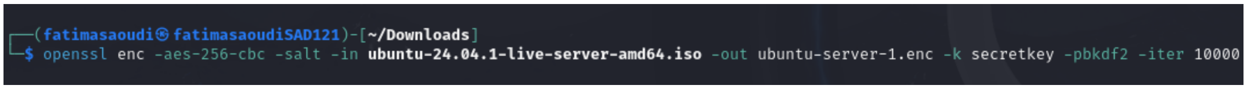
SAD121 Xifratges

Fatima Saoudi Tadlaoui Asixc2B-M11

1. Realització pas a pas

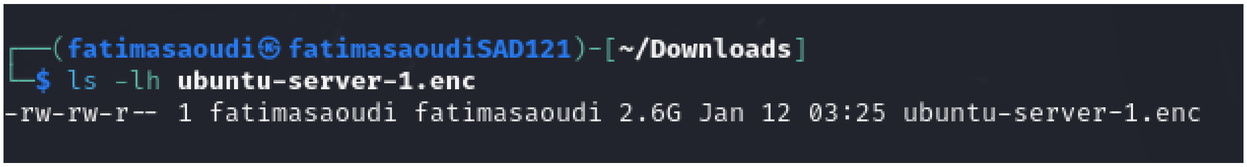
Escull un mètode **simètric** de xifratge **(AES-256-CBC)**

- **(1) Xifra el text clar**



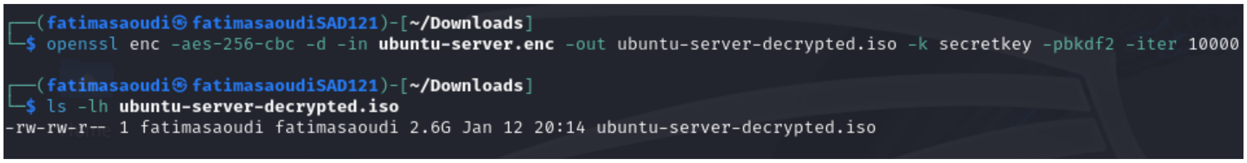
```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ openssl enc -aes-256-cbc -salt -in ubuntu-24.04.1-live-server-amd64.iso -out ubuntu-server-1.enc -k secretkey -pbkdf2 -iter 10000
```

- **-salt** afegeix aleatorietat al procés per millorar la seguretat.
- **-k** secretkey especifica una clau per al xifratge. Aquesta clau ha de ser compartida entre qui xifra i qui desxifra.
- El resultat serà un fitxer xifrat ubuntu-server-1.enc



```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ ls -lh ubuntu-server-1.enc
-rw-rw-r-- 1 fatimasaoudi fatimasaoudi 2.6G Jan 12 03:25 ubuntu-server-1.enc
```

- **(2) Desxifra el resultat**



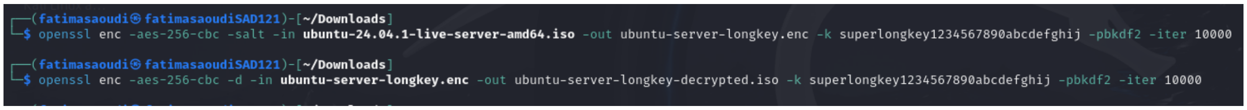
```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ openssl enc -aes-256-cbc -d -in ubuntu-server.enc -out ubuntu-server-decrypted.iso -k secretkey -pbkdf2 -iter 10000

┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ ls -lh ubuntu-server-decrypted.iso
-rw-rw-r-- 1 fatimasaoudi fatimasaoudi 2.6G Jan 12 20:14 ubuntu-server-decrypted.iso
```

- **-d** indica que es vol desxifrar el fitxer.
- El resultat serà el fitxer originalubuntu-server-decrypted.iso

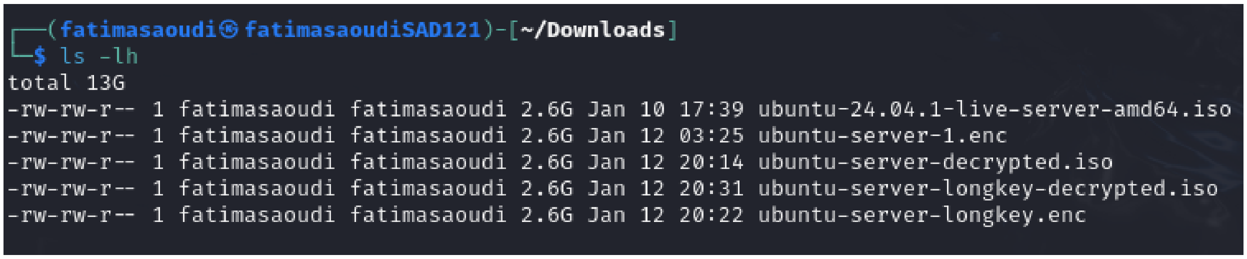
- **(3) i (4) Repeteix emprant una clau 10 vegades més llarga**

Paràmetre	**Clau Curta (secretkey)**	**Clau Llarga (superlongkey1234567890abcdefghij)**
Longitud de la clau	8 caràcters (64 bits)	40 caràcters (256 bits)
Comanda	openssl enc -aes-256-cbc -salt -in ubuntu-24.04.1-live-server-amd	openssl enc -aes-256-cbc -salt -in ubuntu-24.04.1-live-server-amd64.iso -out ubuntu-server-longkey.enc -k

	64.iso -out ubuntu-server.enc -k **secretkey** -pbkdf2 -iter 10000	**superlongkey1234567890abcdefghij** -pbkdf2 -iter 10000
Mida del fitxer	2.6 GB	2.6 GB
Temps d'execució	3.7 segons	3.83 segons



```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ openssl enc -aes-256-cbc -salt -in ubuntu-24.04.1-live-server-amd64.iso -out ubuntu-server-longkey.enc -k superlongkey1234567890abcdefghij -pbkdf2 -iter 10000

┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ openssl enc -aes-256-cbc -d -in ubuntu-server-longkey.enc -out ubuntu-server-longkey-decrypted.iso -k superlongkey1234567890abcdefghij -pbkdf2 -iter 10000
```

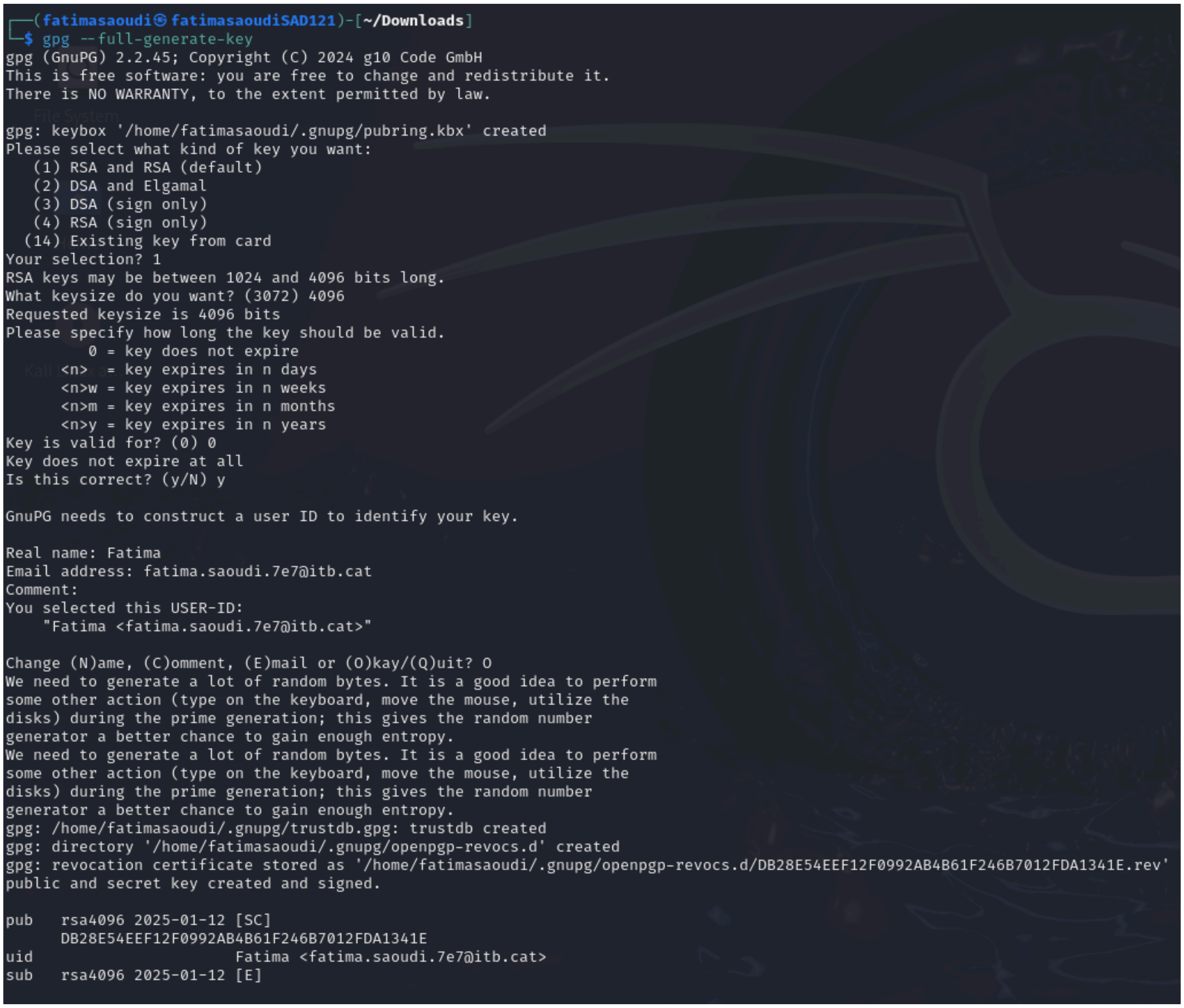


```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ ls -lh
total 13G
-rw-rw-r-- 1 fatimasaoudi fatimasaoudi 2.6G Jan 10 17:39 ubuntu-24.04.1-live-server-amd64.iso
-rw-rw-r-- 1 fatimasaoudi fatimasaoudi 2.6G Jan 12 03:25 ubuntu-server-1.enc
-rw-rw-r-- 1 fatimasaoudi fatimasaoudi 2.6G Jan 12 20:14 ubuntu-server-decrypted.iso
-rw-rw-r-- 1 fatimasaoudi fatimasaoudi 2.6G Jan 12 20:31 ubuntu-server-longkey-decrypted.iso
-rw-rw-r-- 1 fatimasaoudi fatimasaoudi 2.6G Jan 12 20:22 ubuntu-server-longkey.enc
```

- Això incrementa la seguretat, ja que una clau més llarga fa que sigui més difícil de trencar.

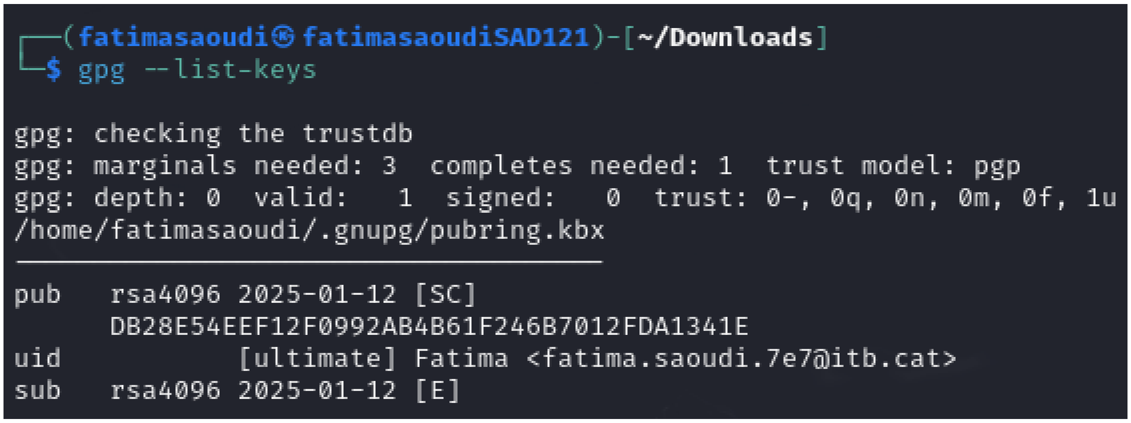
Escull un mètode **asimètric** de xifratge **(GPG)**

- **(5) Crea la teva parella de claus**



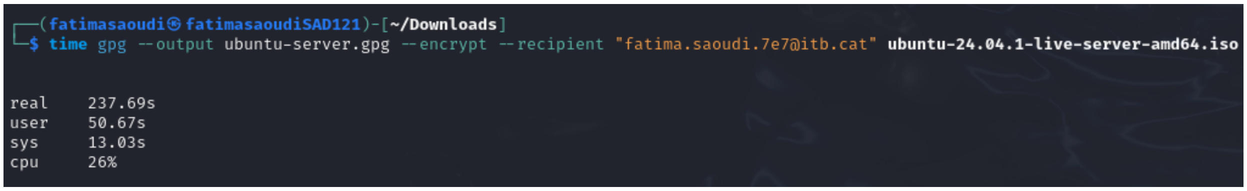
```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ gpg --full-generate-key
gpg (GnuPG) 2.2.45; Copyright (C) 2024 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: keybox '/home/fatimasaoudi/.gnupg/pubring.kbx' created
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
  (14) Existing key from card
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: Fatima
Email address: fatima.saoudi.7e7@itb.cat
Comment:
You selected this USER-ID:
    "Fatima <fatima.saoudi.7e7@itb.cat>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /home/fatimasaoudi/.gnupg/trustdb.gpg: trustdb created
gpg: directory '/home/fatimasaoudi/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/fatimasaoudi/.gnupg/openpgp-revocs.d/DB28E54EEF12F0992AB4B61F246B7012FDA1341E.rev'
public and secret key created and signed.

pub   rsa4096 2025-01-12 [SC]
      DB28E54EEF12F0992AB4B61F246B7012FDA1341E
uid                      Fatima <fatima.saoudi.7e7@itb.cat>
sub   rsa4096 2025-01-12 [E]
```

- GPG t'ofereix l'opció de generar una clau RSA amb una longitud de 4096 bits (opció recomanada per la seguretat).
- Introdueixo una adreça de correu electrònic i una contrasenya per protegir la clau privada.



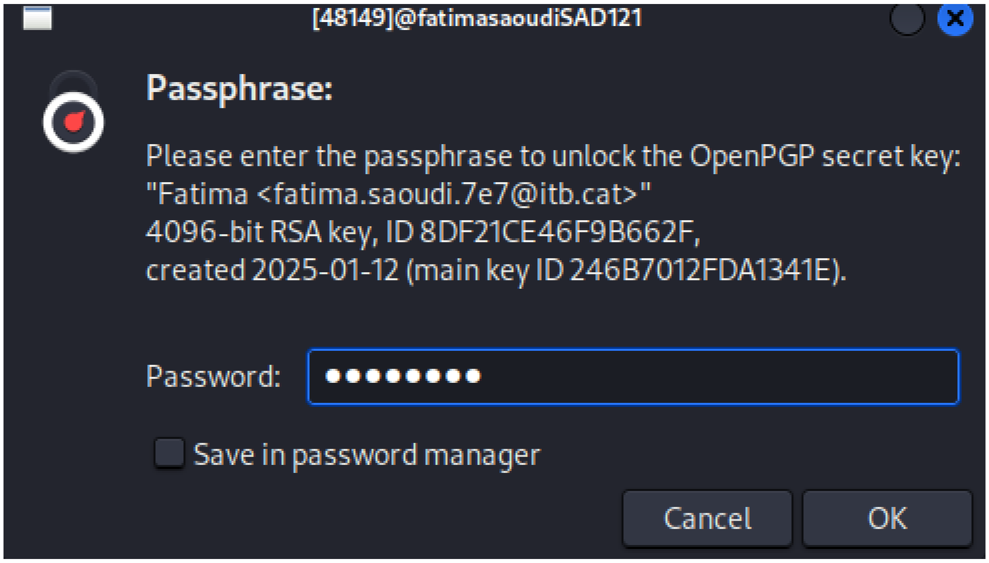
```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ gpg --list-keys

gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
/home/fatimasaoudi/.gnupg/pubring.kbx
─────────────────────────────────────
pub   rsa4096 2025-01-12 [SC]
      DB28E54EEF12F0992AB4B61F246B7012FDA1341E
uid           [ultimate] Fatima <fatima.saoudi.7e7@itb.cat>
sub   rsa4096 2025-01-12 [E]
```

- **(6) Xifra el text clar**



```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ time gpg --output ubuntu-server.gpg --encrypt --recipient "fatima.saoudi.7e7@itb.cat" ubuntu-24.04.1-live-server-amd64.iso


real    237.69s
user    50.67s
sys     13.03s
cpu     26%
```

- **(7) Desxifra el resultat**



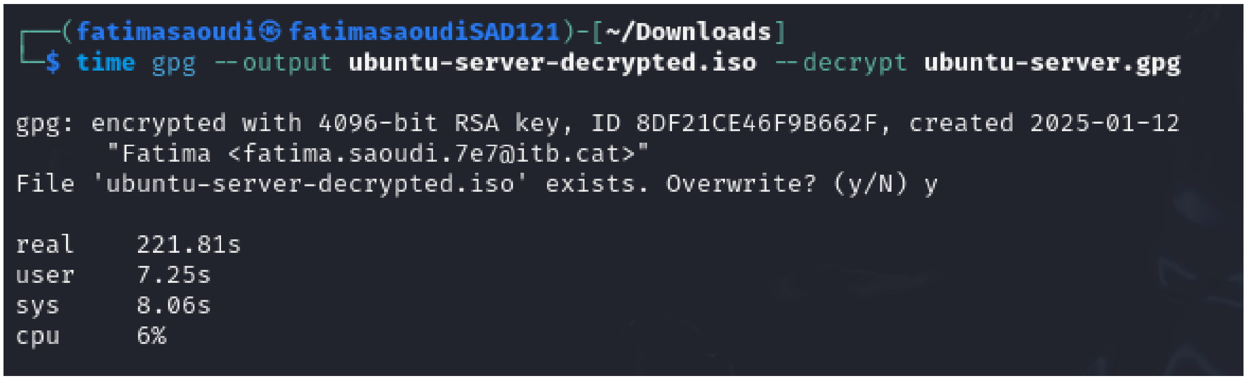
[48149]@fatimasaoudiSAD121

Passphrase:

Please enter the passphrase to unlock the OpenPGP secret key:
"Fatima <fatima.saoudi.7e7@itb.cat>"
4096-bit RSA key, ID 8DF21CE46F9B662F,
created 2025-01-12 (main key ID 246B7012FDA1341E).

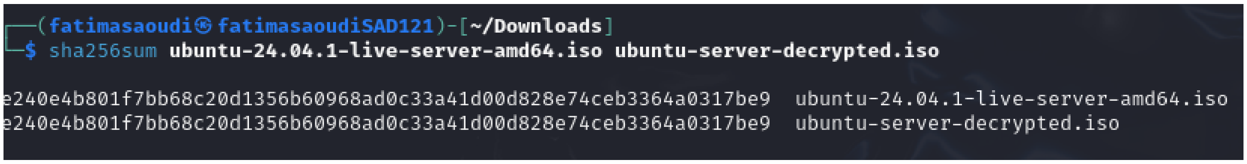
Password: ●●●●●●●●●

☐ Save in password manager



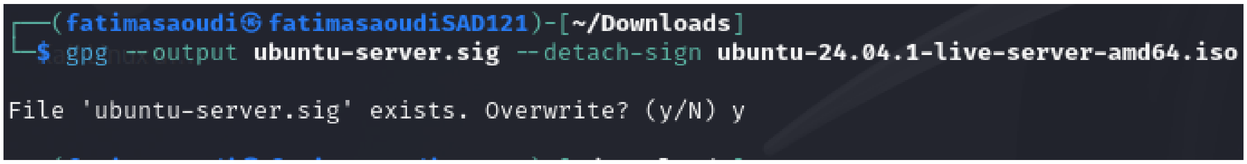
```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ time gpg --output ubuntu-server-decrypted.iso --decrypt ubuntu-server.gpg

gpg: encrypted with 4096-bit RSA key, ID 8DF21CE46F9B662F, created 2025-01-12
      "Fatima <fatima.saoudi.7e7@itb.cat>"
File 'ubuntu-server-decrypted.iso' exists. Overwrite? (y/N) y

real    221.81s
user    7.25s
sys     8.06s
cpu     6%
```

- El fitxer ubuntu-server-decrypted.iso ha de ser idèntic a l’original.
- Verificació amb un hash:



```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ sha256sum ubuntu-24.04.1-live-server-amd64.iso ubuntu-server-decrypted.iso

e240e4b801f7bb68c20d1356b60968ad0c33a41d00d828e74ceb3364a0317be9  ubuntu-24.04.1-live-server-amd64.iso
e240e4b801f7bb68c20d1356b60968ad0c33a41d00d828e74ceb3364a0317be9  ubuntu-server-decrypted.iso
```

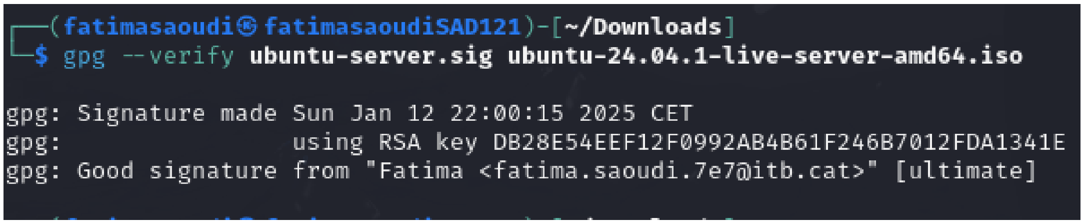
- **(8) Signa el text clar**



```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ gpg --output ubuntu-server.sig --detach-sign ubuntu-24.04.1-live-server-amd64.iso

File 'ubuntu-server.sig' exists. Overwrite? (y/N) y
```

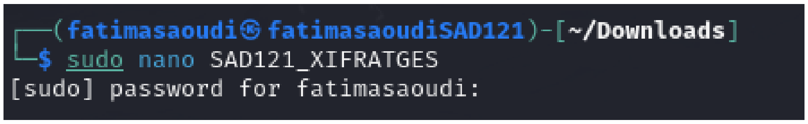
- La signatura garanteix que el fitxer no ha estat modificat i que realment prové de tu.

- **(9) Comprova la signatura**



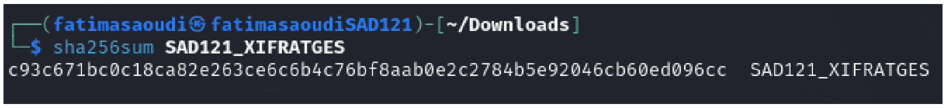
```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ gpg --verify ubuntu-server.sig ubuntu-24.04.1-live-server-amd64.iso

gpg: Signature made Sun Jan 12 22:00:15 2025 CET
gpg:                using RSA key DB28E54EEF12F0992AB4B61F246B7012FDA1341E
gpg: Good signature from "Fatima <fatima.saoudi.7e7@itb.cat>" [ultimate]
```

Escull un métode per a crear **hashes (SHA-256)**



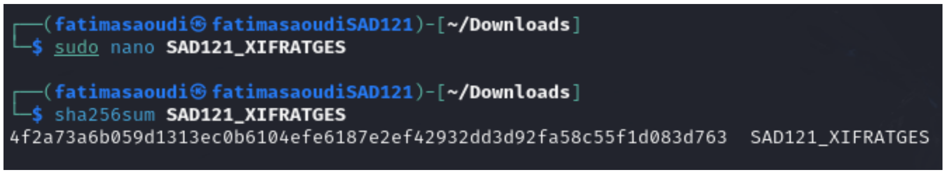
```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ sudo nano SAD121_XIFRATGES
[sudo] password for fatimasaoudi:
```

- **(10) "Hasheja" el text d'aquesta activitat**



```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ sha256sum SAD121_XIFRATGES
c93c671bc0c18ca82e263ce6c6b4c76bf8aab0e2c2784b5e92046cb60ed096cc  SAD121_XIFRATGES
```

- **(11) "Hasheja" el text d'aquesta activitat canviant un sol caràcter**



```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ sudo nano SAD121_XIFRATGES

┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ sha256sum SAD121_XIFRATGES
4f2a73a6b059d1313ec0b6104efe6187e2ef42932dd3d92fa58c55f1d083d763  SAD121_XIFRATGES
```

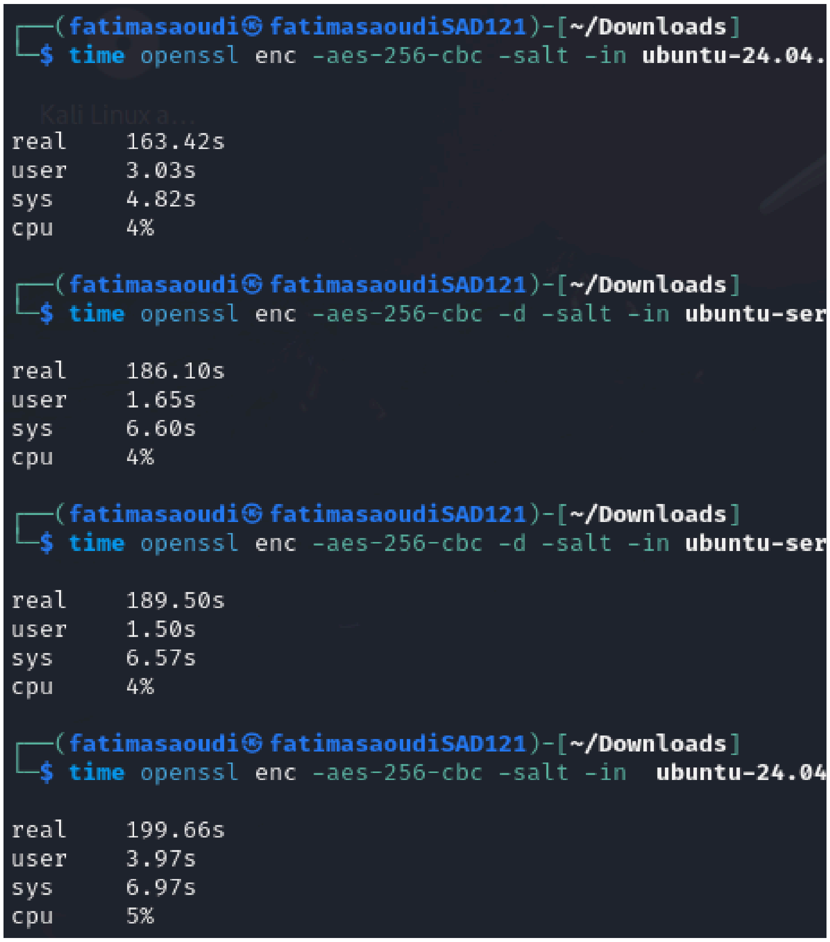
2. Taula comparativa de dades

Punt	Mètode	Longitud de la clau	Comanda emprada	Mida del resultat (en bytes)	Temps emprat
(1)	Simètric (AES-256-CBC)	8 caràcters (64 bits)	`openssl enc -aes-256-cbc -salt -in ubuntu-24.04.1-live-server-amd64.iso -out ubuntu-server.enc -k secretkey -pbkdf2 -iter 10000`	2.6 GB	3.03 s

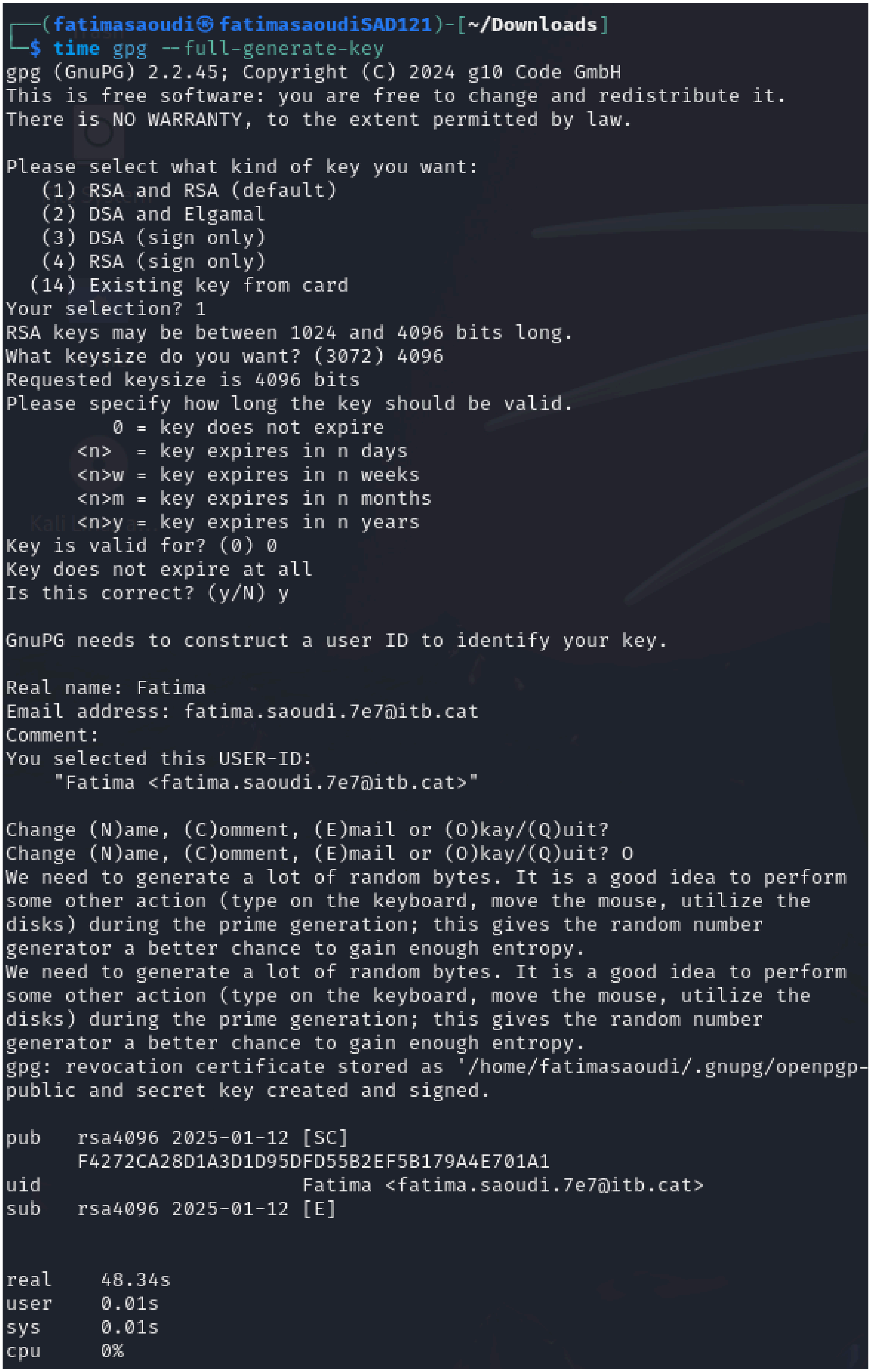
(2)	Simètric (AES-256-CBC)	8 caràcters (64 bits)	`openssl enc -aes-256-cbc -d -salt -in ubuntu-server.enc -out ubuntu-server-decrypted.iso -k secretkey -pbkdf2 -iter 10000`	2.6 GB	1.65 s
(3)	Simètric (AES-256-CBC)	40 caràcters (256 bits)	`openssl enc -aes-256-cbc -salt -in ubuntu-24.04.1-live-server-amd64.iso -out ubuntu-server-longkey.enc -k superlongkey1234567890abcdefghij -pbkdf2 -iter 10000`	2.6 GB	3.97 s
(4)	Simètric (AES-256-CBC)	40 caràcters (256 bits)	`openssl enc -aes-256-cbc -d -salt -in ubuntu-server-longkey.enc -out ubuntu-server-longkey-decrypted.iso -k superlongkey1234567890abcdefghij -pbkdf2 -iter 10000`	2.6 GB	1.50 s
(5)	Asimètric (GPG - Generació de claus)	4096 bits	`gpg --full-generate-key`	2.5K (/home/fatimasaoudi/.gnupg/pubring.kbx)	0.01 s
(6)	Asimètric (GPG - Xifrat)	4096 bits	`gpg --output ubuntu-server.gpg --encrypt --recipient "fatima.saoudi.7e7@itb.cat" ubuntu-24.04.1-live-server-amd64.iso`	2.6 GB	55.15 s
(7)	Asimètric (GPG - Desxifrat)	4096 bits	`gpg --output ubuntu-server-decrypted.iso --decrypt ubuntu-server.gpg`	2.6 GB	5.80 s
(8)	Asimètric (GPG - Signatura)	4096 bits	`gpg --output ubuntu-server.sig --detach-sign ubuntu-24.04.1-live-server-amd64.iso`	566	7.65 s
(9)	Asimètric (GPG - Comprovació de signatura)	4096 bits	`gpg --verify ubuntu-server.sig ubuntu-24.04.1-live-server-amd64.iso`	566	5.03 s

(10)	Hash (SHA-256)	-	`sha256sum SAD121_XIFRATGES`	1.5 K	0.00 s
(11)	Hash (SHA-256)	-	`sha256sum SAD121_XIFRATGES` (després de modificar un caràcter)	1.5K	0.00 s

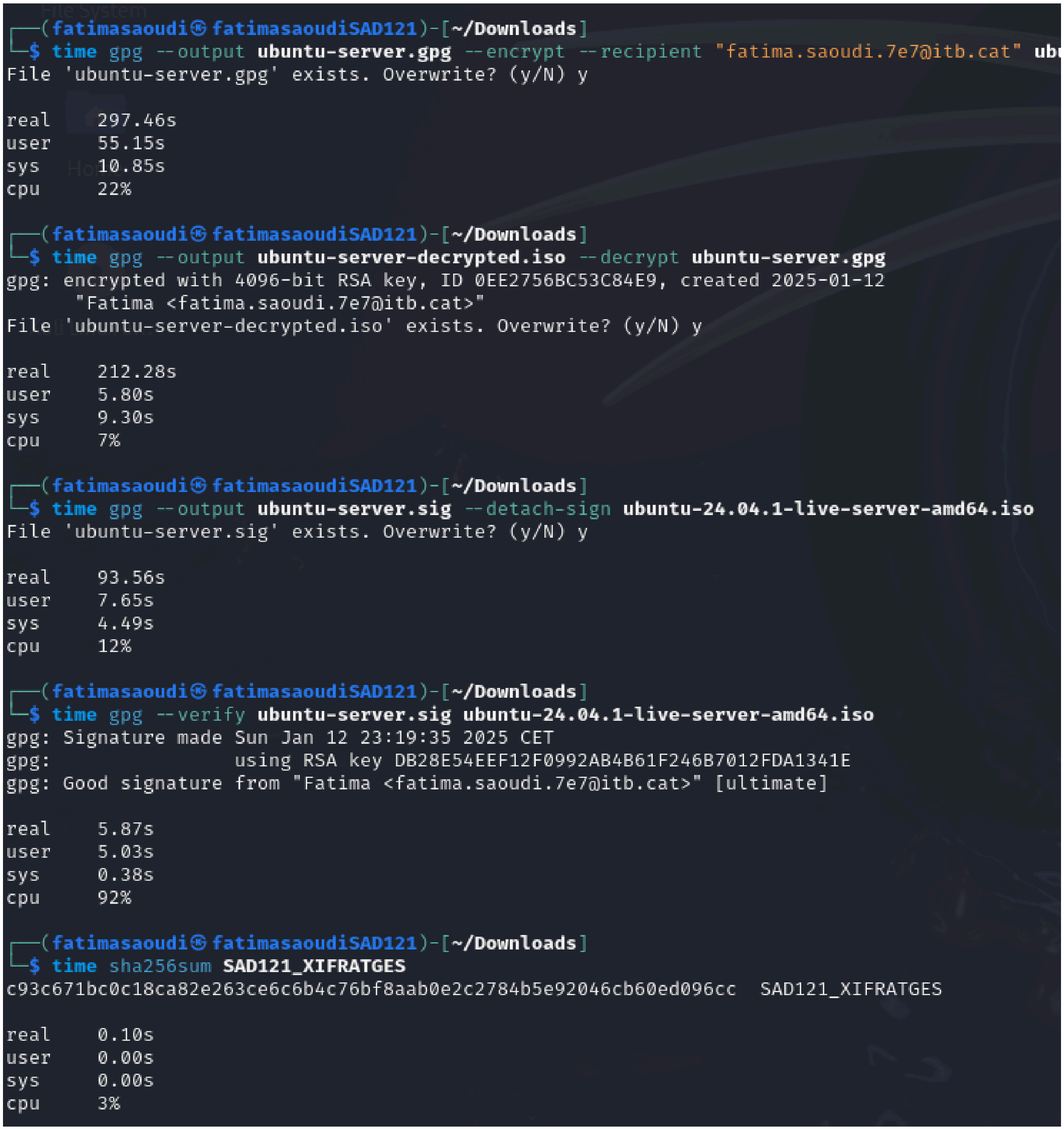
COMANDES ‘time’:



```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ time openssl enc -aes-256-cbc -salt -in ubuntu-24.04.

real    163.42s
user    3.03s
sys     4.82s
cpu     4%

┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ time openssl enc -aes-256-cbc -d -salt -in ubuntu-ser

real    186.10s
user    1.65s
sys     6.60s
cpu     4%

┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ time openssl enc -aes-256-cbc -d -salt -in ubuntu-ser

real    189.50s
user    1.50s
sys     6.57s
cpu     4%

┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ time openssl enc -aes-256-cbc -salt -in  ubuntu-24.04

real    199.66s
user    3.97s
sys     6.97s
cpu     5%
```



```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ time gpg --full-generate-key
gpg (GnuPG) 2.2.45; Copyright (C) 2024 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
  (14) Existing key from card
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: Fatima
Email address: fatima.saoudi.7e7@itb.cat
Comment:
You selected this USER-ID:
    "Fatima <fatima.saoudi.7e7@itb.cat>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit?
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: revocation certificate stored as '/home/fatimasaoudi/.gnupg/openpgp-
public and secret key created and signed.

pub   rsa4096 2025-01-12 [SC]
      F4272CA28D1A3D1D95DFD55B2EF5B179A4E701A1
uid                      Fatima <fatima.saoudi.7e7@itb.cat>
sub   rsa4096 2025-01-12 [E]


real    48.34s
user    0.01s
sys     0.01s
cpu     0%
```



```
┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ time gpg --output ubuntu-server.gpg --encrypt --recipient "fatima.saoudi.7e7@itb.cat" ubu
File 'ubuntu-server.gpg' exists. Overwrite? (y/N) y

real    297.46s
user    55.15s
sys     10.85s
cpu     22%

┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ time gpg --output ubuntu-server-decrypted.iso --decrypt ubuntu-server.gpg
gpg: encrypted with 4096-bit RSA key, ID 0EE2756BC53C84E9, created 2025-01-12
      "Fatima <fatima.saoudi.7e7@itb.cat>"
File 'ubuntu-server-decrypted.iso' exists. Overwrite? (y/N) y

real    212.28s
user    5.80s
sys     9.30s
cpu     7%

┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ time gpg --output ubuntu-server.sig --detach-sign ubuntu-24.04.1-live-server-amd64.iso
File 'ubuntu-server.sig' exists. Overwrite? (y/N) y

real    93.56s
user    7.65s
sys     4.49s
cpu     12%

┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ time gpg --verify ubuntu-server.sig ubuntu-24.04.1-live-server-amd64.iso
gpg: Signature made Sun Jan 12 23:19:35 2025 CET
gpg:                using RSA key DB28E54EEF12F0992AB4B61F246B7012FDA1341E
gpg: Good signature from "Fatima <fatima.saoudi.7e7@itb.cat>" [ultimate]

real    5.87s
user    5.03s
sys     0.38s
cpu     92%

┌──(fatimasaoudi㉿fatimasaoudiSAD121)-[~/Downloads]
└─$ time sha256sum SAD121_XIFRATGES
c93c671bc0c18ca82e263ce6c6b4c76bf8aab0e2c2784b5e92046cb60ed096cc  SAD121_XIFRATGES

real    0.10s
user    0.00s
sys     0.00s
cpu     3%
```