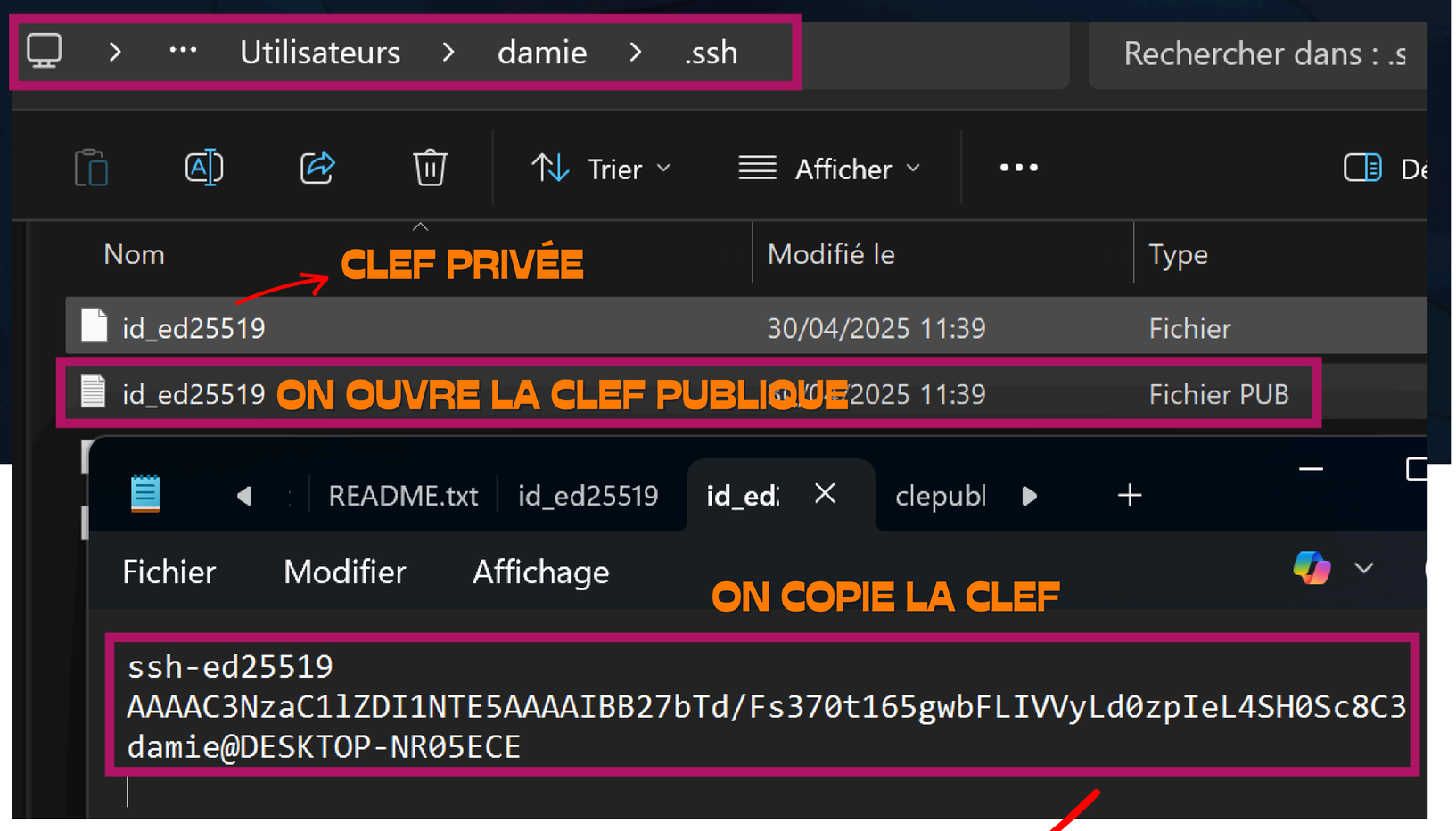
GENERATION SSH-KEY POWERSHELL

```
PS C:\Users\damie> ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:\Users\damie/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\damie/.ssh/id_ed25519
Your public key has been saved in C:\Users\damie/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:iU+ZSzr8aIQlgYNUqFnhn2/vM2/6Wd/KKrq7Dnu9rI4 damie@DESKTOP-NR05ECE
The key's randomart image is:
+--[ED25519 256]--+
|.o++             |
|.o+ .            |
|.o.. .           |
|o  ..... +       |
|     o+. S       |
|      .o.= .     |
|       .B o.  .  |
|       ..O+.+o o .|
|       .E=&&*o..+..|
+----[SHA256]-----+
```

ON GÉNÈRE UNE CLEF

BIEN RETENIR LE CHEMIN




```
PS C:\Users\damie> ssh damien@192.168.20.128
damien@192.168.20.128's password:
```

ON SE CONNECTE EN SSH AVEC LE MOT DE PASSE

```
damien@debian:~$ mkdir .ssh
```

ON CRÉE LE DOSSIER .SSH

ON CRÉE LE FICHIER CI-DESSOUS

```
damien@debian:~/.ssh$ nano authorized_keys
```

```
  GNU nano 7.2                                  authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBB27bTd/Fs370t165gwbFLIVVyLd0zpIeL4SH0Sc8C3 damie@DESKTOP-NR05ECE
```

ON COLLE NOTRE CLEF EN DEDANS

```
PS C:\Users\damie> ssh damien@192.168.20.128
Linux debian 6.1.0-34-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.135-1 (2025-04-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Apr 30 12:05:43 2025 from 192.168.20.1
```

DÉSORMAIS ON PEUX SE CONNECTER SANS RENTRER DE MOT DE PASSE

GENERATION SSH-KEY PUTTY

PuTTYgen
Application

ON OUVRE PUTTYGEN

PuTTY Key Generator

File Key Conversions Help

Key

No key.

ON GÉNÈRE

Actions

Generate a public/private key pair — Generate

Load an existing private key file — Load

Save the generated key — Save public key — Save private key

Parameters

Type of key to generate:
RSA DSA ECDSA EdDSA SSH-1 (RSA)

Number of bits in a generated key: 2048

PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCXbzU57E7H3vI8dPzR
+A5shM2sQiw9LVTPOd4ag1PWReiYIXJh0c9x9Z3adecnhc6G2Yy0Axfmch2YL1QiV20J/NPIbNcFNOen2VLNTK2
vNATGBW3vijzYBnIJ8AIBFWI0S6a6Y1qT/LRWbJdPKcxH5aX8U78dn0uxiCMH1ujD2r5SR9uRNxk5Ah5rawqt0hE
LIdW/C543ExCSYa9q5YpUM21QMT9jb8jeBvG1x82cWXYwQwgO
+nOvhj2C8svmItTupU6VzTQNZKXX7a93STuLkWjHU0HcwhYTC4wsrjyJQe6yXbhzZ9TIjcHFeAoMDPgrUOV4M4
```

Key fingerprint: ssh-rsa 2048 SHA256:rfPb3a9lYTIfLRUM2ZuYV+wYS4pa5AJGt0rV4Hl9rxc

Key comment: rsa-key-20250430

Key passphrase:

Confirm

ON ENREGISTRE

Actions

Generate a public/private key pair — Generate

Load an existing private key file — Load

Save the generated key — Save public key — Save private key

PuTTYgen Warning

Are you sure you want to save this key without a passphrase to protect it?

Oui Non

Save private key as:

Bureau › sch

Organiser Nouveau dossier

Accueil

Galerie

Nom

Aucun éléme

PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCXbzU57E7H3vI8dPzR
+A5shM2sQiw9LVTPOd4ag1PWReiYIXJh0c9x9Z3adecnhc6G2Yy0Axfmch2YL1QiV20J/NPIbNcFNOen2VLNTK2
vNATGBW3vijzYBnIJ8AIBFWI0S6a6Y1qT/LRWbJdPKcxH5aX8U78dn0uxiCMH1ujD2r5SR9uRNxk5Ah5rawqt0hE
LIdW/C543ExCSYa9q5YpUM21QMT9jb8jeBvG1x82cWXYwQwgO
+nOvhj2C8svmItTupU6VzTQNZKXX7a93STuLkWjHU0HcwhYTC4wsrjyJQe6yXbhzZ9TIjcHFeAoMDPgrUOV4M4
```

ON COPIE LA CLEF PUBLIQUE

```
PS C:\Users\damie> ssh damien@192.168.20.128
```

ON SE CONNECTE

```
damien@debian:~/.ssh$ nano authorized_keys
```

ON ÉDITE LE FICHIER

DBERARD

ON COPIE LA CLEF PUBLIQUE DEDANS

GNU nano 7.2 authorized_keys *

<nOvhj2C8svmltTupU6VzTQNZKXX7a93STuLkWjHU0HcwhYTC4wsrjyJQe6yXbhzZ9TIjcHFeAoMDPgrUOV4M4VfKnIlMcFKxCl9 rsa-key-20250430

PuTTY Configuration

Category:

- Session
  - Logging
- Terminal
  - Keyboard
  - Bell
  - Features
- Window
  - Appearance
  - Behaviour
  - Translation
- Selection
- Colours
- Connection
  - Data
  - Proxy
- SSH
- Serial
- Telnet
- Rlogin
- SUPDUP

ON RENSEIGNE

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) | Port

192.168.20.128 | 22

Connection type:

SSH | Serial | Other: Telnet

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit:

Always | Never | Only on clean exit

About | Help | Open | Cancel

ON SE CONNECTE SANS MDP

damien@debian: ~

```
login as: damien
Authenticating with public key "rsa-key-20250430" from agent
Linux debian 6.1.0-34-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.135-1 (2025-04-25)
 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Apr 30 14:09:20 2025 from 192.168.20.1
damien@debian:~$
```

GENERATION SSH-KEY MOBAXTERM

ON LANCE

MobaXterm
Application

MobaXterm SSH Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH server (~/.ssh/authorized_keys file):

ON COPIE

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCTaMeiLZQeiMIR
+jTLtFd6IxFejkA/boUHPfi0RfFyMDI9Kr3ktFB2iH32qII0k0yI2IjKoJCqIpBMn8nSE2MSIbGmsDgkoI2k5Z/TLhyv8FC
h9KoVrHX4RRGBFms9A0/bJPd9pD+rIyTPjTXVoEYvP8tAyfk1Yw3OGIDIsIjt5HDgSekCvhyaE
+y5OxtksqOwbpnIC4I
+5TSgPW7gmmt8a0RvEz1bBIzbHwvDfA87rt9vfA/tZv2Ef80snifJ1xRnjEAO4shP7yXV8Pcq82ez8SNXrmcUZ69KF
```

Key fingerprint: ssh-rsa 2048 SHA256:DwTXzXaLuW9k54zoSHCPlv0RsgaRUXErJuCn/VPqBhw

Key comment: rsa-key-20250430

Key passphrase:

Confirm

Actions

Generate a public/private key pair — Generate

Load an existing private key file — Load

Save the generated key — Save public key | Save private key

ON SAVE LA CLEF PRIVÉ

Parameters

Type of key to generate:

RSA | DSA | ECDSA | EdDSA | SSH-1 (RSA)

Number of bits in a generated key: 2048

Tools Games Settings Macros Help

System

- MobApt packages manager (experime
- X11 tab with Dwm
- X11 window with Fvwm
- X11 window with Twm
- List hardware devices
- List running processes
- Command Prompt (admin)
- Windows Powershell (admin)

Office

- MobaTextEditor
- MobaDiff
- Ascii table

Network

- Network services
- MobaSSHTunnel (port forwarding)
- MobaKeyGen (SSH key generator)

ON GÉNÈRE

pub | pub1 | ssh-rsa AAAAI

Fichier | Modifier | Affichage

ON COPIE LA CLEF PUBLIQUE

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCIlPQLvgX+
8P0dt5BMFeQOxIJhhBKl7ZBR4S+B/WHDUV8zhjOAvYjJYv71mh9vtDEs/50r+a+nuVNNO732tlXLA
4dlu+rT2EQ08zgCOt8GAD0KlM6OM9V9JrEm7dNvSXEL1+
8xnL6H1oS4YFkkUBgv/iVfi/Tm1BfN0I7Z/fsbNr+j3UvFr8fiHrM0bT6UqiV2rgjme45xsBcs3ka
87IXrsUEy593eJ+
9jm9xMA9bBYKOTbSysGG+ObN94pJIchpBjsQEBE3Yo250dyoPlItdrufdOShOKSf8Kn3sk75mZyT1
EovIzG6hSJbqBU5YvB6QsMLMKyixbCr8FW9xaEIPx rsa-key-20250430
```

ON ÉDITE LE FICHIER

```
damien@debian:~/.ssh$ nano authorized_keys
```

ON COLLE LA CLEF PUBLIQUE

```
 GNU nano 7.2                                  authorized_keys *
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBB27bTd/Fs370t165gwbFLIVVyLd0zpIE43H05C0C3 damie@DESKTOP-NR05EGE
<G+ObN94pJIchpBjsOEBE3Yo250dvoPlItdrufdOShOKSf8Kn3sk75mZvT1EovIzG6hSJbqBU5YvB6OsMLMKvixbCr8FW9xaEIPx rsa-key-20250430
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCXbzU57E7H3vl8dPzR+A5shM2sQiw9LVTPOd4ag1PWReiYlXJh0c9x9Z3adecnhc6G2Yy0Axfmch2YL1QiV20J/NPIbNcFNOen2VLNTK2vNAT>
```

ON RENSEIGNE

Sessions | View

New session

Session settings

SSH | Telnet | Rsh | Xdmcp | RDP | VNC | FTP | SFTP | Serial | File | Shell | Browser | Mosh | Aws S3 | WSL

Basic SSH settings

Remote host * 192.168.20.128 | Specify username damien | Port 22

Advanced SSH settings | Terminal settings | Network settings | Bookmark settings

X11-Forwarding | Compression | Remote environment: Interactive shell

Execute command:

Do not exit after command ends

SSH-browser type: SFTP protocol

Follow SSH path (experimental)

Use private key C:\Users\damie\Desktop\AAAAP

Expert SSH settings

Execute macro at session start: <none>

OK | Cancel

ON UTILISE LA CLEF PRIVÉ SAUVEGARDÉ PLUS HAUT

Connexion to 192.168.20.128 (port 22)

It seems to be the first time you connect to this server:
the remote server identity is not yet known by MobaXterm.

Press "Accept" if you trust this identity and want to carry on connecting.
Press "Cancel" if you want to abandon this connection.

ON ACCEPTE

Accept | Cancel | More info...

Do not show this message again

6. 192.168.20.128 (damien)

```
• MobaXterm Personal Edition v25.1 •
(SSH client, X server and network tools)

▸ SSH session to damien@192.168.20.128
  • Direct SSH      : ✔
  • SSH compression : ✔
  • SSH-browser     : ✔
  • X11-forwarding  : ✔  (remote display is forwarded through SSH)

▸ For more info, ctrl+click on help or visit our website.
```

ON EST BIEN CONNECTÉ SANS MDP

AUTHENTIFICATION AVEC GOOGLE AUTHENTIFICATOR

```
damien@debian:~$ sudo apt update
sudo apt install libpam-google-authenticator
```

ON INSTALLE LE PAQUET

```
damien@debian:~$ google-authenticator

Do you want authentication tokens to be time-based (y/n) y
Warning: pasting the following URL into your browser exposes the OTP secret to Google:
  https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/damien@d
```

ON TAPE ÇA

ON SCAN LE QR CODE AVEC L'APPLICATION GOOGLE AUTHENTIFICATOR

```
Your new secret key is: SAZ23N4ODI3DYAKJMA5ZFQDYEU
Enter code from app (-1 to skip) 614352
Code confirmed
Your emergency scratch codes are:
  44667343
  13984993
  67229983
  42997227
  95085154

Do you want me to update your "/home/damien/.google_authenticator" file? (y/n y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n n

By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server,
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.
Do you want to do so? (y/n) n

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n) n
damien@debian:~$
```

ON TAPE LE CODE REÇU