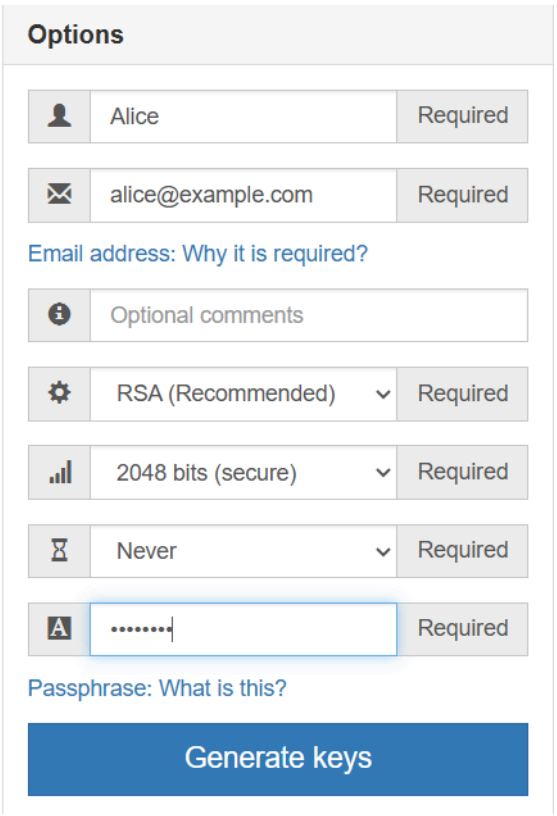
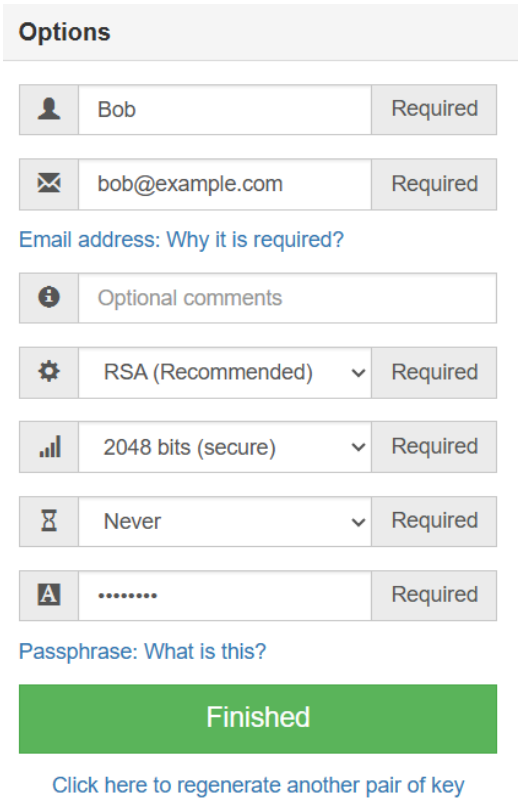
Travail à faire :

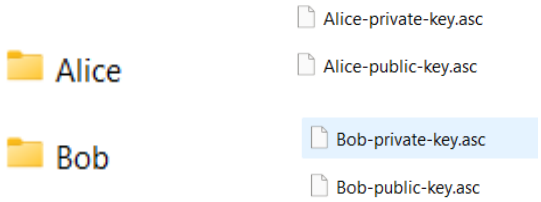
Etape 0 : génération des clés et mise à disposition des clés publiques.

Génération des clés pour **Alice** et **Bob**.





Sauvegarde des clés sous les noms explicites :

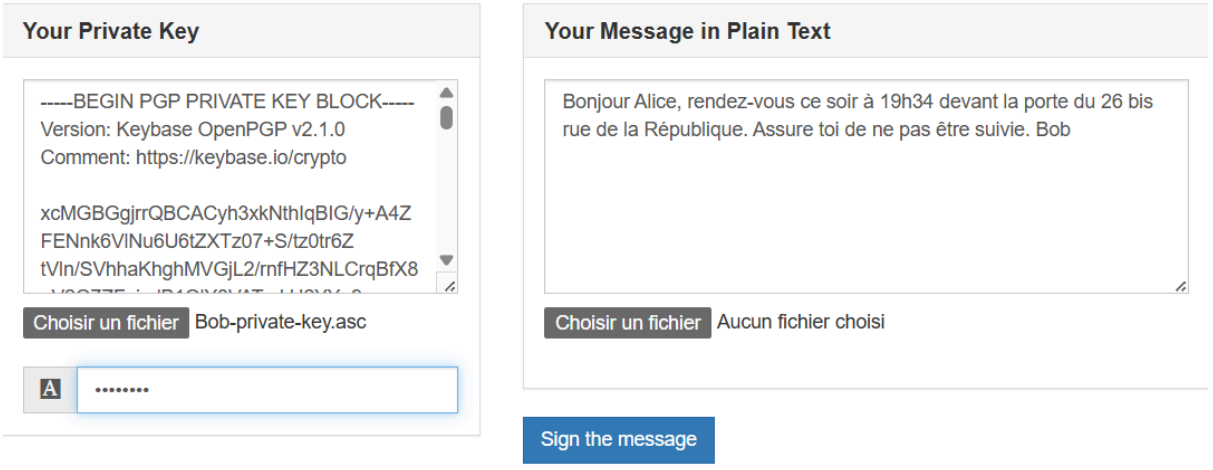


Etape 1 : signer et vérifier un message

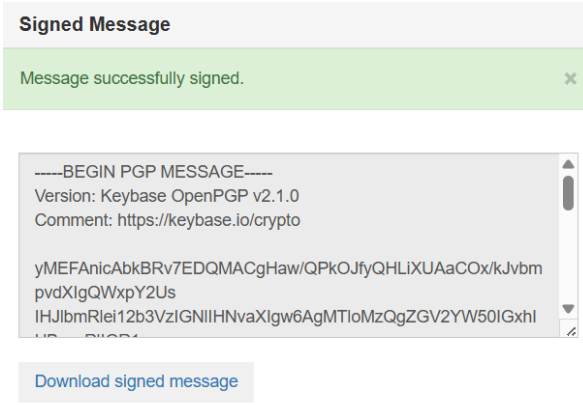
La signature numérique est générée avec la clé privée, et elle pourra être vérifiée avec la clé publique correspondante.

-Bob utilise sa **clé privée** pour signer le message :

« Bonjour Alice, rendez-vous ce soir à 19h34 devant la porte du 26 bis rue de la République. Assure-toi de ne pas être suivie. Bob »



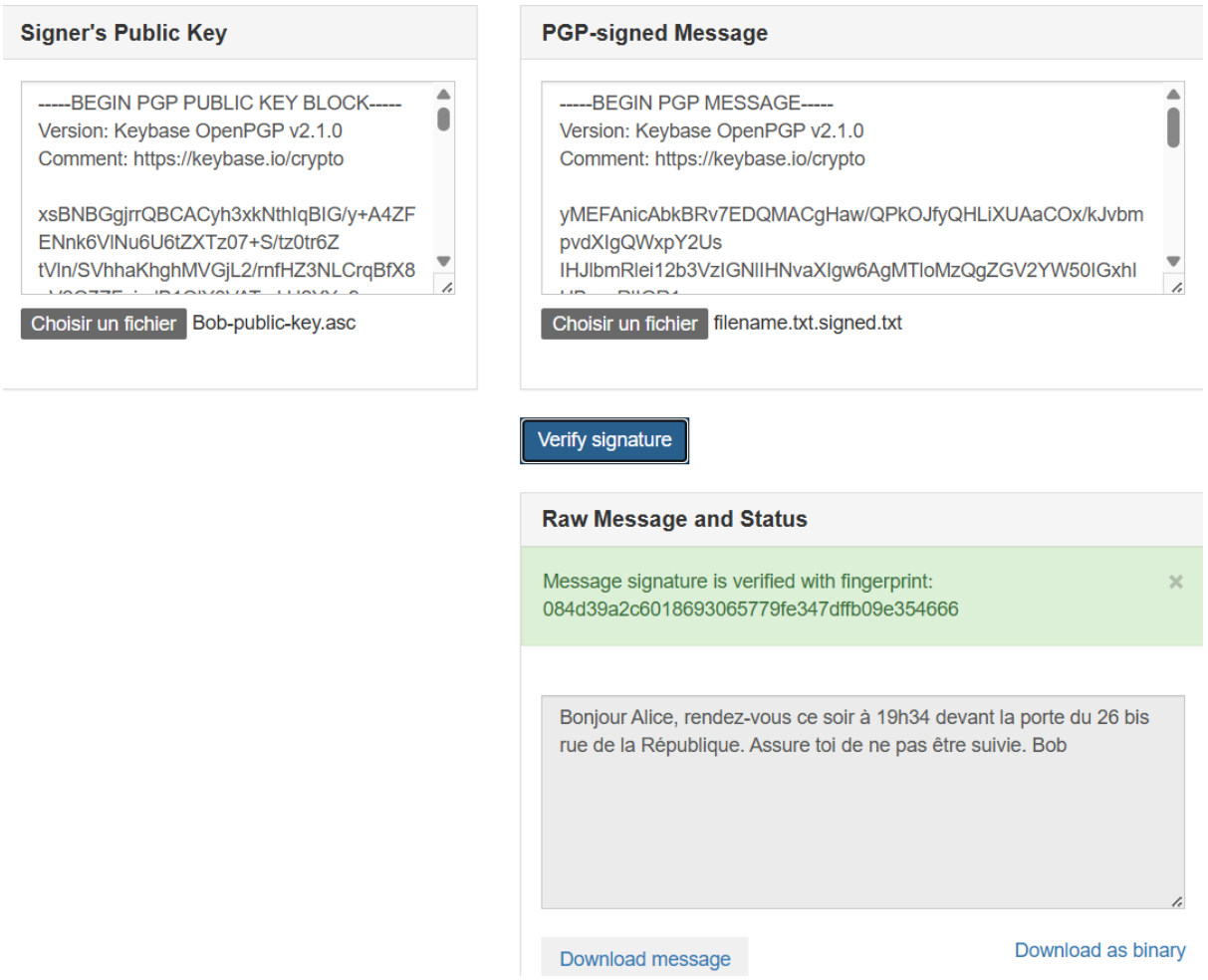
je signe ensuite le message et je télécharge le message signé



le message est bien envoyée

Je rentre la clé publique du signataire et je mets le fichier que j'ai téléchargé dans message signé PGP et je fais vérifier la signature.

-Alice utilise la **clé publique de Bob** pour **vérifier la signature** :

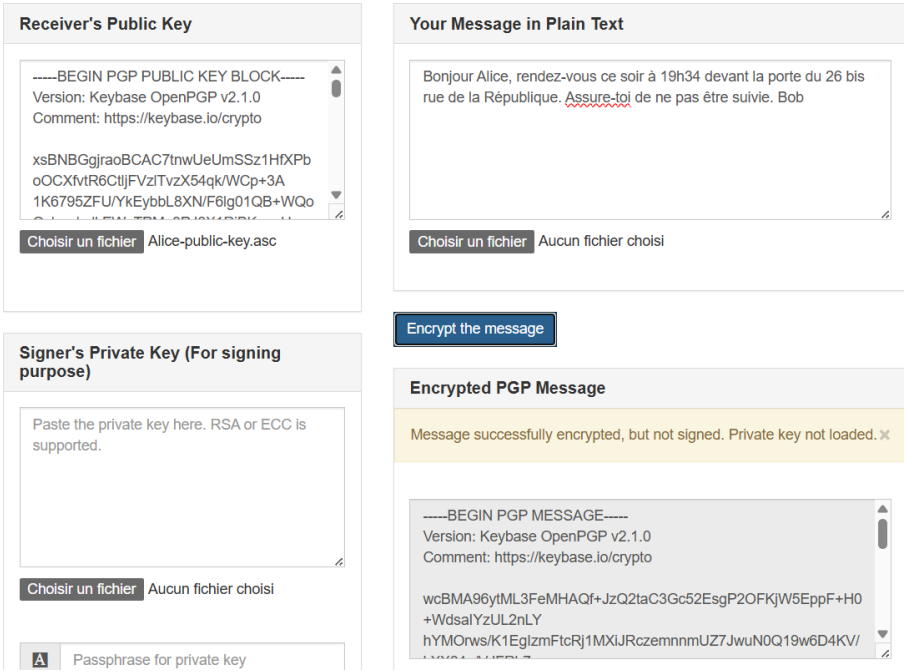


-Signature vérifiée avec la bonne clé.

-Vérification échoue avec une autre clé publique → preuve que seule la clé publique de Bob fonctionne.

Etape 2 : chiffrer un message

-Bob chiffre le message avec la **clé publique d'Alice** (sans le signer).

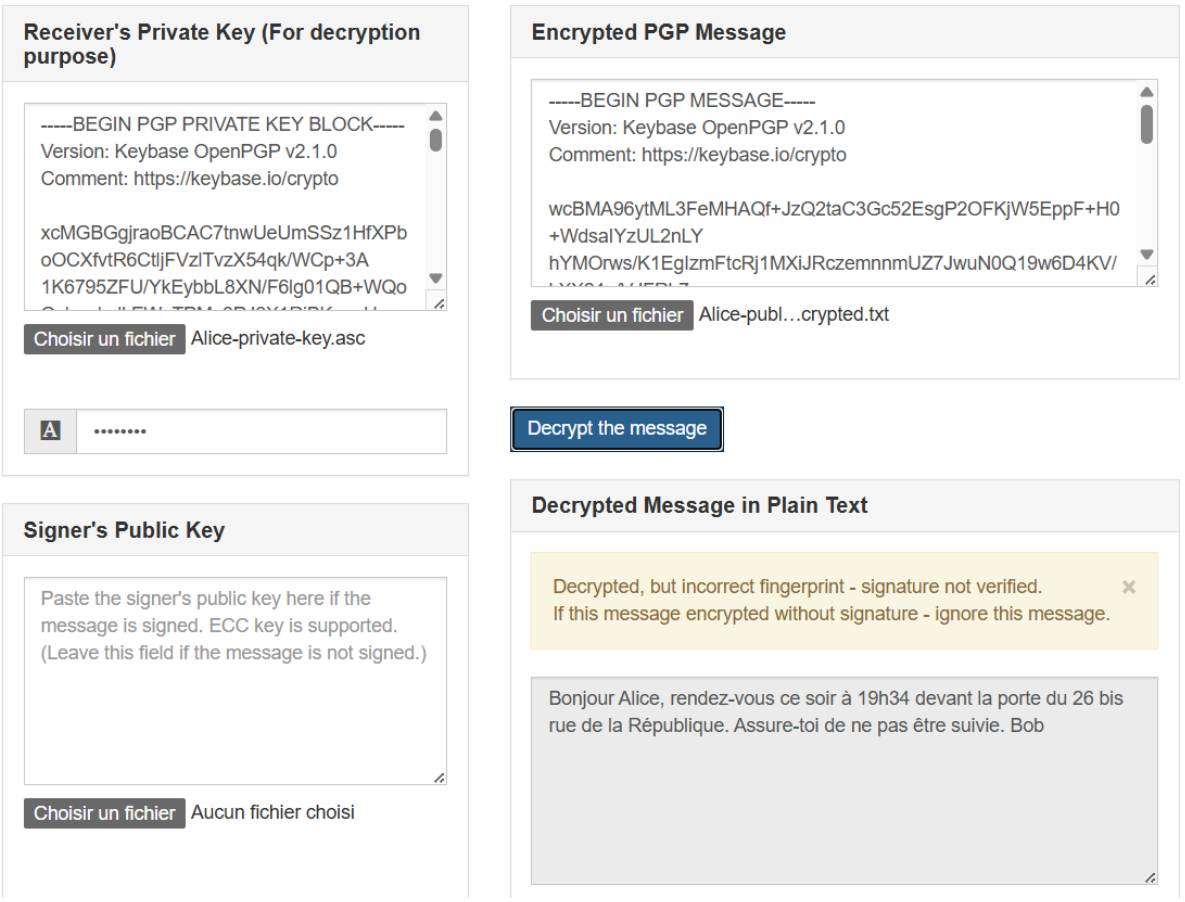


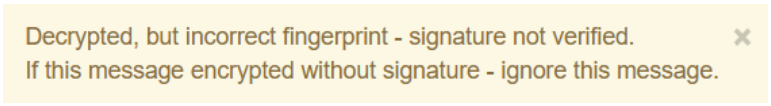
voici le message encryptée

```
-----BEGIN PGP MESSAGE-----
Version: Keybase OpenPGP v2.1.0
Comment: https://keybase.io/crypto

wcBMA96ytML3FeMHAQf+JzQ2taC3Gc52EsgP2OFKjW5EppF+H0+WdsaIYzUL2nLY
hYMOrws/K1EgIzmFtcRj1MXiJRczemnnmUZ7JwuN0Q19w6D4KV/kXX64n/VJFRh7
BoXTaR3ksJP2U9vODDAI0yxejYcm27P06HDAQuknsV5tIArgY8ttkpk+ZDEPEtVR
bsai60oyTZgIBTLTnv+8ad2G81zYfoPZ3u6Nn7c12gFF5P83ouGLpLPV+9JV53sb
cPil1NR1wr7rtj0EVDip8C9lbBKNRcG5uNGvqqu3h6qFH01i7Z1JDQJF+I41riQK
ybfvSLS4tw/aVZPYzeeDrIqu0bKO6jmsp+KoJocm89KyAdauyajTfxBpguze81+v
xCoR9u3hTJ3MW5jxrXbfucZnjJkPjDkUAQgju7JfDOOv2ixge+m0DFu+EhqJCWL2
zffoOU6i5tKG/xWnn2gcclGKvLAouOtnf0j6ntHcRxfiMvAlJNde5SUrIVtvjKXr
E1bhaXb5qD1rtf+kKsdCXVXmOUUprac3FsuNEqTeXhIkujkVuaEBxx2ua76HZnxr
xMXrrESlTkFMPqPItifnQvHFcQ==
=QU4y
-----END PGP MESSAGE-----
```

-Alice utilise sa **clé privée** pour le déchiffrer.





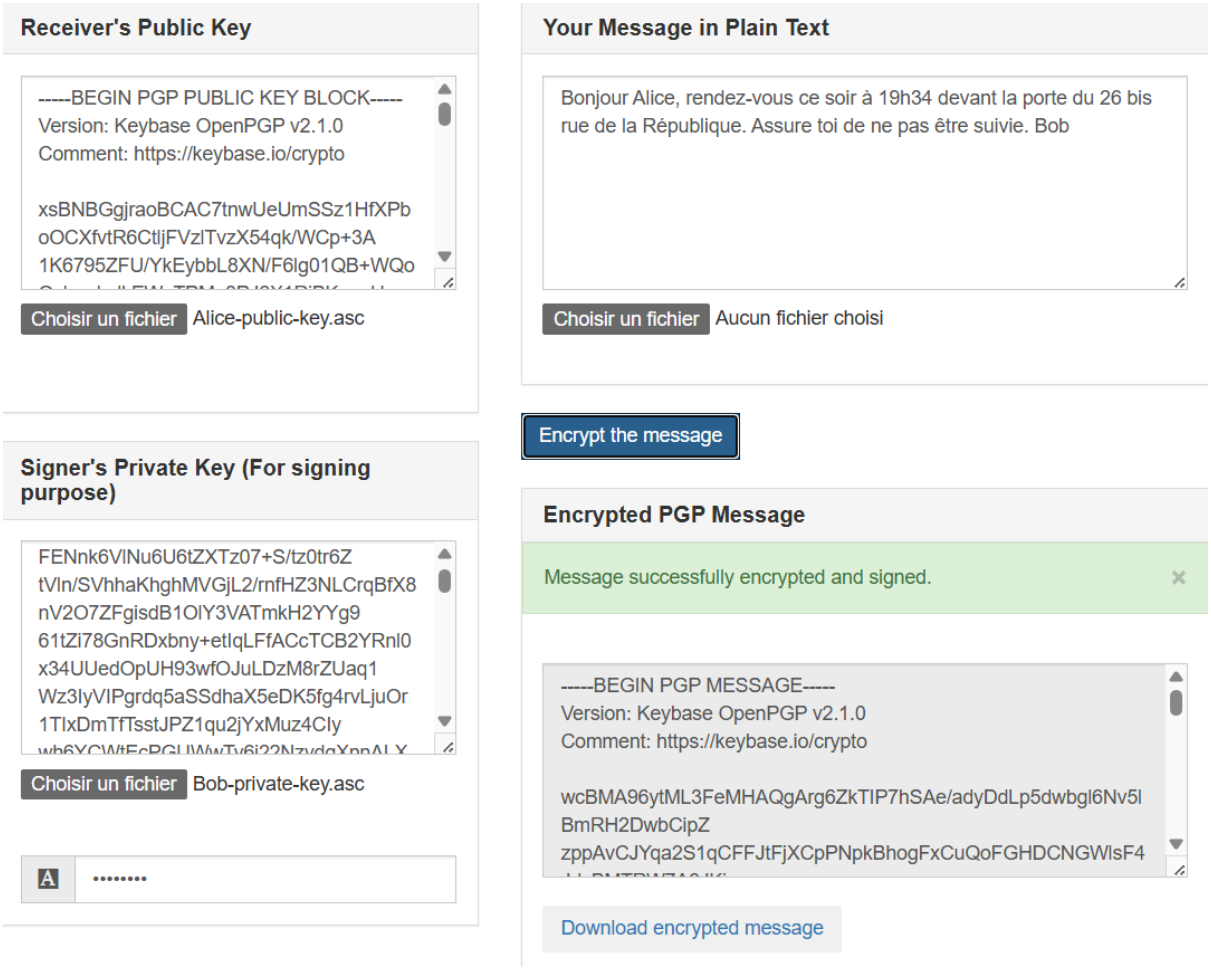
on va dans crypt pour chiffrer et decrypt pour déchiffrer

Observation :

- Le message est bien chiffré/déchiffré.
- Mais Alice **ne peut pas prouver que c'est Bob** qui l'a envoyé ⟶ absence de signature.

Etape 3 : chiffrer et signer un message

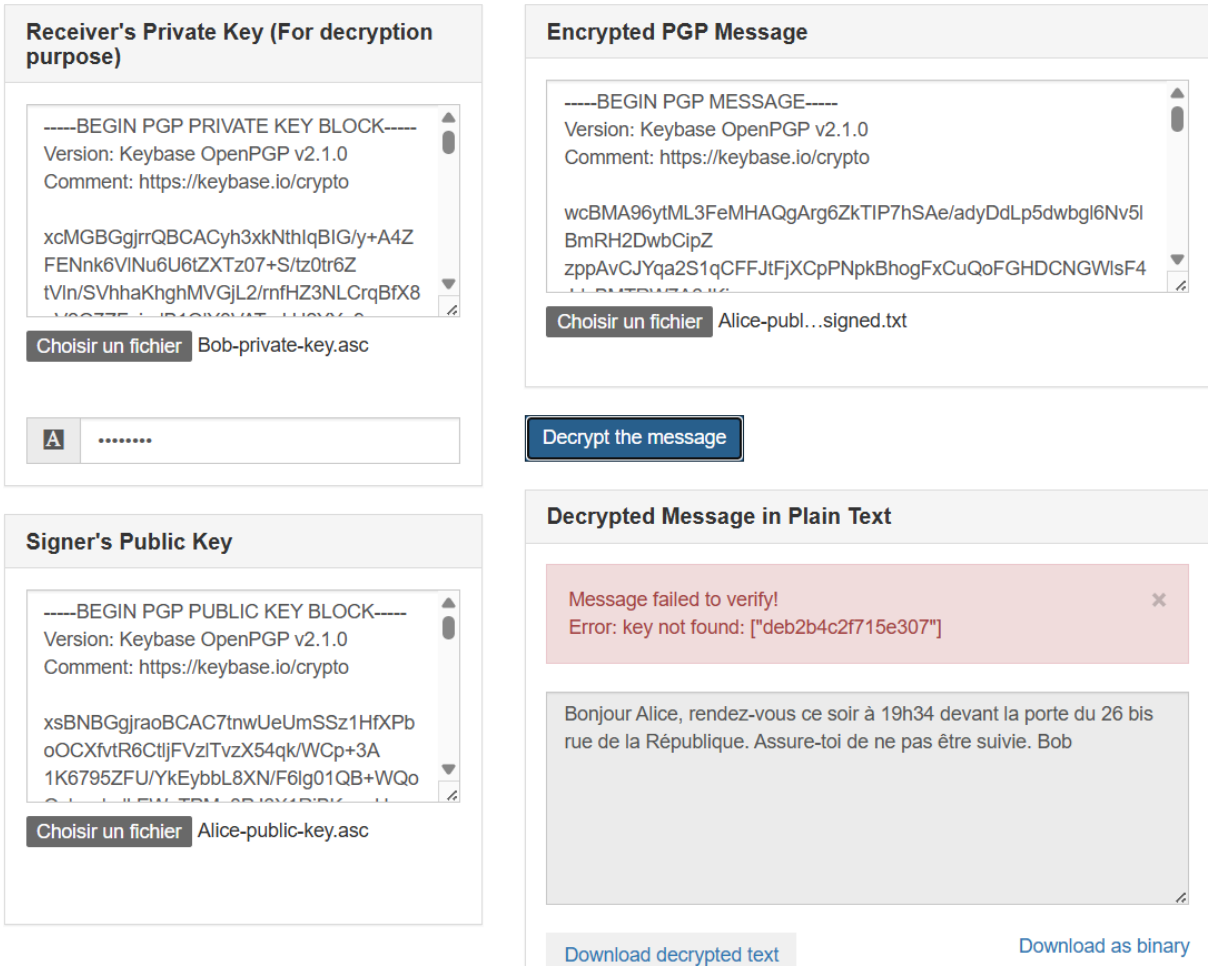
Bob chiffre le message avec la **clé publique d'Alice** et le **signe avec sa clé privée**.



Alice :

-Utilise la **clé publique de Bob** pour **vérifier la signature**.

-Utilise sa **clé privée** pour **déchiffrer** le message.



Que garantit cette méthode ?

-Alice peut lire le message.

-Alice peut **prouver que c'est Bob** qui a envoyé le message.

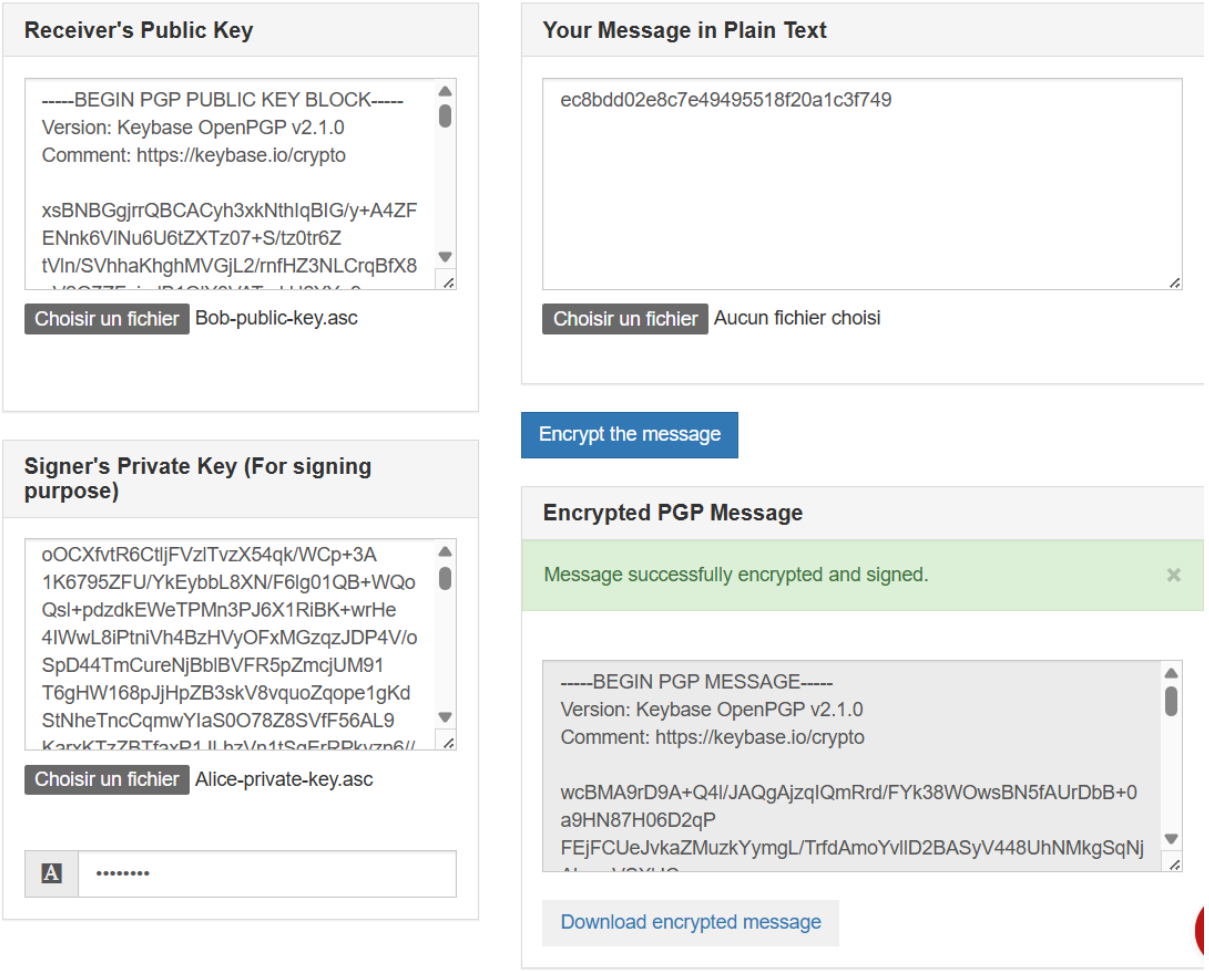
Étape 4 : Échange sécurisé de fichiers avec AES et PGP

Génération d'une clé AES

Outil : https://asecuritysite.com/encryption/plain

clé générée
hex key :
ec8bdd02e8c7e49495518f20a1c3f749

generation cle aes avec pgp
clé publique de bob et clé privé d'alice



voici le message encryptée

```
-----BEGIN PGP MESSAGE-----
Version: Keybase OpenPGP v2.1.0
Comment: https://keybase.io/crypto

wcBMA9rD9A+Q4l/JAQgAjzqIQmRrd/FYk38WOwsBN5fAUrDbB+0a9HN87H06D2qP
FEjFCUeJvkaZMuzkYymgL/TrfdAmoYvllD2BASyV448UhNMkgSqNjAksyyVSXlJC
aFWt8FMH9gZEU6Bshu0oM1VjV5z5/osIZjGhDjCqPBE+74A8Gn0NXz+87qL+wOM7
7zU6p48H4bls0wgXUsSAypYV7Gti92NCENIXphAVRax5CyJ9aesrpb61NggJqzxB
HnnSmVwu9yjYL9Ha9pGHVletx4CDk+CDmupIQ0INqxUO4NBPp8VzPkkhTL3e1dcC
JNklEUGJJLWvt/nykR7GdXQ27p9ciJJDYbwgVqSb/tLAzgGHXGY8LJ/JHf5gucCF
RwAJTBd22jwVPDn42eGeYTjKBh5amiPy7v9/ptmCnTIe8/3OTMCOcdnKXTT3RrFo
/BDBq27a4RY6qvn6sns4bEaN1FqY63ESHcW/L2jt1gZTeRmrhMbsYMakTtsusBi6
V27Zxuz6PFW7bH+DMY/3PA3lH5BlKN5LI5h64y6qQv09MiJTiUyxECQa6X7eCsHQ
0EqPIvQXcQGnJgTDrDB/Hvva5Lp7pETfjub0EhwBXwFIrUOHg+vbmm+Mhqy5e7OP
Lhdcsh7BUWv60yrHw45I8b4Dc1ogByAFsrOnJylqjev9QehcOfybf0BtWLK3S7RZ
P0Ymww5H8ub4f875wQWtc/auKl4E6dNGtXBZSb7vGZz02Jh11P4HSSkZaLyBiLML
0fvbBCUfOxAlnDaj83evcktJUDUruv/6yCLkIihd31dYxZjKgZjjvP1NA9796KGs
KtxkhaMe75SgDyonvjUlkH30GpXQt2IcGzgpDYmvIps8ILTxwDI8zVDi0xofhKHo
=tk2f
-----END PGP MESSAGE-----
```

Chiffrement du fichier avec la clé AES

Outil : CyberChef

Paramètres :

- **Key** : HEX
- **Mode** : ECB
- **Input / Output** : Raw

Modifier les paramètres

Recipe

AES Encrypt

Key
ec8bdd02e8c7e4949551...
HEX

IV
HEX

Mode
ECB

Input
Raw

Output
Raw

Input

Bonjour Alice, rendez-vous ce soir à 19h34 devant la porte du 26 bis rue de la République. Assure toi de ne pas être suivie. Bob

ABC 128 1 0 Raw Bytes LF

Output

>ê½õ••%•råþ•dETXs¡a•¤Ó•:fÖÊ•SYNÀË
µ•ì¤6iÀÛÅüÕè£:ê•0ÀÉB®?pEu³•¾øô£e•ñTSIvæÙmzì«ãEÐ•DH••þ:]
±ût8••ÓÚ;DBS•GS±gµEMCANÁ[2,ú/•(íÕp~u•G,EUSK[•¾"³8Þ^Ú•
w·71"Ò°°5Á&®•

5.Utiliser la clé aes pour déchiffrer le fichier

Déchiffrement par Bob :

Déchiffrement du fichier via CyberChef avec la clé AES.