

# 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
<b>4</b>	<b>Observation, interprétation et conclusion</b>	<b>5</b>

# **1 Introduction**

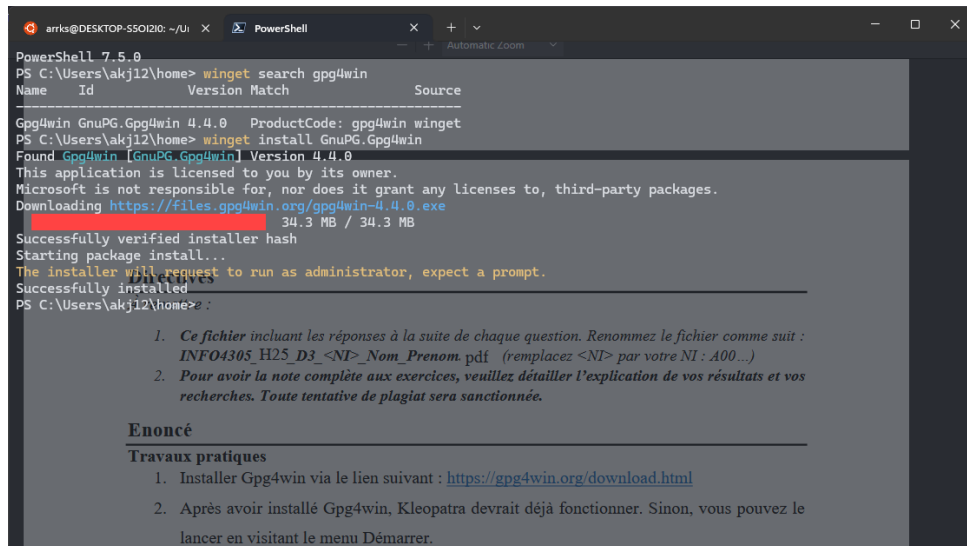
## **2 Objectif du TP**

[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).

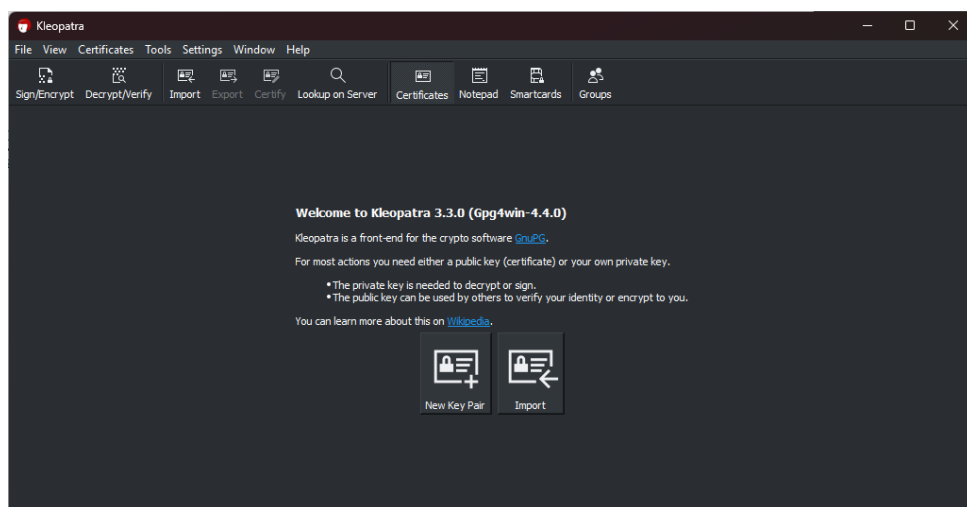


Figure 2: Menu initial Kleopatra

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

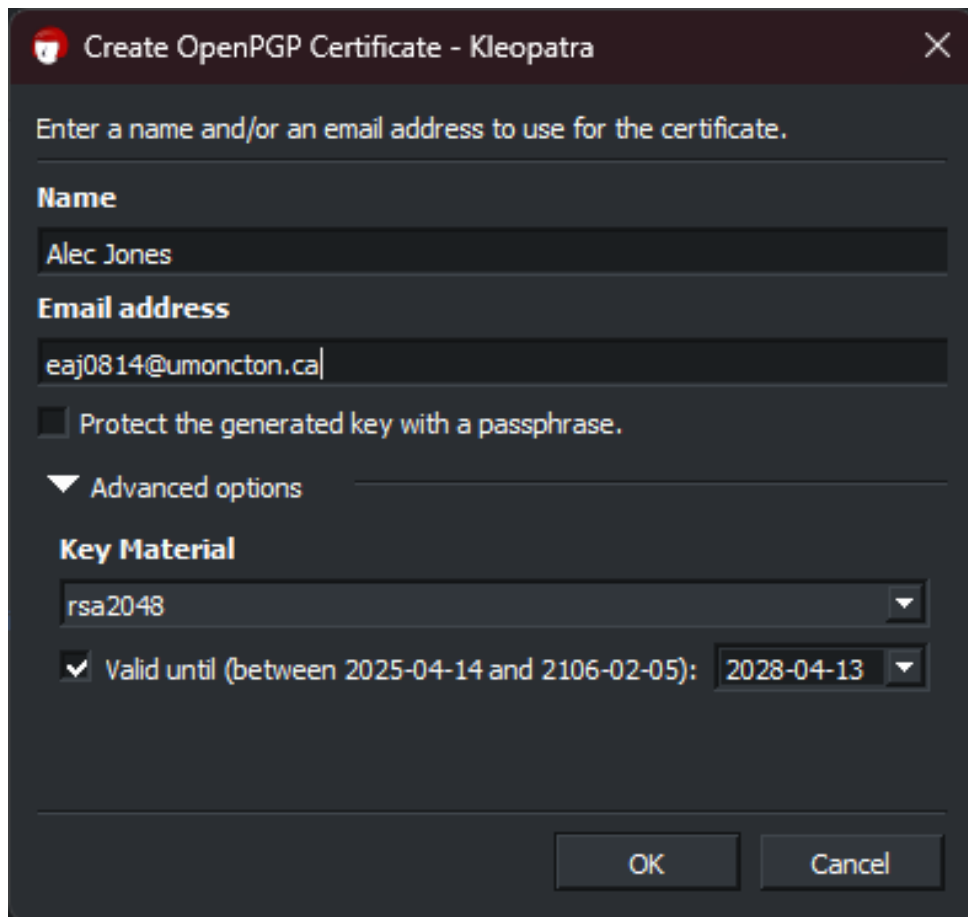


Figure 3: Création de clés dans Kleopatra

### 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 apperçoit les deux clés créés précédemment (voir figure 5).

## 3.4 Partie 4

Pour exporter les clés publiques, on utilise la commande:

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

```

PS C:\Users\akj12\home> gpg
gpg (GnuPG) 2.0.7; Copyright (C) 2004 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
(2) DSA and ElGamal
(3) DSA (sign only)
(4) RSA (sign only)
(0) ECC (sign and encrypt) *default*
(10) ECC (sign only)
(14) Existing key from card
Your selection: 1
RSA keys may be between 1024 and 4096 bits long;
Requested keysize is 2048 bits
What keysize do you want? (3072) 2048
Please specify how long the key should be valid.
0 = key does not expire
<#> = key expires in # days
<#w> = key expires in # weeks
<#m> = key expires in # months
<#y> = key expires in # 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: Alec Jones
Email address: eaj0814@umoncton.ca
Comment:
You selected this USER-ID:
"Alec Jones <eaj0814@umoncton.ca>"

Change (N)ame, (C)omment, (E)mail or (O)key/(O)ut? 0
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
disk) 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
disk) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: revocation certificate stored as 'C:\Users\akj12\AppData\Local\Temp\gpg-revocs.d\3DC487558F2A8E841DE96427B8BD30E1266C8233.rev'
public and secret key created and signed.

pub rsa2048 2025-04-13 [SC]
3DC487558F2A8E841DE96427B8BD30E1266C8233
uid [ultimate] Alec Jones <eaj0814@umoncton.ca>
sub rsa2048 2025-04-13 [E]
  
```

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

```

PS C:\Users\akj12\home> gpg --list-keys
[keyboard]

-----

pub rsa2048 2025-04-13 [SC]
3DC487558F2A8E841DE96427B8BD30E1266C8233
uid [ultimate] Alec Jones <eaj0814@umoncton.ca>
sub rsa2048 2025-04-13 [E]

pub rsa2048 2025-04-13 [SC]
77458201B3F3319E01585A7CCAA6B8AE5E694E5A
uid [ultimate] Alec Jones <eaj0814@umoncton.ca>
sub rsa2048 2025-04-13 [E]

PS C:\Users\akj12\home>
  
```

Figure 5: Liste des clés

## 4 Observation, interprétation et conclusion

[Vos observations et conclusions]

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