Information Systems Security - Practical 9

cryptography

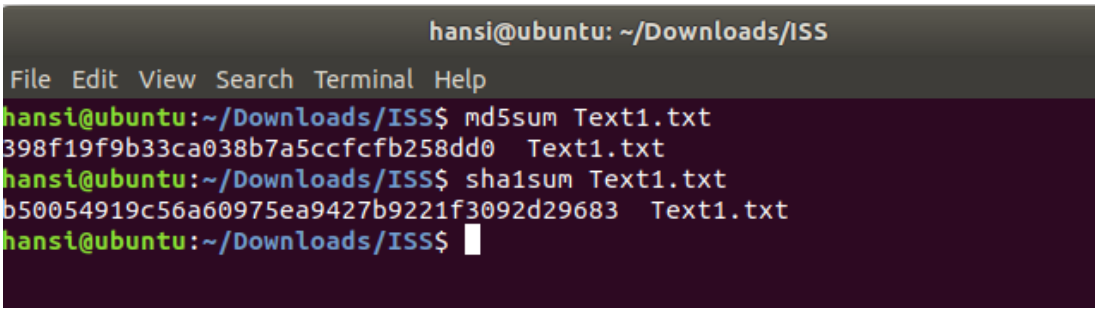
W.H.M.Gunathilaka
18020275

IS2109 Information Systems Security - Practical 9

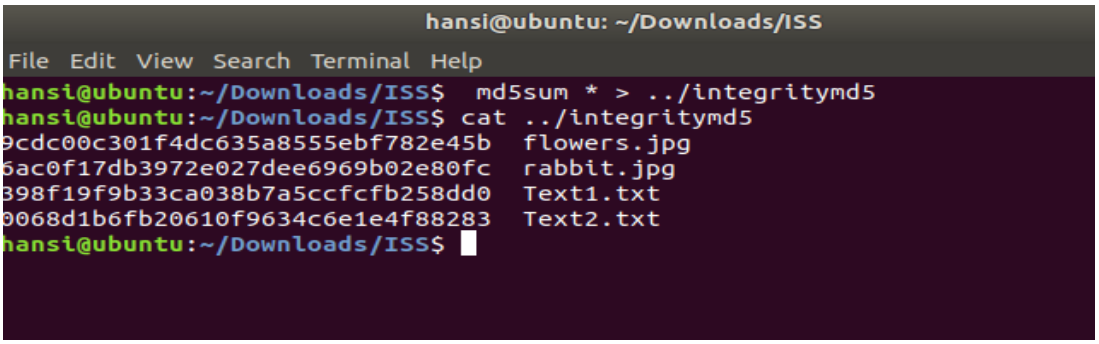
Cryptography

Checking integrity

1.

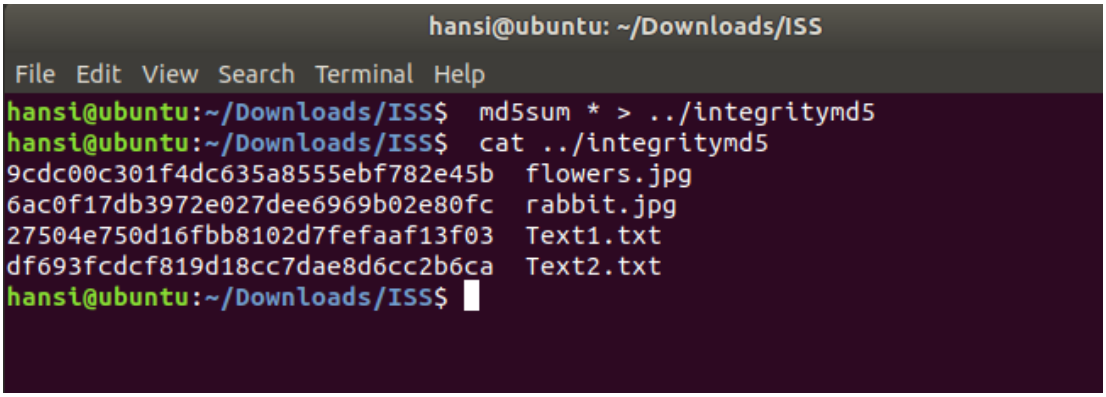


2.



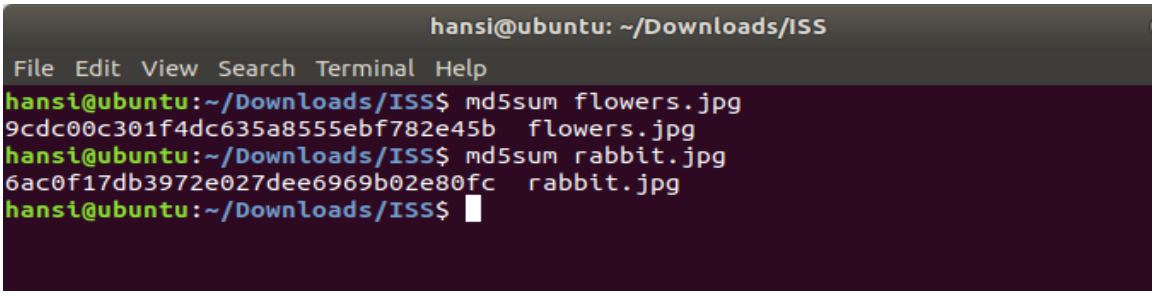
3.

I have changed the Text1.txt file. Getting md5 hash value after the change we can see that hash value is changed. That means we can identify that file has changed.



Collisions in MD5 and SHA-1

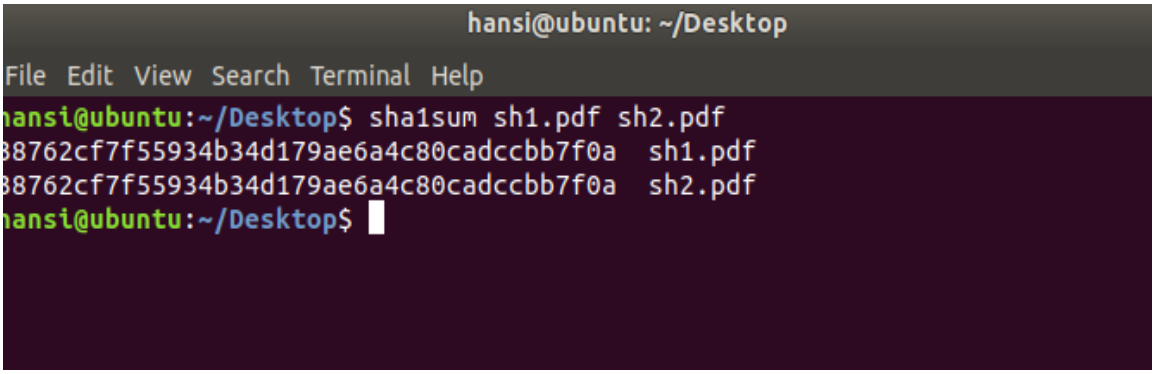
1.



2.

There might be some setups which are not released by NetBeans. So that they can harm the computer after installing that kind of software. Therefore, to check whether the software setup is original one, the hash value is given to check with it.

3.



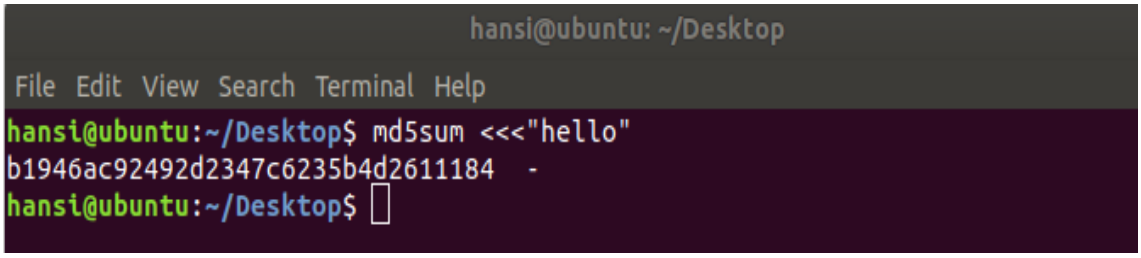
Both files show the same sha value here.

Reverse Hashing

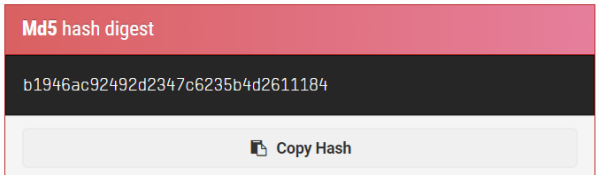
1.

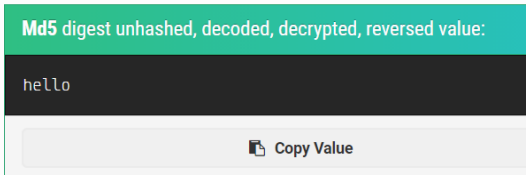
Passwords usually stored as hash value in the databases in the system. Reversing hash value to the password is quite impossible. So that the websites will prompt us to change to new password instead of sending password to us.

2.

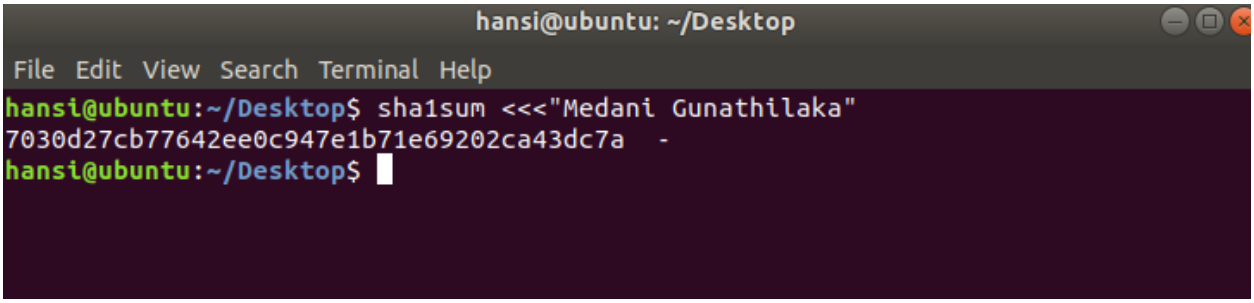


I googled it and it reversed successfully.

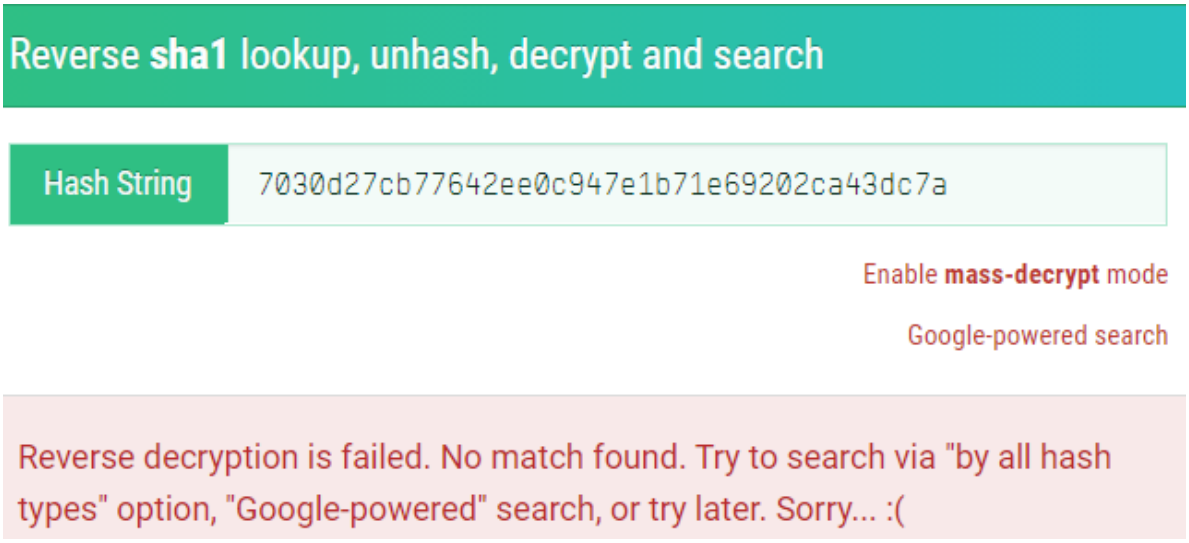




3.



Reverse decryption is failed here.



4.

These websites have stored the hash values of some common phrases such as "hello" and reverse the search when requested by users. But the specific names were not included in these pages.

5.

We should have a habit of using very strong passwords rather than using common names, birthdays, name of countries etc... If we use a password strongly, the hash reverse lookup sites would not have the reversed password for the hash value of the password. Therefore, no one can find the password from the hash value even hacked.