



FINTECH

Unità Formativa (UF): Linux Server

Docente: Wolfgang Cecchin

Titolo argomento: SSH (Secure Shell)



SSH (Secure Shell)

SSH è un servizio (ma anche un protocollo) che consente la comunicazione sicura via rete (sicura perché crittografata) tra un client e un server.

Attraverso SSH un utente può inviare comandi a un computer remoto.

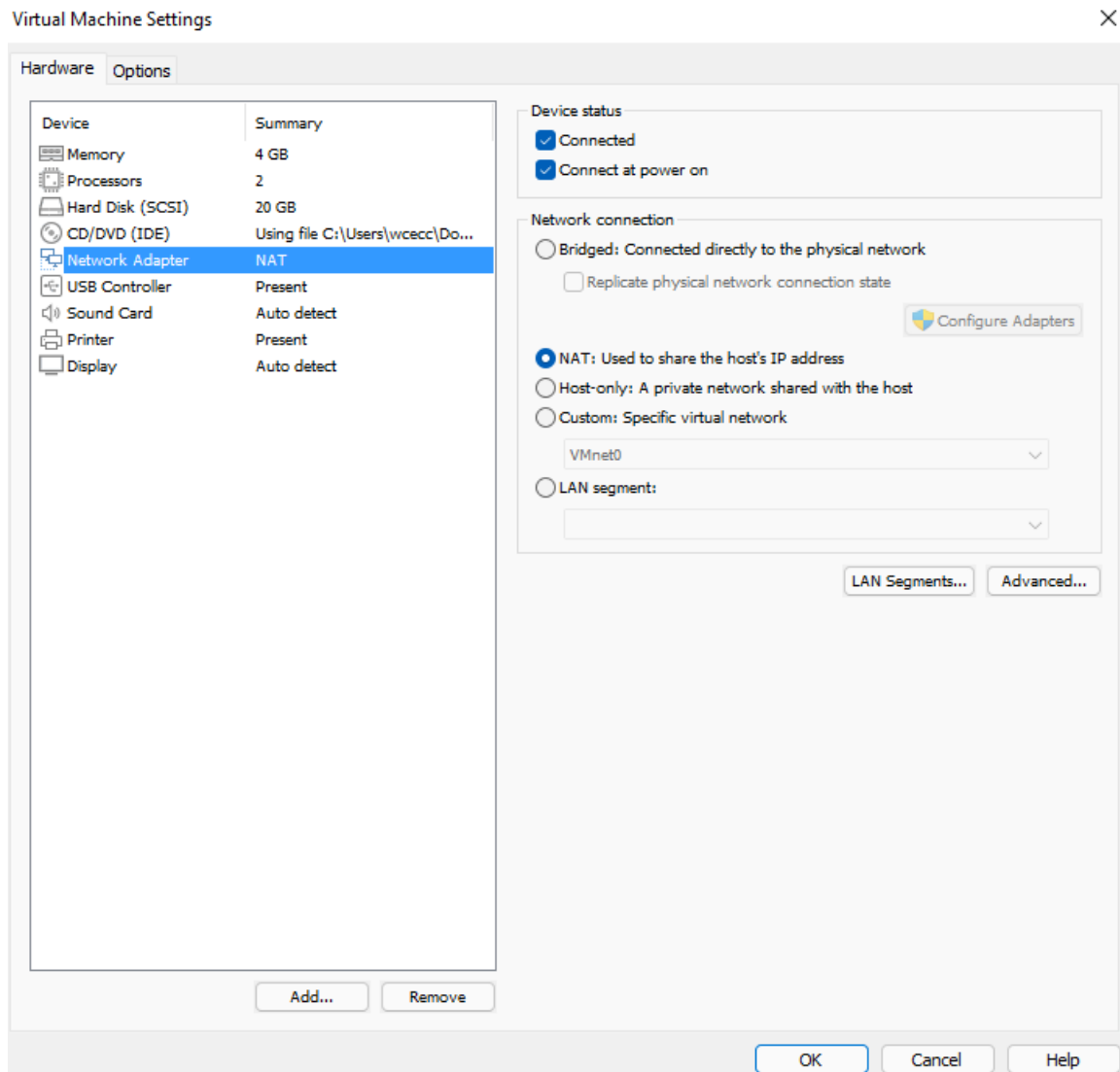
Precedentemente per collegarsi alle macchine si utilizzava Telnet: servizio che è stato abbandonato, perché la comunicazione tra client e server avveniva in chiaro.

Approfondimenti:

https://en.wikipedia.org/wiki/Secure_Shell

Utilizziamo VM Workstation in modalità “rete privata”

Per evitare di avere conflitti con altre macchine (e con la rete di ITS) utilizziamo VM Ware Workstation con NAT (“Network Address Translation”)



Installiamo su Debian il server SSH

Aggiorniamo i repositories:

```
$ sudo apt update
```

```
$ sudo apt install openssh-server
```

Controlliamo di avere installato:



\$ sudo systemctl status sshd

Controlliamo che sia in ascolto sulla porta 22:

\$ netstat -tulpn | grep 22

Impostiamo il server SSH perché parta all'avvio:

\$ sudo systemctl enable ssh

Nel caso in cui sia installato un firewall, dobbiamo consentire l'ingresso per ssh:

\$ sudo ufw allow ssh

Il file di configurazione di ssh si trova all'interno di /etc

Attenzione:

/etc/ssh_config → è il file di configurazione del client ssh del sistema

/etc/ssh_d_config → è il file di configurazione del server ssh

Invece:

/etc/ssh_config_d → è una directory. Vengono inclusi tutti i files di configurazione del client ssh del sistema

/etc/ssh_d_config_d → è una directory. Vengono inclusi tutti i files di configurazione del server ssh del sistema

A noi, se vogliamo modificare le configurazioni di ssh, interessa modificare il file:

/etc/ssh_d_config

Individuiamo l'IP della macchina

\$ hostname -I



Dalla macchina Windows (cioè la macchina host) possiamo utilizzare un client ssh per connettersi alla macchina:

```
$ ssh its-user@ip-della-macchina-guest
```

Crittografia simmetrica

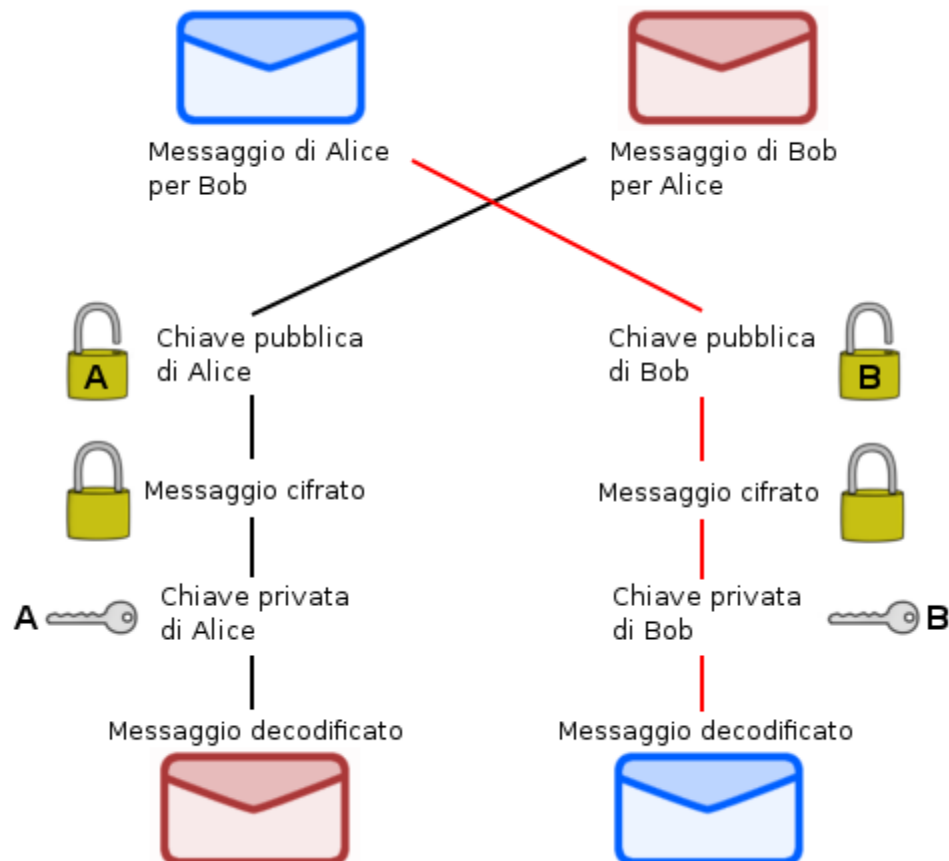
https://it.wikipedia.org/wiki/Crittografia_simmetrica





Crittografia asimmetrica

https://it.wikipedia.org/wiki/Crittografia_asimmetrica





Connessione tramite SSH

SSH utilizza **crittografia simmetrica** per crittografare la connessione tra client e server. La crittografia del canale in modalità asimmetrica sarebbe troppo onerosa (troppo lenta) a livello di calcolo.

Tuttavia **la fase di autenticazione** può avvenire attraverso crittografia asimmetrica e chiave pubblica.

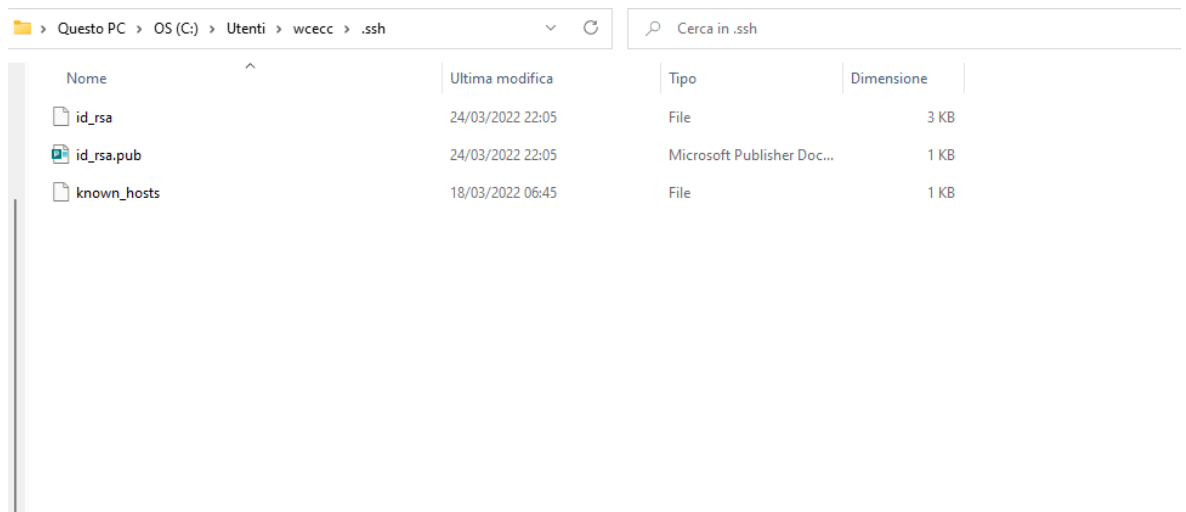
Nella powershell di Windows generiamo una coppia di chiavi pubblica/privata (non specificando nulla verrà usato l'algoritmo RSA):

```
> ssh-keygen
```

```
Windows PowerShell
PS C:\Users\wcecc> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\wcecc\.ssh\id_rsa):
```



Nella home dell'utente è stata creata una cartella `.ssh` con le chiavi pubbliche e private.



Questo PC > OS (C:) > Utenti > wcecc > .ssh		Cerca in .ssh	
Nome	Ultima modifica	Tipo	Dimensione
id_rsa	24/03/2022 22:05	File	3 KB
id_rsa.pub	24/03/2022 22:05	Microsoft Publisher Doc...	1 KB
known_hosts	18/03/2022 06:45	File	1 KB

In Debian andiamo a copiare la chiave pubblica nella cartella `/root/.ssh`

Ci sono molti modi per farlo, ad esempio da Windows:

```
> scp .\id_rsa.pub its-user@192.168.206.128:/home/its-user
> ssh its-user@192.168.206.128
```

E poi nella macchina Debian:

```
$ cat id_rsa.pub >> ~/.ssh/authorized_keys
```

Il contenuto del file **authorizes_keys** è una lista di chiavi pubbliche:

```
its-user@debian-its:~$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDQPxdoqEUYPE0cPcps3bkfnRXev+0o0pHTgBnnYbJaojRnNwBgv29080PTCyg
hiwe7JqRDl450Evt0qiRIrGE80eCvAC8JgPwtT/n84ZLeZ+jPBk9eaS6LPjbKSJbP3vfATdHyYsljaZ56pY03Uqjc4x/EaI8g6R
O/WcPnRpeUPbNJUXi95M8nSX947htv7reFHNJIEVPG0vLXZR0lpvfw3a7mSNFvA6TMpp7rrkUjWX00VLcf7UDqeYt+En+enTE
n d7hCy57ZKIZRF4ZeTSDENUAMdMuZiEcBkhS6dV6k6aH3Z0G6lN4qI9iNLI0H+T6ydEhTEyrlTi+A+WwTLXITiBErFwrgFbbsZeh
GfhNmoyIIa5TP07EmeN4vJqAQ+6jbZiudq2iYhSyggNdLLPCRP+kKjGXihDYVXV07aQdEMyTIikgTQE9miLsePGAMmLKzTpfyqv
VaBEJHS1x9MPdeu1iB/YXSIqc+wTfyul7B1j81o+ZPIJPgTaYuZMHKv0= wcecc@DESKTOP-0T330MQ
```