# ⚒ Connexió amb un servei SSH amb un parell de claus RSA

- [ ] Generació del certificat

Per a poder connectar amb un servei SSH sense introduir la contrasenya en establir la sessió d'usuari, hem de configurar l'autenticació amb clau pública/privada.

Si no tenim un parell de claus, podem fer servir la ferramenta ssh-keygen per a generar el nostre parell de claus:

```
user@host$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/profe/.ssh/id_rsa):
/home/profe/.ssh/prova-generacio-rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/profe/.ssh/prova-generacio-rsa
Your public key has been saved in /home/profe/.ssh/prova-generacio-rsa.pub
The key fingerprint is:
SHA256:z+ynwWds65K7qWWcgU6skVWhm1F8hDnt+u+mb4TdQQw profe@clearvictus
The key's randomart image is:
+---[RSA 3072]----+
|         .+*.Eo  |
|         += o  o |
|        +  +  .  |
|       + =  .  . |
|      o S .. o ..|
|       = *.+. o .|
|      . . @o=.   |
|         +o*o.o  |
|        ..*B+B+  |
+----[SHA256]-----+
```

Podem comprovar com hem generat el parell de claus al directori /home/profe/.ssh/

```
profe@clearvictus$ ls -la /home/profe/.ssh/
total 24
drwx------  2 profe profe 4096 Nov 13 19:37 .
drwxr-xr-x 11 profe profe 4096 Nov  2 14:43 ..
-rw-r--r--  1 profe profe 3330 Nov 13 08:20 known_hosts
-rw-------  1 profe profe 2602 Nov 13 19:37 prova-generacio-rsa
-rw-r--r--  1 profe profe  571 Nov 13 19:37 prova-generacio-rsa.pub
```

Al fitxer prova-generacio-rsa trobarem la clau privada generada, i al fitxer prova-generacio-rsa.pub trobarem la clau pública corresponent.

- [ ] Configuració de l'autenticació amb parell de claus RSA al servei SSH

Per a poder fer servir les claus generades per a connectar amb un servei SSH remot, haurem de copiar la clau pública al servidor remot, associant-la amb l'usuari remot desitjat.

Per exemple, si volem habilitar l'autenticació amb el parell de claus, al host 192.168.53.3 amb l'usuari 'alumne', haurem d'executar el següent comandament:

```
 profe@clearvictus$ ssh-copy-id -i /home/profe/.ssh/prova-generacio-rsa.pub
alumne@192.168.53.3
```

Si tot ha anat bé, haurem copiat la nostra clau pública, emmagatzemada al fitxer prova-generacio-rsa.pub del client, com a part del fitxer authorized_keys al servidor.

- [ ] Connexió del client al servidor, fent servir el parell de claus generades

Per a connectar al servidor amb el parell de claus, haurem d'indicar quin certificat hem de fer servir per autenticar-nos, i el servei ssh no ens demanarà contrasenya.

```
profe@clearvictus$ chmod 400 /home/profe/.ssh/prova-generacio-rsa
profe@clearvictus$ ssh -i /home/profe/.ssh/prova-generacio-rsa
alumne@192.168.53.3
```