Trent Giever

Ch 3 Basic Cryptography

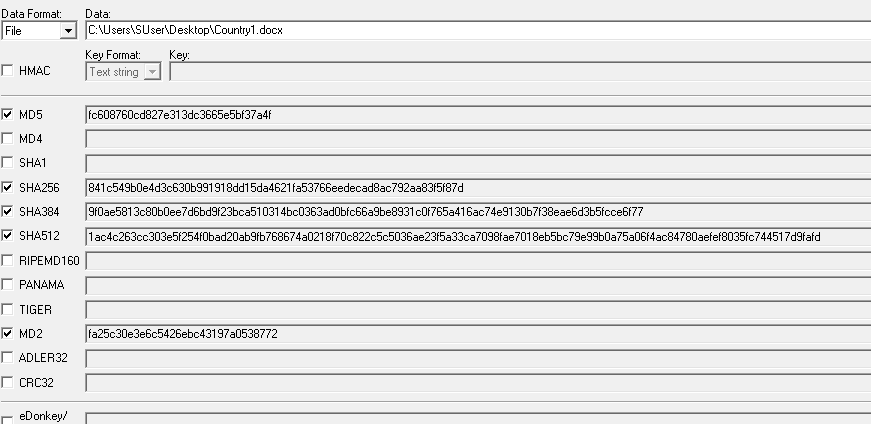
Project 3-3 and 3-4

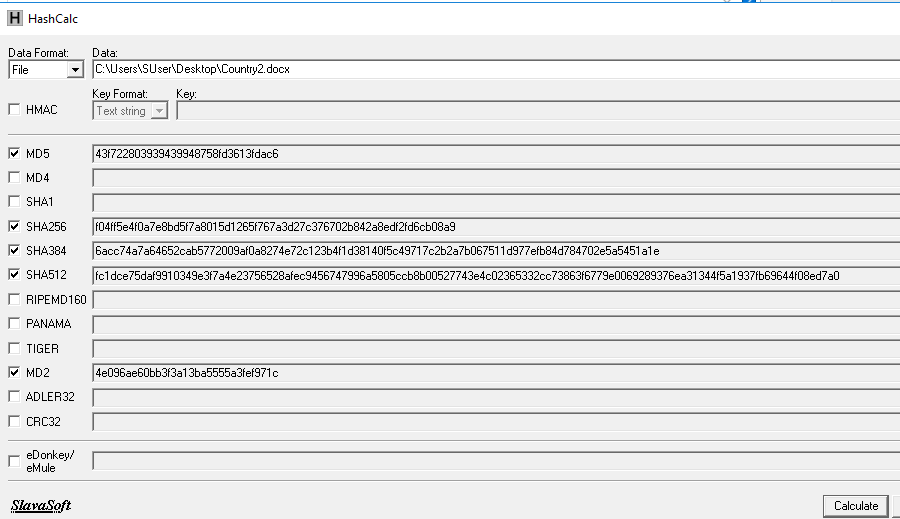
7/5/18

Project 3-3 Installing GUI Hash generator and comparing digests

3-3-16 – What can you say about the digests? Compare MD2 with SHA512. What makes SHA512 better than MD2? Why?

The first thing I noticed when I saw the results was that the SHA512 was by far the best algorithm in length. The MD2 and MD5 looked to have about the same number of characters in the hashing. The SHA256 seamed to have about double the length of characters than MD5 does. The SHA384 seemed to have the SHA256 plus MD5 in length and is a similar pattern for SHA 512. The overall pattern is each one is a factor of MD2/5, so SHA256 is two times, SHA384 is three times, and SHA512 is four times MD2/5. The hashing is deferent in each type but is more secure by how long it is. The only difference between MD2 and SHA512 is that having about 4 times the size of characters makes it more secure and less hack prone.





3-3-22 Are the digits different? What does this tell you about hashing digests?

The digits are different because every character and symbol counts in the encryption. The hashing output looks different because having similar outputs would make it easy for computers to crack the decryption program. This tells me that encryption is secure for having a different gibberish for similar items.

Project 3-4 Using Microsoft Encrypting File System

3-4-11 Was there any delay in the operation?

I could not see any delay from loading an encrypted word document. The document loaded fast like it was not protected.

3-4-12 Was it faster or slower?

I could not see any difference in speed between the encrypted and non-encrypted documents.