

TP 5 :

Je crée un fichier texte contenant mon message qui sera ensuite crypté et signé :

```
test@modele:~/Bureau$ mkdir BTSSIOS-TP5
test@modele:~/Bureau$ ls
BTSSIOS-TP5  TPS
test@modele:~/Bureau$ cd BTSSIOS-TP5/
test@modele:~/Bureau/BTSSIOS-TP5$ █
```

Une fois mon message rédigé , je crypte le fichier afin de le rendre illisible :

```
test@modele:~/Bureau/BTSSIOS-TP5$ gpg --symmetric --armour mail_tp5
```

```
1 -----BEGIN PGP MESSAGE-----
2
3 jA0ECQMCp8ghjPzjiYT/0pUBjjJKs8QTc18t1g5ebwUxRQbLTFKWGN+xutgS4X5z
4 m17W4/7SosgyANQRas13XBuHPS0lk6j0gCFRw+VNz5h/b6dqexxFQc5xsUc+rUZs
5 A8pDytdMcgGNTNDbZATJCnNKpQMhx5K8x2t4UlHV/C/YdhBJybdGYSFsDKD+9j+/
6 VQZ8S4Rg2Wk2Sv18t1apwcxWl2+/jQ==
7 =qJq+
8 -----END PGP MESSAGE-----|
```

Puis à l'aide du message secret , je décrypte le message afin de voir si ça marche

```
test@modele:~/Bureau/BTSSIOS-TP5$ gpg --decrypt mail_tp5.asc
gpg: données chiffrées avec AES256.CFB
gpg: chiffré avec 1 phrase secrète
Bonjour Monsieur ,

Voici mon fichier crypté et signé .

Cordialement .
Ahouari Idriss.
```

Je crée une clé puis je regarde si elle s'affiche bien :

```
test@modele:~/Bureau/BTSSIOS-TP5$ gpg --list-keys
/home/test/.gnupg/pubring.kbx
-----
pub    rsa3072 2025-01-23 [SC] [expire : 2027-01-23]
      C4CCDDC718EE0E3B49FB39D423A5C89E0D2A4D95
uid          [ ultime ] idriss <ahouari.idriss@gmail.com>
sub    rsa3072 2025-01-23 [E] [expire : 2027-01-23]
```

Je signe le fichier puis je vérifie que ma signature à bien été pris en compte :

```
test@modele:~/Bureau/BTSSIOS-TP5$ gpg --sign-key idriss
sec rsa3072/23A5C89E0D2A4D95
    créé : 2025-01-23  expire : 2027-01-23  utilisation : SC
    confiance : ultime      validité : ultime
ssb rsa3072/8473937E99638140
    créé : 2025-01-23  expire : 2027-01-23  utilisation : E
[ ultime ] (1). idriss <ahouari.idriss@gmail.com>

« idriss <ahouari.idriss@gmail.com> » a déjà été signée par la clef 23A5C89E0D2A4D95
Rien à signer avec la clef 23A5C89E0D2A4D95
```

```
test@modele:~/Bureau/BTSSIOS-TP5$ gpg --verify mail_tp5_signe.asc
gpg: Signature faite le jeu. 23 janv. 2025 14:38:37 CET
gpg:                               avec la clef RSA C4CCDDC718EE0E3B49FB39D423A5C89E0D2A4D95
gpg: Bonne signature de « idriss <ahouari.idriss@gmail.com> » [ultime]
test@modele:~/Bureau/BTSSIOS-TP5$
```

Voici le message final , crypté et signé .

```
1 -----BEGIN PGP SIGNED MESSAGE-----
2 Hash: SHA512
3
4 -----BEGIN PGP MESSAGE-----
5
6 jA0ECQMCp8ghjPzjiYT/0pUBjjJKs8QTc18t1g5ebwUxRQbLTFKWGN+xutgS4X5z
7 m17W4/7SosgyANQRas13XBuHPS0lk6j0gCFRw+VNz5h/b6dqexxFQc5xsUc+rUZs
8 A8pDytdMcgGNTNDbZATJCNkPQMhx5K8x2t4UlHV/C/YdhBJybdGYSFsDKD+9j+/
9 VQZ8S4Rg2Wk2Sv18t1apwcxWl2+/jQ==
10 =qJq+
11 -----END PGP MESSAGE-----
12 -----BEGIN PGP SIGNATURE-----
13
14 iQGzBAEBCgAdFiEExMzdxxjuDjtJ+znUI6XIIng0qTZUFAmesRL0ACgkQI6XIIng0q
15 TZWHEAv/dqGcfpdMLdN0SVxrShoMLU6KYt+2noGLklU0opEmzVbQB73pSrVfDdGT
16 EljLz30GvSxuEifzbRGhvOuayJsQlBis85Rg4T6ackPJNaY0veeKBoGDYop7j5Lj
17 ekR/X/hQsyvEaJQz89GGFcZMAmoTxZViWfGLWo/8HFm0/aXcXi/w7A5uMCUiYkuh
18 zh08HQvgYcPiNQ51mzPcF+yPwsYcBTrVaGQ2hZmN22XSUqb86W5dE9187E2v/zPj
19 +WWwuWGiEjIWKJXw3tgMrlxrkMCGNeUayE3Hv/jthNu6yhUcy4akPoJDRqtSnhVP
20 46j1T7TTz/NckyxprtVdRj+6EQWVkxaHkWh/jyHiVjSuR6dSxl/SqjmDCHT8EPAP
21 R80tfFFfkM4bxS5re3NWNorzER8DsK9j0uaCMENLbr6i/IUMZdgnMermAnlJHSF/A
22 tY9WevMzT3zdugIlhIIwlGr02GWaJyLwX51EsKUuvZkYHGEEvN07e0jfKA/qfku9
23 jAPMijsD
24 =owb5
25 -----END PGP SIGNATURE-----
```

INFO UTILES :

Message Secret : message_idriss

```
« idriss <ahouari.idriss@gmail.com> » a déjà été signée par la clef 23A5C89E0D2A4D95
Rien à signer avec la clef 23A5C89E0D2A4D95
```