# Security Practical Test Week 6 (Feb/Mar 2018)

## Set-up information

You can complete this test anywhere that you can run OpenSSL. You will need to download some files to complete some questions on this paper. **Make sure to clear the contents of the download folder on the machine you are using before you begin.** The files are located on Moodle and are named as follows:

|  |
| --- |
| **symkey** |
| **secondsymkey** |
| **privateRSA.pem** |
| **publicRSA.pem** |

|  |
| --- |
| **names.bin** |
| **relations.bin** |
| **setup.bin** |
| **rota-sig.bin** |

## Questions – Part A Symmetric Encryption

Q1(a) Decrypt the file **names.bin** using the OpenSSL implementation of the **bf-cbc** algorithm. It was encrypted using the key named **symkey** Name the output file from your OpenSSL decryption command **found.txt**. Write the contents of the file here:

Q2(a) The file **relations.**bin has been encrypted. Can you decrypt this file using one of the keys available on Moodle and a **symmetric** encryption algorithm (des-cbc)? If you can write Cousin Marty’s age here: