Guided Exercises

1. Complete the table by providing the correct filename:

Description	**Filename**
Trust database	
Directory for revocation certificates	
Directory for private keys	
Public keyring	

2. Answer the following questions:
   - What type of cryptography is used by *GnuPG*?
   - What are the two main components of public key cryptography?
   - What is the `KEY-ID` of the public key fingerprint `07A6 5898 2D3A F3DD 43E3 DA95 1F3F 3147 FA7F 54C7`?
   - What method is used to distribute public keys at a global level?
3. Put the following steps in the right order concerning private key revocation:
   - Make the revoked key available to your correspondents.
   - Create a revocation certificate.
   - Import the revocation certificate to your keyring.

   The correct order is:

Step 1:	
Step 2:	
Step 3:	

4. Regarding file encryption, what does the `--armor` option imply in the command `gpg --output encrypted-message --recipient carol --armor --encrypt unencrypted-`

`message`?

Explorational Exercises

1. Most `gpg` options have both a long and a short version. Complete the table with the corresponding short version:

Long version	Short version
`--armor`	
`--output`	
`--recipient`	
`--decrypt`	
`--encrypt`	
`--sign`	

2. Answer the following questions concerning key export:
   - What command would you use to export all of your public keys to a file called `all.key`?
   - What command would you use to export all of your private keys to a file called `all_private.key`?

3. What `gpg` option allows for carrying out most key management related tasks by presenting you with a menu?

4. What `gpg` option allows you to make a cleartext signature?