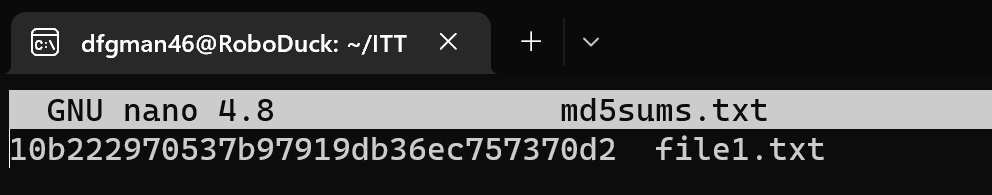
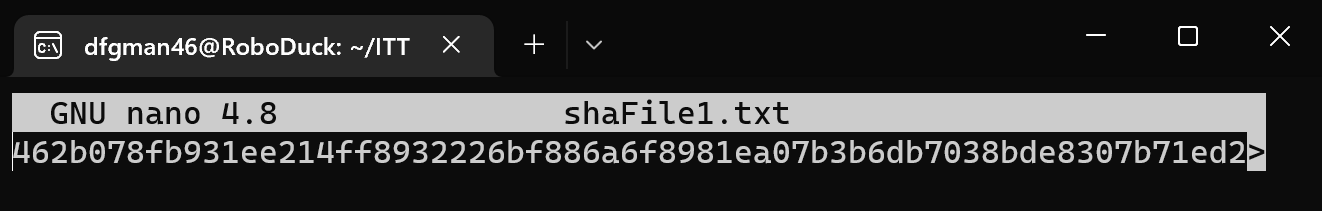
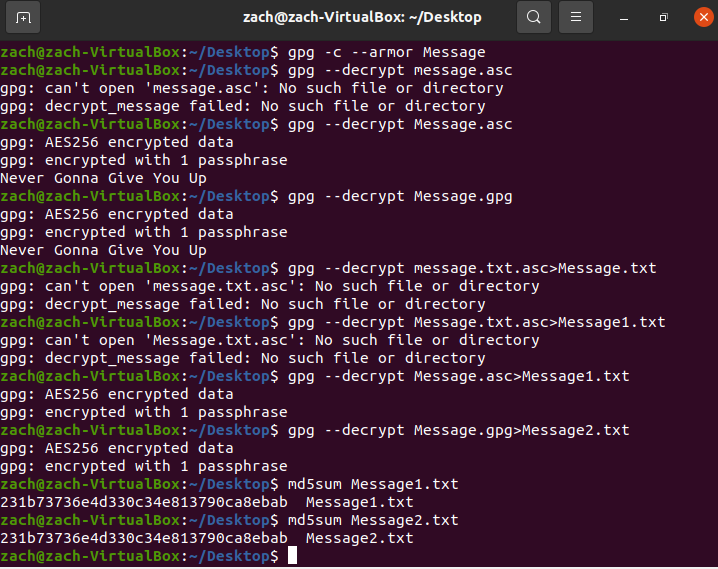
1. **Explain what hashing does and how it is different from encryption.**

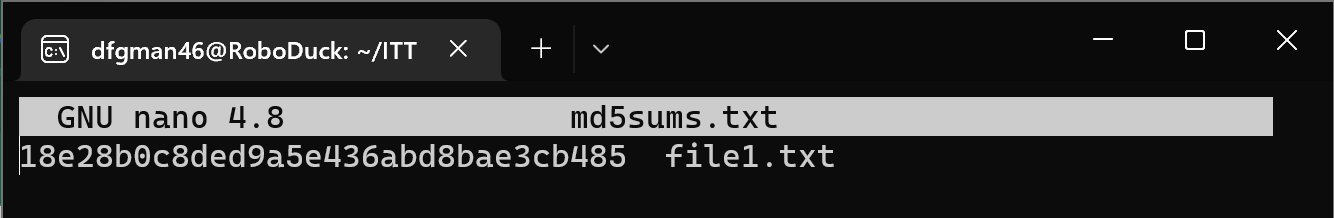
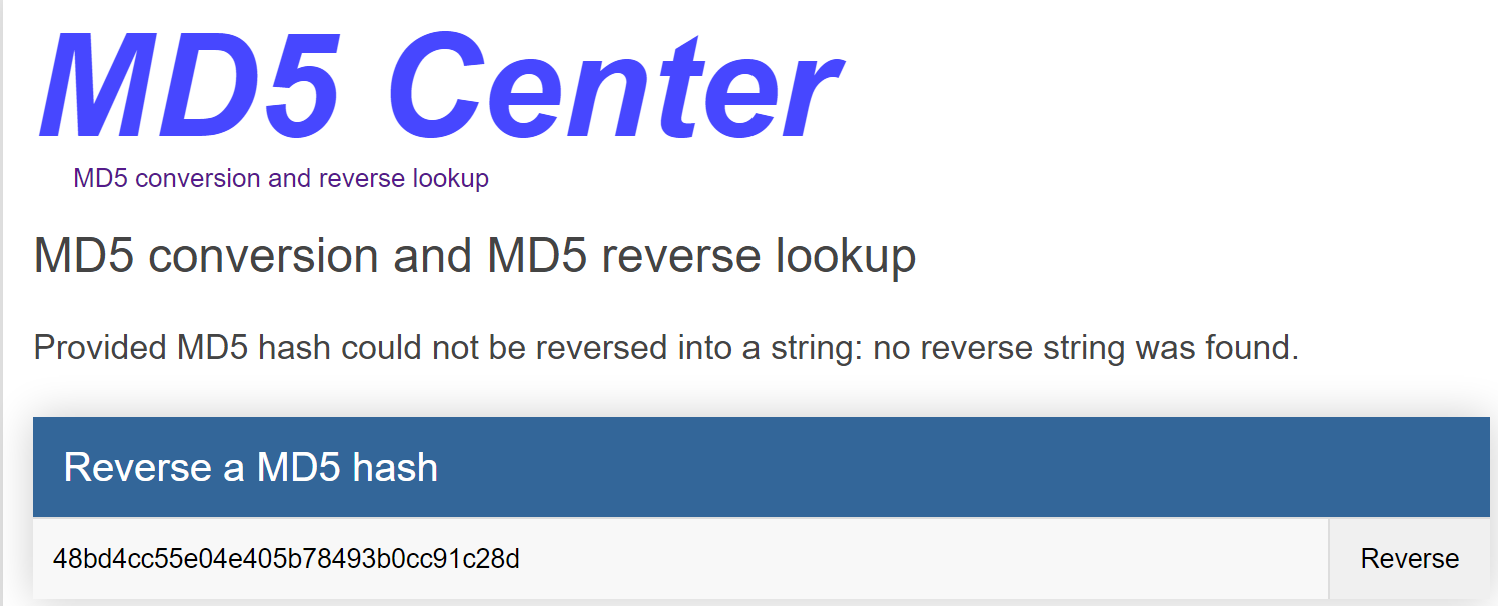
An algorithm is used to map data of any size to a fixed length through the process of hashing. The hashing function is one-way, unlike encryption (Nohe, 2021). Although possible, the computing power required for reverse-hashing makes it impractical. While data is in transit, hashing ensures that it has not been altered, thereby proving its authenticity. Essentially, it is a sort of check, (Nohe, 2021).

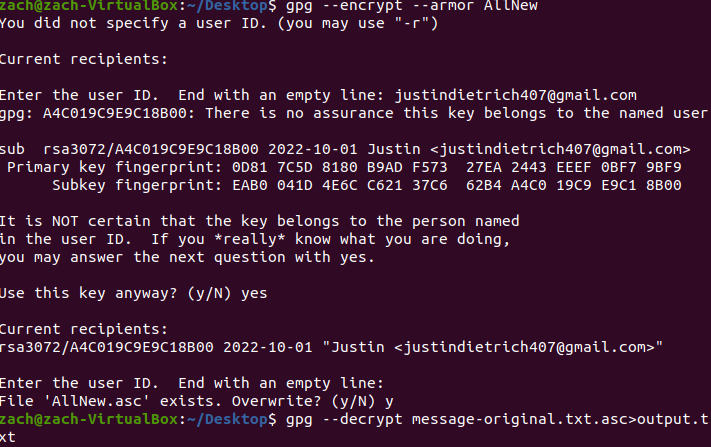
The encryption process, on the other hand, encrypts texts and other information that can only be accessed by a single entity with the decryption key. You can rest assured that cybercriminals will not be able to access any of your sensitive data. In fact, in modern communication systems, encryption is the best method of ensuring data security (The SSL Store, 2022). Passwords or keys are required to decrypt encrypted messages so they can be read by the receiver.

In short, encryption can be defined as a two-way function since it encrypts and decrypts the information using a key, while hashing can be defined as a one-way function because it converts plain text into an irreversible, unique code.

1. **Demonstrate the use of shasum or md5 or both.**
   1. **Figure 1:** Creating a text file with apassword for the hashing algorithm  
      
   2. **Figure 2:** Using MD5 as a hashing algorithm  
      
   3. **Figure 3:** Using sha512sum as a hashing algorithm  
      
2. **Change one character of a password and compare hashes. The hash results should be different even in the case of a minor change.  
   **

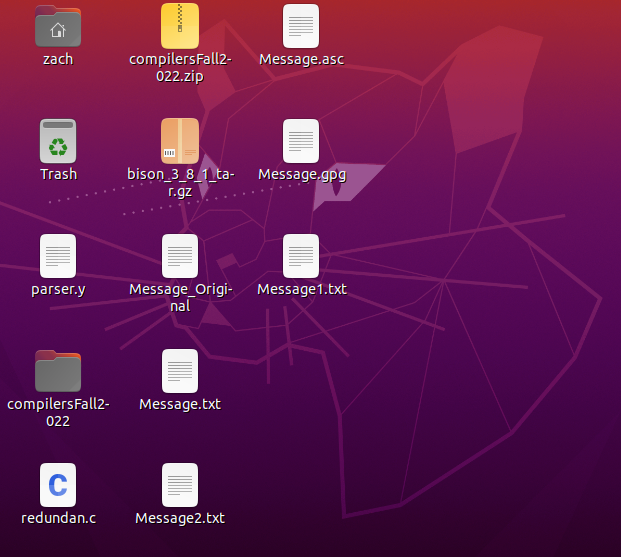
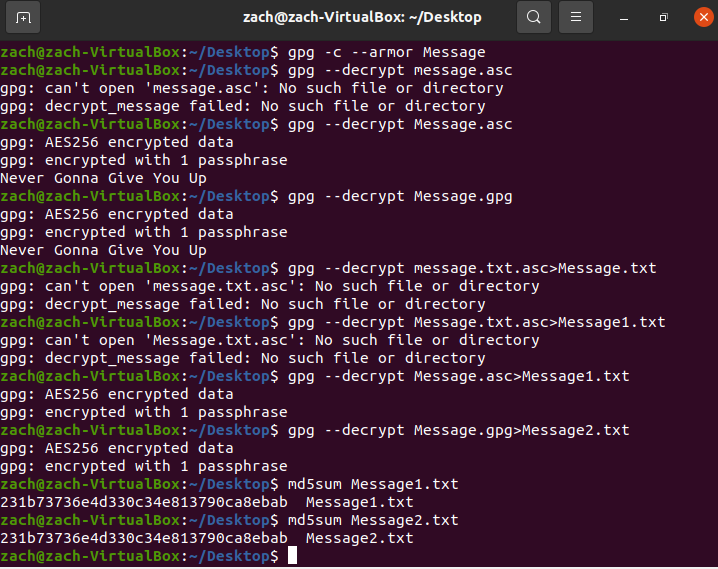
**Demonstrate the weakness of MD5.**

* 1. **Create some md5 hashed passwords for common words “steelers,” “Cardinals,” “superman,” etc.**
  2. **Try to find the hash string using a simple Google search.**   
     
  3. **Hash some slightly more complex passwords using MD5. Search Google for the hashes. Determine how complex a password needs to be in order to avoid being hacked by a rainbow table result.**  
     A reverse string could not be found for passwords that were already given (*MD5 Hash Generator*). Searches of several sources did not yield the reverse string. A more complex password never hurts, however! (As long as you remember it!)

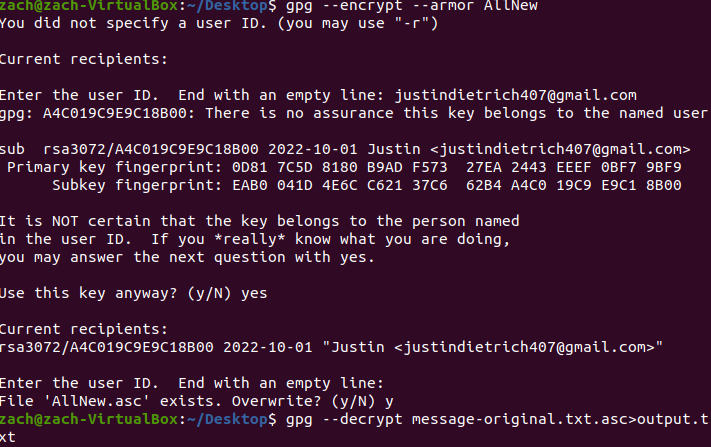
**1. Encrypt a file using default settings.**  


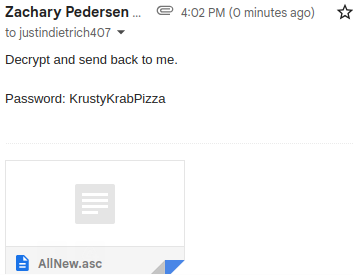
The contents of the file will be encrypted, and a new one is created. A text editor will not be able to display this file properly.

**2-4. Encrypt a file that can be copied into an email message. The armor option creates an output file that contains only ASCII standard characters instead of the default (and unreadable by a text editor) binary format. Decrypt the two files and verify they have not changed.**

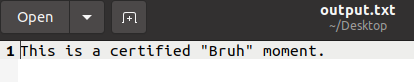


**5. Create and share keys!**



**6. Email a friend!**  


**7. Decrypt!**

****

References

Dan's Tools. (n.d.). MD5 Hash Generator. Retrieved October 2, 2022, from https://www.md5hashgenerator.com/

Nohe, P. (2021, March 24). The difference between encryption, hashing and salting. Hashed Out by The SSL Store™. Retrieved October 2, 2022, from https://www.thesslstore.com/blog/difference-encryption-hashing-salting/

SSL2BUY. (2022, April 12). Difference between hashing and encryption. SSL2BUY Wiki - Get Solution for SSL Certificate Queries. Retrieved October 2, 2022, from https://www.ssl2buy.com/wiki/difference-between-hashing-and-encryption