**Lab 6**

**Hash Lab 1**

**Secure Comms 2018-19, james Finglas, B00094138**

1. What is the MD5 of the file hashme.txt?

622E9F7F585ADB048DD3E55A4F228B03

1. What is the SHA1 of the same file?

A5C91D3CC789776D859161BFFC9965054CF924F3

1. Are the MD5 and SHA1 hashes the same length? Explain why you think this is the case?

No. This is the case, because MD5 is only 64-bit encryption where as SHA1 is 128, leading to more bits, and therefore a longer hash.

1. Do you think your hashes match your classmate’s hashes? Why?

Yes. Hashes are not unique when generated on a different computer, if the hash to be calculated is of an identical file. This is a unique identify to that file, or copy of that file, not any one copy of the file. This allows the hash to be reversed, or decrypted, on any computer.

1. Open your hashme.txt file and add a space after one of the numbers. Recalculate both the MD5 andSHA1 hashes. Have they changed much if at all from the original hashes we calculated?

New hash of hashme.txt = 12BDD1BA7E528693A1F5C3232694C216. The file has altered significantly as it is no longer the same file.

1. If you changed the file name to hashme1.txt and recalculate the hashes, do you think the hashes will change? Test and see what actually happens.

No. Altering the name of the file does not alter the contents of the bits of the file, so the hash will not change. New hash of file hashme1.txt = 12BDD1BA7E528693A1F5C3232694C216

1. .
2. .
3. .
4. .
5. ..