

Travail à faire :

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

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

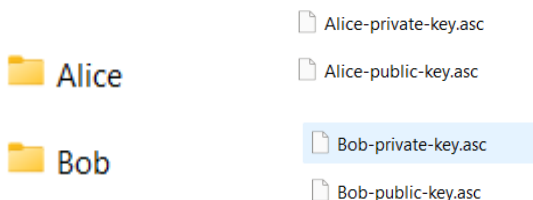
Options

	Alice	Required
	alice@example.com	Required
Email address: Why it is required?		
	Optional comments	
	RSA (Recommended) ▾	Required
	2048 bits (secure) ▾	Required
	Never ▾	Required
	Required
Passphrase: What is this?		
Generate keys		

Options

	Bob	Required
	bob@example.com	Required
Email address: Why it is required?		
	Optional comments	
	RSA (Recommended) ▾	Required
	2048 bits (secure) ▾	Required
	Never ▾	Required
	Required
Passphrase: What is this?		
Finished		
Click here to regenerate another pair of key		

Sauvegarde des clés sous les noms explicites :



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

The screenshot shows a web interface for PGP verification. It is divided into several sections:

- Signer's Public Key:** A text area containing a PGP public key block starting with "-----BEGIN PGP PUBLIC KEY BLOCK-----". Below the text is a "Choisir un fichier" button and the filename "Bob-public-key.asc".
- PGP-signed Message:** A text area containing a PGP signed message block starting with "-----BEGIN PGP MESSAGE-----". Below the text is a "Choisir un fichier" button and the filename "filename.txt.signed.txt".
- Verify signature:** A blue button with the text "Verify signature".
- Raw Message and Status:** A section with a green background indicating success: "Message signature is verified with fingerprint: 084d39a2c6018693065779fe347dfb09e354666". Below this is a text area containing the 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". At the bottom of this section are two buttons: "Download message" and "Download as binary".

-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).

Receiver's Public Key

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

xsBNBGgJraoBCAC7tnwUeUmSSz1HfXPb
oOCXvtR6CtIjFVzITvzX54qk/WCp+3A
1K6795ZFU/YkEybbL8XN/F6lg01QB+WQo
```

Choisir un fichier Alice-public-key.asc

Your Message in Plain Text

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

Choisir un fichier Aucun fichier choisi

Encrypt the message

Signer's Private Key (For signing purpose)

Paste the private key here. RSA or ECC is supported.

Choisir un fichier Aucun fichier choisi

Encrypted PGP Message

Message successfully encrypted, but not signed. Private key not loaded. ✖

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

wcBMA96ytML3FeMHAQf+JzQ2taC3Gc52EsgP20FKjW5EppF+H0
+WdsalYzUL2nLY
hYMOOrws/K1EglzmFtcRj1MXiJRczemnmUZ7JwuN0Q19w6D4KV/
```

voici le message encryptée

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

wcBMA96ytML3FeMHAQf+JzQ2taC3Gc52EsgP20FKjW5EppF+H0+WdsalYzUL2nLY
hYMOOrws/K1EglzmFtcRj1MXiJRczemnmUZ7JwuN0Q19w6D4KV/kXX64n/VJFRh7
BoXTaR3ksJP2U9vODDAI0yxejYcm27P06HDAQuknsV5tIArgY8ttkpk+ZDEPETVR
bsai60oyTZgIBTLTnv+8ad2G81zYfoPZ3u6Nn7c12gFF5P83ouGLpLPV+9JV53sb
cPil1NR1wr7rtj0EVDip8C91bBKNRcG5uNGvqqu3h6qFH01i7Z1JDQJF+I41riQK
ybfvSLS4tw/aVZPYzeeDrIqu0bK06jmsp+KoJocm89KyAdauyaJTfxBpguze81+v
xCoR9u3hTJ3MW5jxrXbfucZnjJkPjDkUAQgju7Jfd00v2ixge+m0DFu+EhqJCWL2
zffo0U6i5tKG/xwnn2gcc1GKvLAou0tnf0j6nthcRxfiMvAlJNde5SURIVtvjKXr
E1bhaXb5qD1rtf+kKsdCXVm0UUp rac3FsuNEqTeXhIkujkVuaEBxx2ua76HZnxr
xMXrrESlTkFMPqPitifnQvHFcO==
=QU4y
-----END PGP MESSAGE-----
```

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

Receiver's Private Key (For decryption purpose)

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

xcMGBGgjraoBCAC7tnwUeUmSSz1HfXPb
oOCXfvR6CtIjFVzITvzX54qk/WCp+3A
1K6795ZFU/YkEybbL8XN/F6lg01QB+WQo
-----BEGIN PGP PRIVATE KEY BLOCK-----
```

Choisir un fichier Alice-private-key.asc

A

Encrypted PGP Message

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

wcBMA96ytML3FeMHAQf+JzQ2taC3Gc52EsgP2OFKjW5EppF+H0
+WdsalYzUL2nLY
hYMOrws/K1EglzmFtcRj1MXiJRczemnmUZ7JwuN0Q19w6D4KV/
-----BEGIN PGP MESSAGE-----
```

Choisir un fichier Alice-publ...crypted.txt

Decrypt the message

Signer's Public Key

Paste the signer's public key here if the message is signed. ECC key is supported. (Leave this field if the message is not signed.)

Choisir un fichier Aucun fichier choisi

Decrypted Message in Plain Text

Decrypted, but incorrect fingerprint - signature not verified. ✕
 If this message encrypted without signature - ignore this 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

Decrypted, but incorrect fingerprint - signature not verified. ✕
 If this message encrypted without signature - ignore this message.

on va dans crypt pour chiffrer et decrypt pour déchiffrer

Encrypt (+Sign)
Decrypt (+Verify)

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**.

The screenshot shows a web-based PGP encryption interface. It is divided into several sections:

- Receiver's Public Key:** A text area containing a PGP public key block. Below it is a button labeled "Choisir un fichier" and the filename "Alice-public-key.asc".
- Your Message in Plain Text:** A text area containing the 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". Below it is a button labeled "Choisir un fichier" and the text "Aucun fichier choisi".
- Encrypt the message:** A blue button.
- Encrypted PGP Message:** A section with a green success message: "Message successfully encrypted and signed." Below it is a text area containing the encrypted PGP message block. Below this is a button labeled "Download encrypted message".
- Signer's Private Key (For signing purpose):** A text area containing a PGP private key block. Below it is a button labeled "Choisir un fichier" and the filename "Bob-private-key.asc".
- Signature:** A text input field with a dropdown menu set to "A" and a password field with dots.

Alice :

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

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

Receiver's Private Key (For decryption purpose)

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

xcMGBGgjrrQBCACyh3xkNthlqBIG/y+A4Z
FENnk6VINu6U6tZXTz07+S/tz0tr6Z
tVIn/SVhhaKhghMVGjL2/rmfHZ3NLCrQBfX8
-----
```

Choisir un fichier Bob-private-key.asc

A

Encrypted PGP Message

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

wcBMA96ytML3FeMHAQgArg6ZkTIP7hSAe/adyDdLp5dwbgl6Nv5l
BmRH2DwbCipZ
zppAvCJYqa2S1qCFFJtFjXCpPNpkBhogFxCuQoFGHDCNGWisF4
-----
```

Choisir un fichier Alice-publ...signed.txt

Decrypt the message

Signer's Public Key

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

xsBNBGgjraoBCAC7tnwUeUmSSz1HfXPb
oOCXfvtR6CtjFVzITvzX54qk/WCp+3A
1K6795ZFU/YkEybbL8XN/F6lg01QB+WQo
-----
```

Choisir un fichier Alice-public-key.asc

Decrypted Message in Plain Text

Message failed to verify!
Error: key not found: ["deb2b4c2f715e307"]

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

Download decrypted text Download as binary

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

The screenshot displays the ASecuritySite encryption tool interface. It is divided into several sections:

- Receiver's Public Key:** Shows a public key block starting with "-----BEGIN PGP PUBLIC KEY BLOCK-----". The key is associated with "Bob-public-key.asc".
- Signer's Private Key (For signing purpose):** Shows a private key block starting with "oOCXftR6CtjFVzITvzX54qk/Wcp+3A". The key is associated with "Alice-private-key.asc".
- Your Message in Plain Text:** Contains the hex key "ec8bdd02e8c7e49495518f20a1c3f749".
- Encrypt the message:** A blue button to initiate the encryption process.
- Encrypted PGP Message:** A green notification box states "Message successfully encrypted and signed." Below it, the encrypted message block is shown, starting with "-----BEGIN PGP MESSAGE-----".
- Download encrypted message:** A button to download the resulting encrypted message.

voici le message encryptée

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

```
wcBMA9rD9A+Q4l/JAQgAjzqIQmRrd/FYk38WowsBN5fAUrDbB+0a9HN87H06D2qP  
FEjFCUeJvkaZMuzkYymgL/TrfdAmoYv1lD2BASyV448UhNMkgSqNjAksyyVSXlJC  
aFwt8FMH9gZEU6Bshu0oM1VjV5z5/osIZjGhdjCqPBE+74A8Gn0NXz+87qL+wOM7  
7zU6p48H4b1s0wgXUsSAypYV7Gti92NCENIXphAVRax5CyJ9aesrpb61NggJqzxB  
HnnSmVwu9yjYL9Ha9pGHV1etx4CDk+CDmupIQ0INqxU04NBp8VzPkkhTL3e1dcC  
JNk1EUGJJLWvt/nykR7GdXQ27p9ciJJDYbwgVqSb/tLAzgGHXGY8LJ/JHf5gucCF  
RwAJTBd22jwVPDn42eGeYTjKBh5amiPy7v9/ptmCnTIe8/30TMC0cdnKXTT3RrFo  
/BDBq27a4RY6qvn6sns4bEaN1FqY63ESHcw/L2jt1gZTeRmrhMbsYMakTtsusBi6  
V27Zxuz6PFW7bh+DMY/3PA3lH5BlKN5LI5h64y6qQv09MiJTiUyxECQa6X7eCsHQ  
0EqPIvQXcQgnJgTDrDB/Hvva5Lp7pETfjub0EhwBXwFIrUOHg+vbmM+Mhgy5e7OP  
Lhdcsh7BUWv60yrHw45I8b4Dc1ogByAFsrOnJylqjev9QehcOfybf0BtWLK3S7RZ  
P0Ymww5H8ub4f875wQwtc/auKl4E6dNGtXBZSb7vGZz02Jh11P4HSSkZaLyBiLML  
0fvbBCUf0xAlnDaj83evcktJUDUruv/6yCLkIihd31dYxZjkgZjjvP1NA9796KGs  
KtxkhaMe75SgDyonvjUlkh30GpXQt2IcGzgpDYmvIps8ILTwxDI8zVDi0xofhKH0  
=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

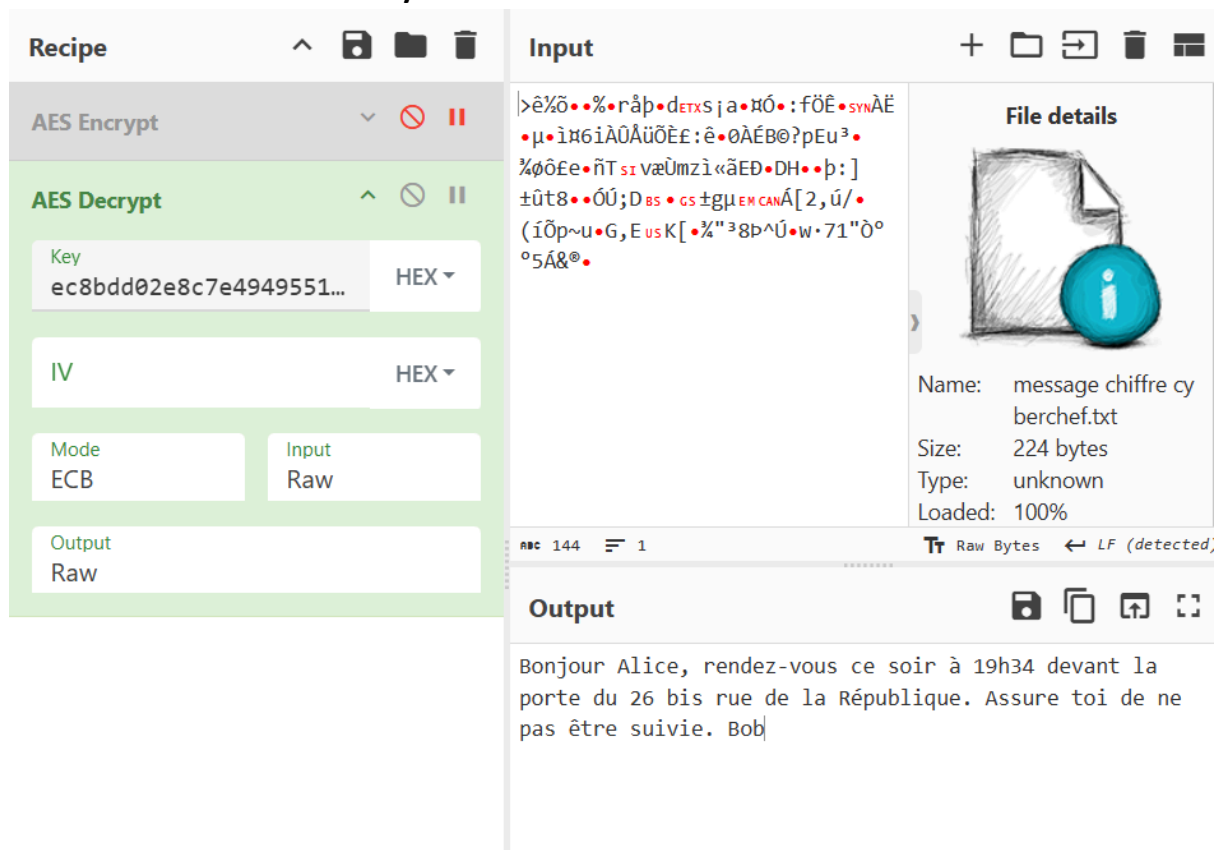
Output

```
>ë%õ••%•râp•dETXS ja•RÓ•:fÖË•SYNÄË
μ•i#6iÄÜÄüÖËf:ê•0ÄÉB0?pEu³•%øðfe•ñT sI væÛmzì«ãEÐ•DH••p:]
±ût8•ÓÚ;D BS • GS ±gμEM CANÁ[2,û/(iÖp~u•G, E us K[•%"³8p^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.



The screenshot shows the CyberChef web application interface. On the left, the 'Recipe' panel is active, showing 'AES Decrypt' selected. The key is set to 'ec8bdd02e8c7e4949551...' in HEX mode. The IV is empty. The Mode is set to 'ECB' and the Input is 'Raw'. The Output is also 'Raw'. The main 'Input' panel shows a file named 'message chiffre cyberchef.txt' with a size of 224 bytes. The 'Output' panel displays the decrypted text: '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'.

Recipe

- AES Encrypt
- AES Decrypt**
- Key: ec8bdd02e8c7e4949551... (HEX)
- IV: (HEX)
- Mode: ECB
- Input: Raw
- Output: Raw

Input

File details:

- Name: message chiffre cyberchef.txt
- Size: 224 bytes
- Type: unknown
- Loaded: 100%

Output

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