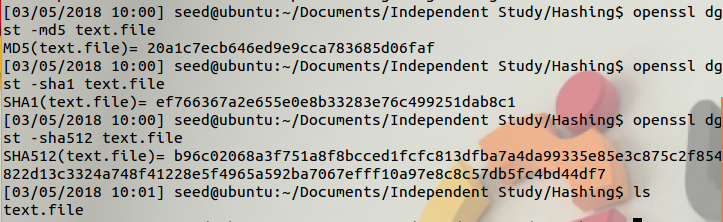
Garrett Bogart

Daniel Oliveros

Hashing

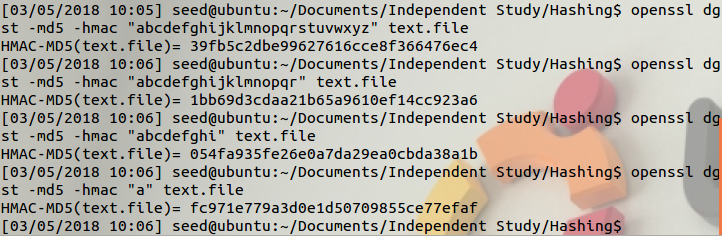
**Task 3.1**

Hashing text.file with md5, sha1, and sha256 we can see that each hash algorithm gives us a different hash of the same file.

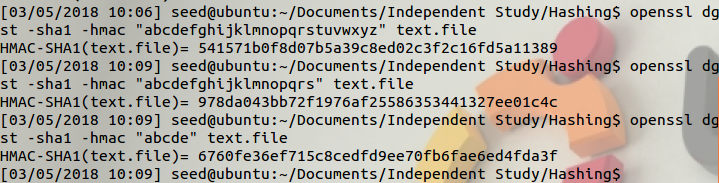


**Task 3.2**

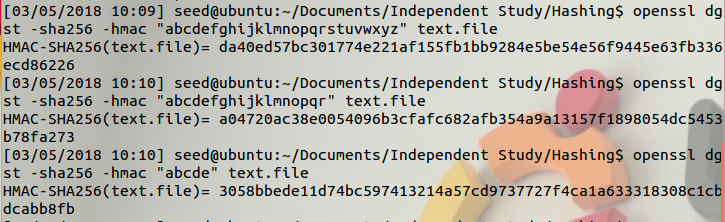
Md5 hmac hash



Sha1 hmac hash

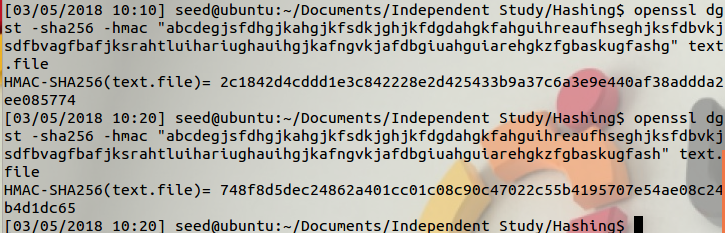


Sha256 hmac hash



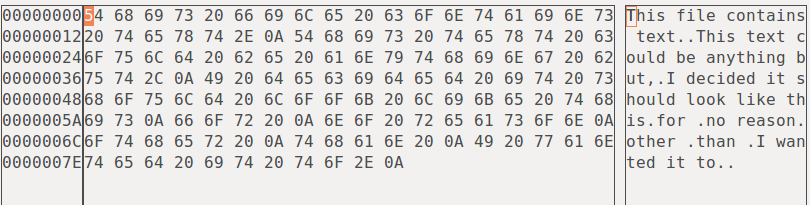
It can be seen that varying the key produces unique hashes by the same hash algorithm. Further each hash algorithm produces its own unique hash.

The length of the key can be any length. The key itself is used to derive an inner key and an outer key. Generally a 32 byte key is sufficient because it provides sufficient entropy that the key wont be guessable. For fun I made a lengthy key and only changed it by one letter and got a different hash.



**Task 3.3**

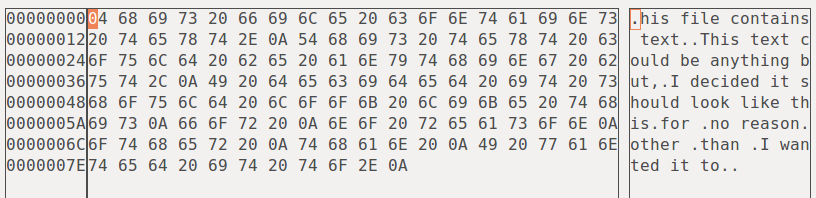
Taking a hash of text.file. Looking at the file in ghex



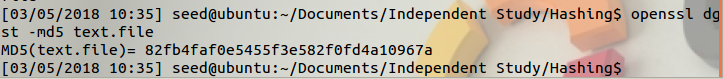
Then taking the hash



Changing a single bit



Taking the same hash again



The two hash are share no discernable similarities other than being made up of the same character set.