102

```
gugler@debian1:/home$ ssh 192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established.
RSA key fingerprint is 7e:28:e3:aa:43:a1:dc:bb:67:81:11:dc:d8:bd:35:34.
Are you sure you want to continue connecting (yes/no)?
```



SERVIDOR
debian2

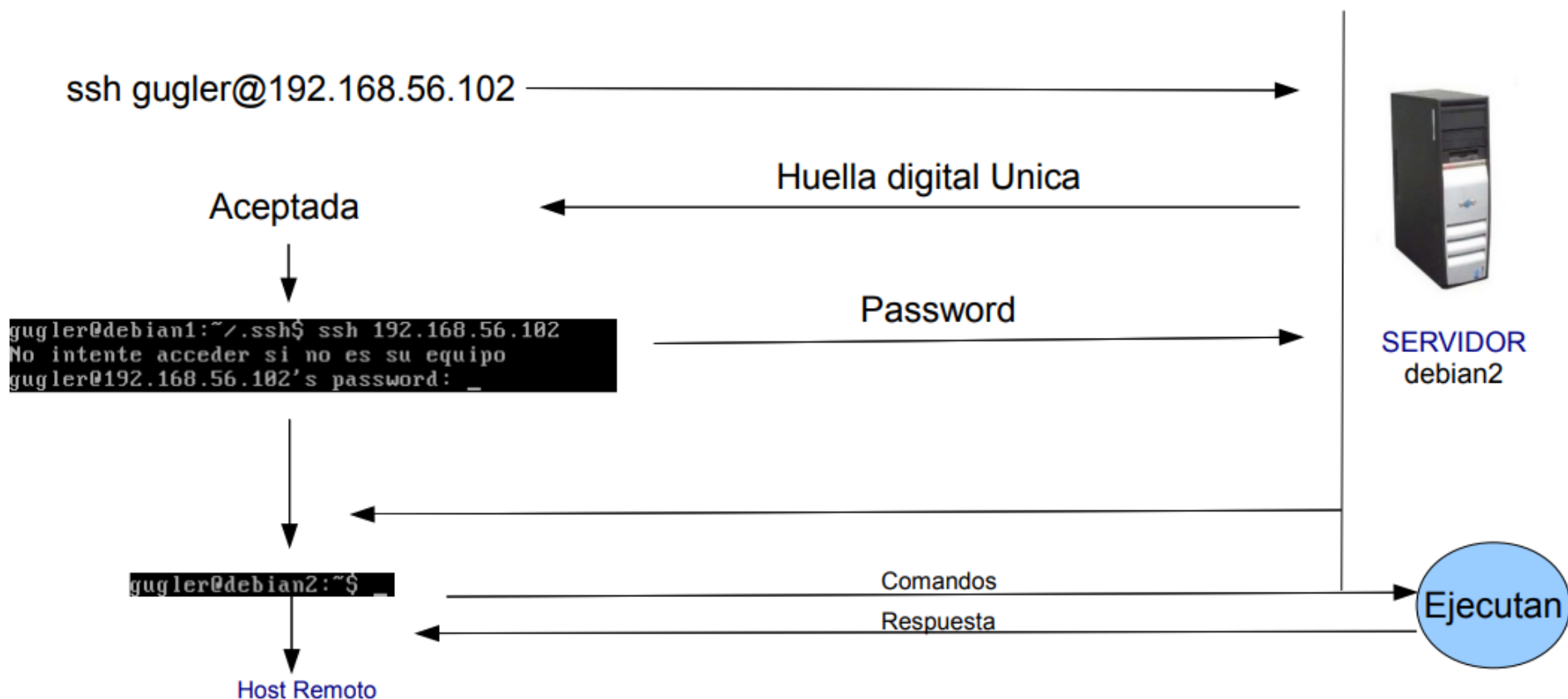
Huella digital Unica

yes

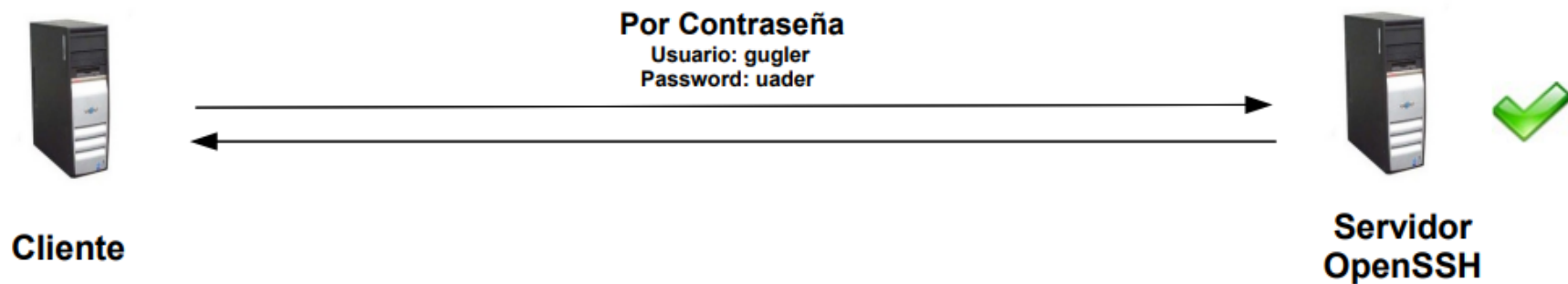
```
Warning: Permanently added '192.168.56.102' (RSA) to the list of known hosts.
```

* Se agrega de forma permanente al archivo known_host dentro de nuestra HOME/.ssh

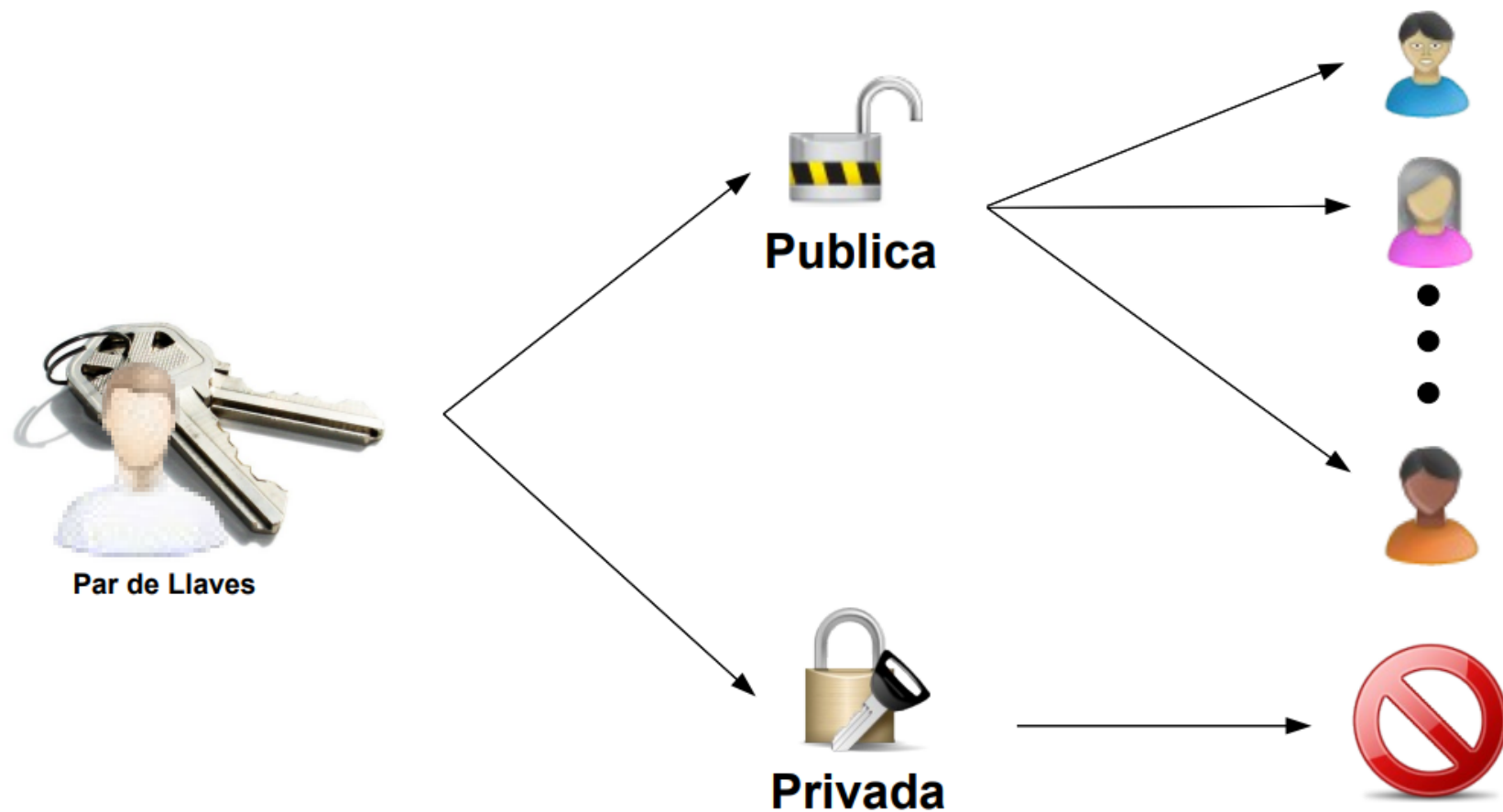
ssh (secure shell):



Metodos de autenticar usuarios:



Autenticar usuarios utilizando el algoritmo RSA y DSA:



Generando las llaves RSA(Rivest, Shamir y Adleman):



Par de Llaves
Cliente

```
ssh-keygen -t rsa -b (768- 2048- X)
```

```
Generating public/private rsa key pair.  
Enter file in which to save the key  
(/home/gugler/.ssh/id_rsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in  
/home/gugler/.ssh/id_rsa.  
Your public key has been saved in  
/home/sergio/.ssh/id_rsa.pub.  
The key fingerprint is:  
e7:0e:2e:d6:aa:90:6e:9b:ac:ad:7f:6f:1d:23:50:28  
gugler@cliente
```

Privada ←

Publica ←

Huella Digital



```
ssh-keygen -lf id_rsa.pub
```

```
e7:0e:2e:d6:aa:90:6e:9b:ac:ad:7f:6f:1d:23:50:28
```

Generando las llaves DSA(Algoritmo de Firma digital):



Par de Llaves
Cliente

```
ssh-keygen -t dsa -b 1024
```

```
Generating public/private dsa key pair.  
Enter file in which to save the key  
(/home/gugler/.ssh/id_dsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in  
/home/gugler/.ssh/id_dsa.  
Your public key has been saved in  
/home/sergio/.ssh/id_dsa.pub.  
The key fingerprint is:  
e7:0e:2e:d6:aa:90:6e:9b:ac:ad:7f:6f:1d:23:50:28  
gugler@cliente
```

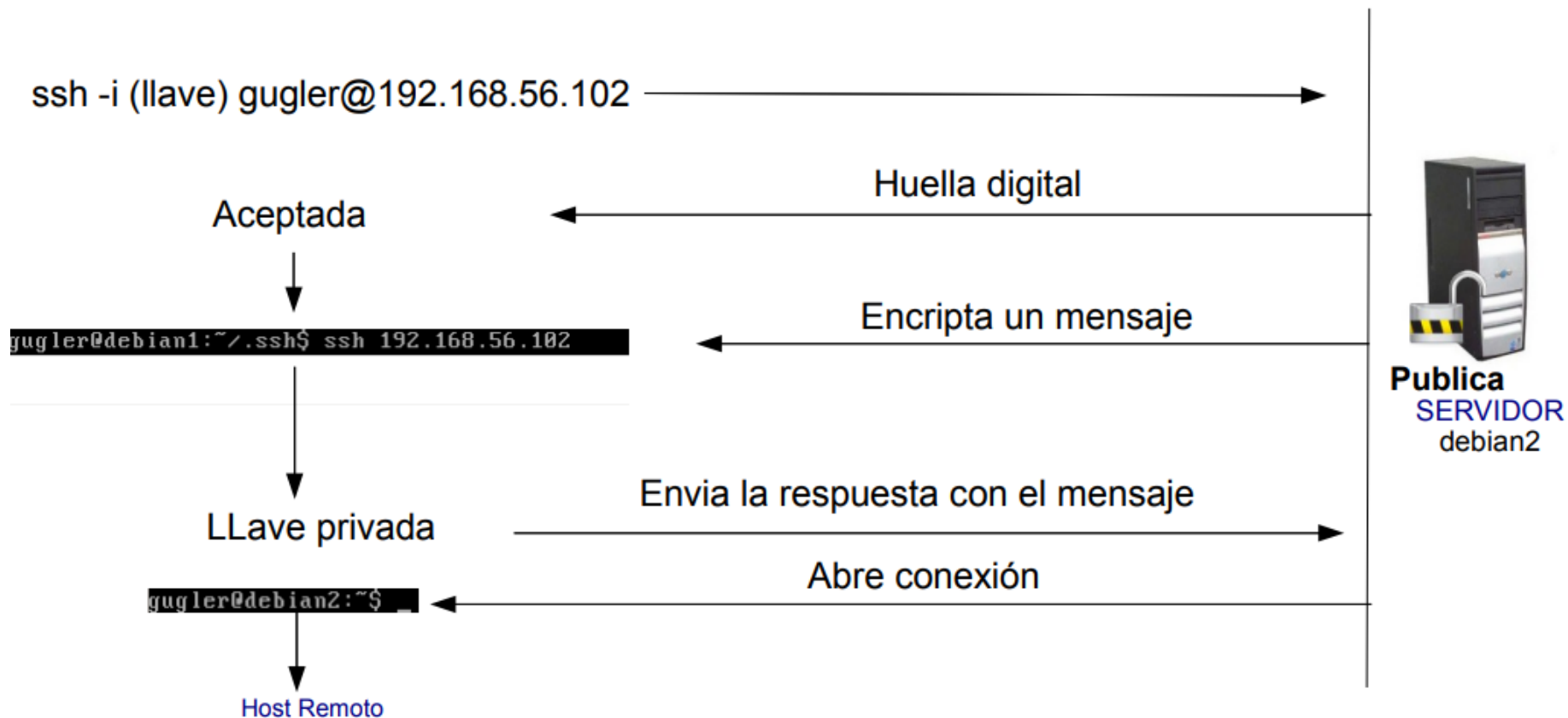
Privada ←

Publica ←

Huella Digital ← **ssh-keygen -lf id_dsa.pub**

```
e7:0e:2e:d6:aa:90:6e:9b:ac:ad:7f:6f:1d:23:50:28
```

ssh (secure shell):



Configuración de OpenSSH:

Archivo de configuración
del Servidor



/etc/ssh/sshd_config

```
Port 22000
ListenAddress 192.168.1.10
Protocol 2
LoginGraceTime 30
PermitRootLogin no
MaxAuthTries 2
MaxStartups 1
AllowUsers: gugler@IP
AllowUsers sergio@192.168.0.*

Banner /etc/ssh/mibanner
```

Ademas

```
hotkey /etc/ssh/ssh_host_dsa.key
hotkey /etc/ssh/ssh_host_dsa.key
PasswordAuthentication no
RSAAuthentication yes
PubkeyAuthentication yes
```

Práctica de laboratorio

1) Instalar OpenSSH.

`apt install ssh`

2) Conectase a una maquina de otro compañero en la misma red. (Solicitar la dirección IP al compañero).

`ssh 192.168.1.34@root`

3) Ejecutar el comando:

→ `eject`

→ `eject -t`