Answers to Guided Exercises

1. Complete the table by providing the correct file name:

Description	**Filename**
Trust database	`trustdb.gpg`
Directory for revocation certificates	`opengp-revocs.d`
Directory for private keys	`private-keys-v1.d`
Public keyring	`pubring.kbx`

2. Answer the following questions:

   - What type of cryptography is used by *GnuPG*?

     Public key cryptography or asymmetric cryptography.

   - What are the two main components of public key cryptography?

     The public and the private keys.

   - What is the `KEY-ID` of the public key fingerprint `07A6 5898 2D3A F3DD 43E3 DA95 1F3F 3147 FA7F 54C7`?

     `FA7F 54C7`

   - What method is used to distribute public keys at a global level?

     Key servers.

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:	Create a revocation certificate
Step 2:	Import the revocation certificate to your keyring

Step 3:	Make the revoked key available to your correspondents

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

   It produces ASCII armored output, which allows you to copy the resulting existing encrypted file into an email.

Answers to 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`	`-a`
`--output`	`-o`
`--recipient`	`-r`
`--decrypt`	`-d`
`--encrypt`	`-e`
`--sign`	`-s`

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`?

     `gpg --export --output all.key` or `gpg --export -o all.key`

   - What command would you use to export all of your private keys to a file called `all_private.key`?

     `gpg --export-secret-keys --output all_private.key` or `gpg --export-secret-keys -o all_private.key` (`--export-secret-keys` can be replaced by `--export-secret-subkeys` with a slightly different outcome — check `man pgp` for more information).

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

   `--edit-key`

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

   `--clearsign`