## Moodle exercise

The following files are on Moodle zipped together for you to download and extract.

* ***veronicaspublickey.pem***
* ***keysymm***
* ***calendar.pdf***
* ***daycare.bin***
* ***secretsig.bin***
* ***peterspublickey.pem***

1. Encrypt the file **calendar.pdf** with each of the following symmetric encryption algorithms and make a note of the average (user) time taken in each case (use the **time** command). You should create a 256 bit key file to use for all the encryptions. Please fill in your timings below to the nearest tenth of a second.

\_\_\_\_\_\_\_\_ 256-bit AES (in CBC mode)

\_\_\_\_\_\_\_\_ DES

\_\_\_\_\_\_\_\_ Triple DES

\_\_\_\_\_\_\_\_ RC4

\_\_\_\_\_\_\_\_ Blowfish (*bf* in OpenSSL)

1. Decrypt the file **daycare.bin** with the symmetric key supplied (**keysymm**). Use the OpenSSL implementation of the **des3** algorithm. The plaintext should be a text file. Read the decrypted file and write the contents below.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. You have a file named **secretsig.bin** which has been signed by either Peter or Veronica. Using the keys provided on Moodle can you find out which one of them has signed the file? Write your answers below:

What are the contents of the file? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Who signed the file? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

How did you find out? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Swop your sheet with your partner and correct each other’s work**