

# Devoir 3

INFO4305

Alec Jones  
A00216262

# Table des matières

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Objectif du TP</b>	<b>2</b>
<b>3</b>	<b>Déroulement du TP</b>	<b>3</b>
3.1	Partie 1 . . . . .	3
3.2	Partie 2 . . . . .	3
3.2.1	Partie a . . . . .	3
3.2.2	Partie b . . . . .	4
3.3	Partie 3 . . . . .	4
3.4	Partie 4 . . . . .	4
3.5	Partie 5 . . . . .	5
3.6	Partie 6 . . . . .	6
3.7	Partie 7 . . . . .	6
3.8	Partie 8 . . . . .	6
3.9	Partie 9 . . . . .	7
<b>4</b>	<b>Observation, interprétation et conclusion</b>	<b>7</b>

# **1 Introduction**

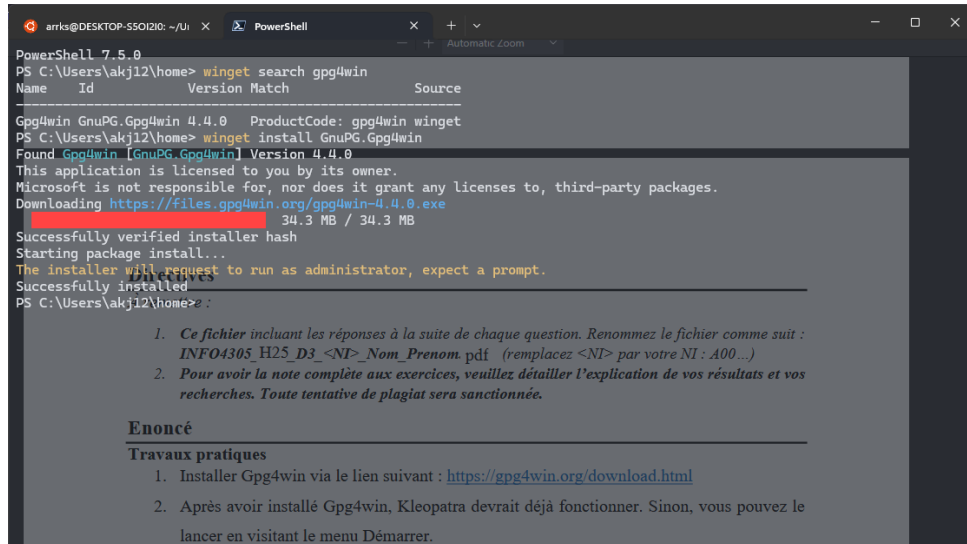
## **2 Objectif du TP**

[Les objectifs du TP]

## 3 Déroulement du TP

### 3.1 Partie 1

Premièrement on doit d'abord installer Gpg4win, j'ai installer le logiciel à l'aide du manager de paquets WinGet (voir la figure 1).



```
PowerShell 7.5.0
PS C:\Users\akj12\home> winget search gpg4win
Name      Id          Version Match          Source
-----
Gpg4win   GnuPG.Gpg4win 4.4.0   ProductCode: gpg4win winget
PS C:\Users\akj12\home> winget install GnuPG.Gpg4win
Found Gpg4win [GnuPG.Gpg4win] Version 4.4.0
This application is licensed to you by its owner.
Microsoft is not responsible for, nor does it grant any licenses to, third-party packages.
Downloading https://files.gpg4win.org/gpg4win-4.4.0.exe
34.3 MB / 34.3 MB
Successfully verified installer hash
Starting package install...
The installer will request to run as administrator, expect a prompt.
Successfully installed
PS C:\Users\akj12\home>
```

**Travaux pratiques**

1. Ce fichier incluant les réponses à la suite de chaque question. Renommez le fichier comme suit : **INFO4305\_H25\_D3\_<NI>\_Nom\_Prenom.pdf** (remplacez <NI> par votre NI : A00...)
2. Pour avoir la note complète aux exercices, veuillez détailler l'explication de vos résultats et vos recherches. Toute tentative de plagiat sera sanctionnée.

**Enoncé**

**Travaux pratiques**

1. Installer Gpg4win via le lien suivant : <https://gpg4win.org/download.html>
2. Après avoir installé Gpg4win, Kleopatra devrait déjà fonctionner. Sinon, vous pouvez le lancer en visitant le menu Démarrer.

Figure 1: Installation de Gpg4win

### 3.2 Partie 2

#### 3.2.1 Partie a

Pour créer une paire de clé à l'aide de l'interface graphique, on doit ouvrir le logiciel Kleopatra, ensuite on selectionne l'option new key pair (voir la figure 2).

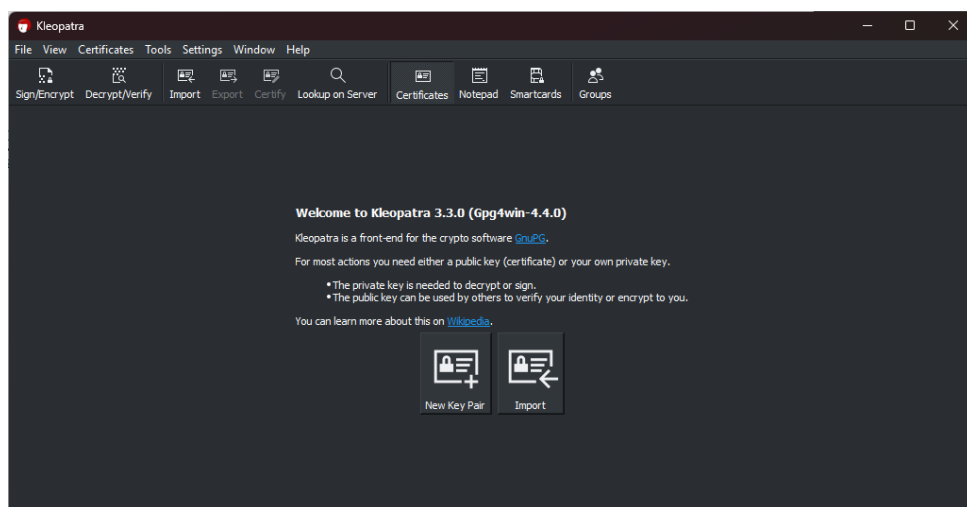


Figure 2: Menu initial Kleopatra

Ensuite, on doit sélectionné options avancés et puis rsa2048. On doit aussi remplir notre nom et notre courriel pour le certificat (voir 3).

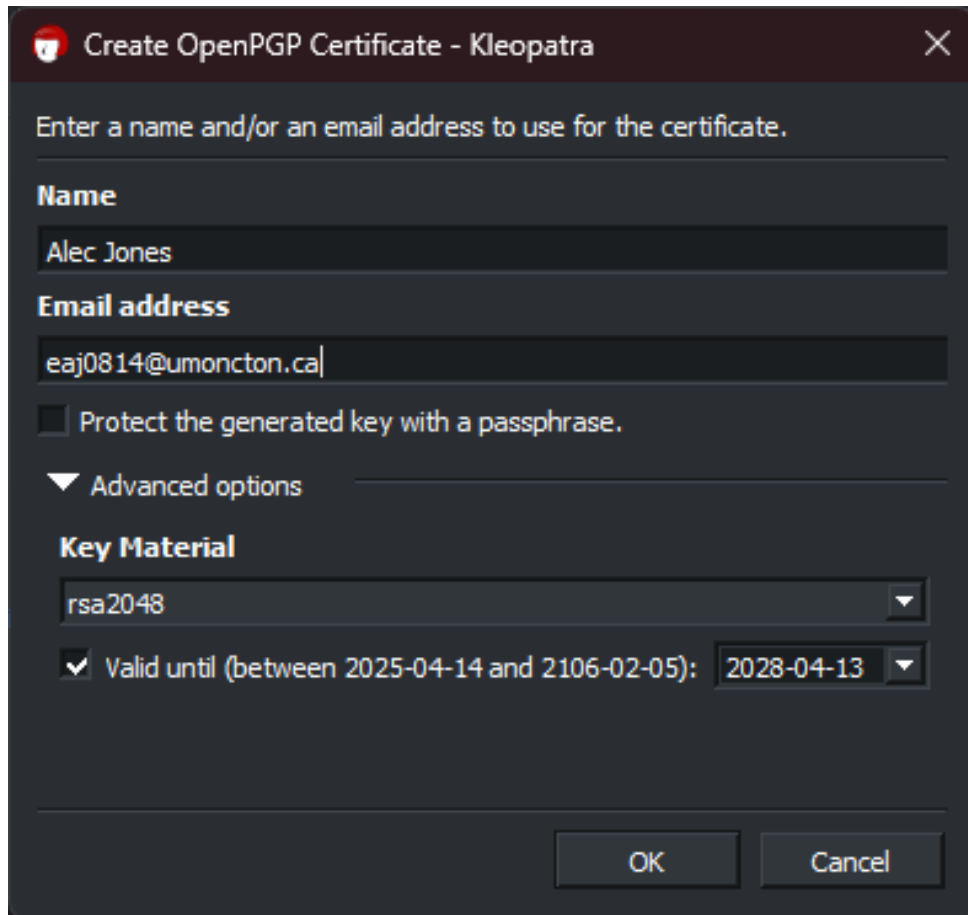


Figure 3: Création de clés dans Kleopatra

### 3.2.2 Partie b

Pour créer une paire de clé en ligne de commande, vous pouvez utiliser la commande suivante dans un terminal :

```
gpg --full-generate-key
```

Cette commande lance un assistant interactif vous permettant de choisir le type de clé, la longueur (par exemple, rsa2048 ou rsa4096) et de renseigner les informations nécessaires (nom, adresse électronique, etc.). Une fois terminé, votre paire de clés sera générée et stockée dans votre trousseau GPG (voir figure 4).

## 3.3 Partie 3

Pour Lister notre trousseau de clés, on peut utiliser la commande suivante:

```
gpg --list-keys
```

En exécutant la commande on aperçoit les deux clés créés précédemment (voir figure 5).

## 3.4 Partie 4

Pour exporter les clés publiques, on utilise la commande:

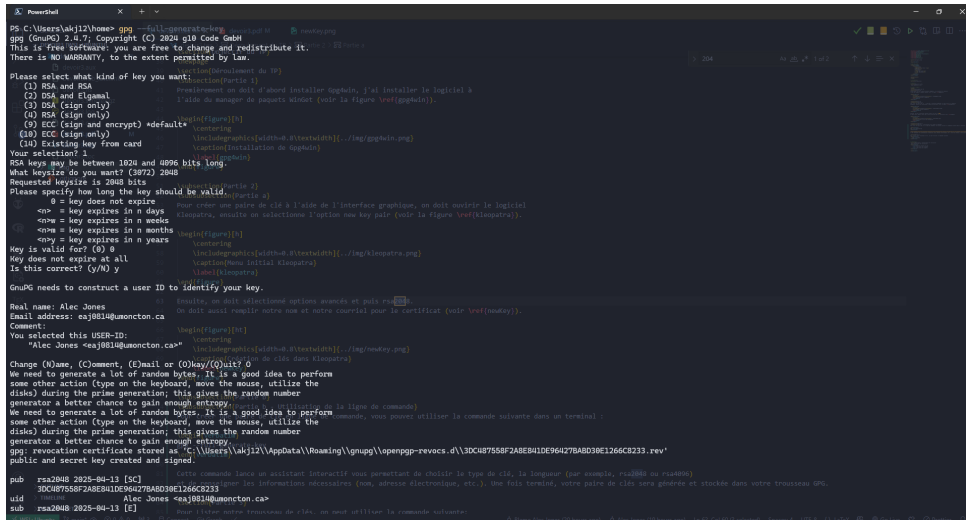


Figure 4: Création de clés à l'aide de la ligne de commande

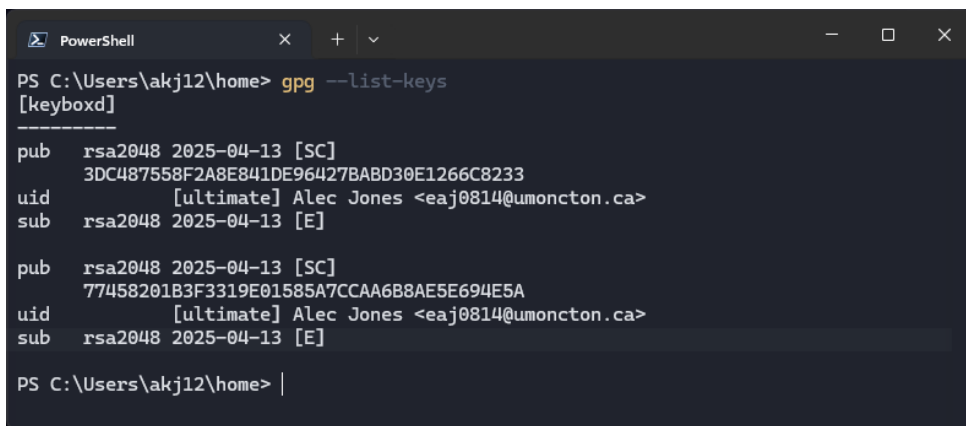


Figure 5: Liste des clés

```
gpg --armor --output maclé.asc --export UserID
```

Puisqu'on spécifie le UserID, par exemple ej0814@umoncton.ca, qui a été utiliser dans les deux clés, on obtient la concaténation des deux dans un fichier. On remarque alors que maclé.asc est effectivement la concaténation des deux clés publiques créer tout à l'heure.

### 3.5 Partie 5

Pour chiffrer un fichier, on utilise la commande suivante (voir figure 6 pour un exemple):

```
gpg -er UserID document.txt
```



Figure 6: text clair à gauche, chiffrer à droite

## 3.6 Partie 6

Si on voulait ensuite déchiffrer ce texte, on utiliserait la commande suivant :

```
gpg --output doc --decrypt doc.gpg
```

## 3.7 Partie 7

Pour signer un document et laisser le text en clair, on utilise la commande suivante (Voir la figure 7 pour exemple de résultat):

```
gpg --clearsign document.txt
```

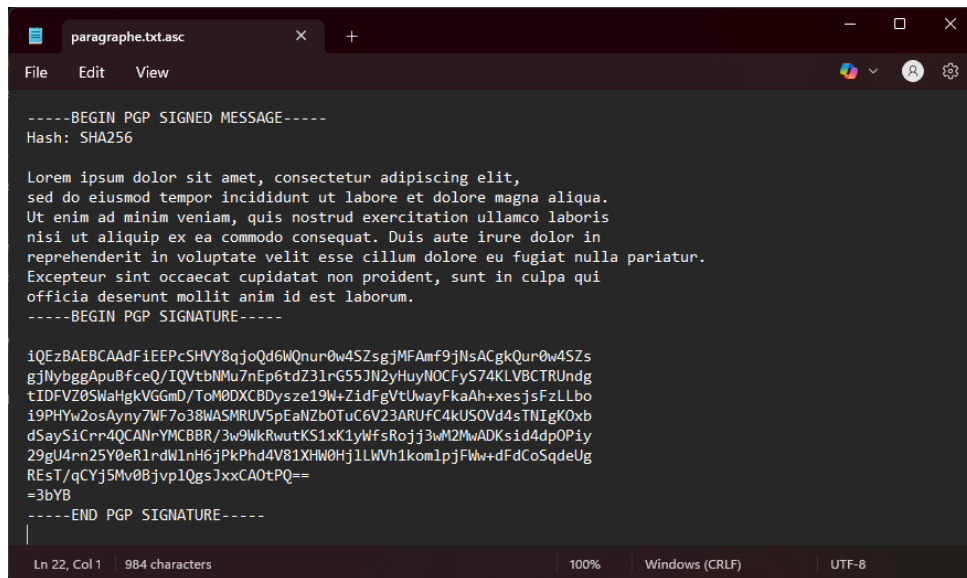


Figure 7: Document signé

## 3.8 Partie 8

Pour vérifier la signature, on utilise la commande suivante (voir figure 8):

```
gpg --verify document.txt.asc
```

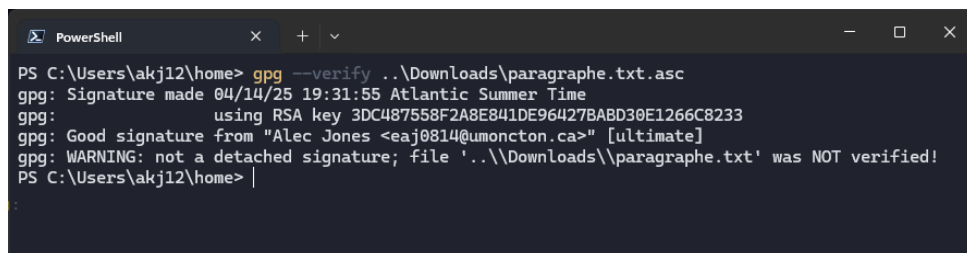
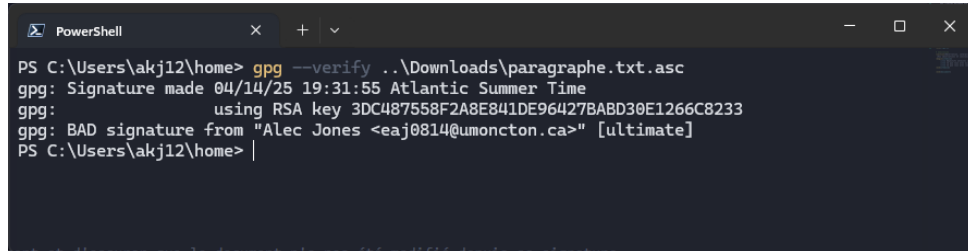


Figure 8: Vérification de la signature

### 3.9 Partie 9

L'utilité de la signature dans ce contexte est de garantir l'intégrité du document et d'assurer que le document n'a pas été modifié depuis sa signature. En vérifiant la signature, on peut s'assurer que le document provient bien de la personne qui l'a signé et qu'il n'a pas été altéré. (voir figure 9 pour un exemple de document modifier).



```
PS C:\Users\akj12\home> gpg --verify ..\Downloads\paragraphe.txt.asc
gpg: Signature made 04/14/25 19:31:55 Atlantic Summer Time
gpg:          using RSA key 3DC487558F2A8E841DE96427BABD30E1266C8233
gpg: BAD signature from "Alec Jones <eaj0814@umoncton.ca>" [ultimate]
PS C:\Users\akj12\home> |
```

Figure 9: Vérification de la signature sur un document modifié, le premier mot a été enlevé

## 4 Observation, interprétation et conclusion

[Vos observations et conclusions]

- Objectifs atteints ou non
- Ce que vous avez accompli
- Ce que vous avez compris