



Information Systems Security - Practical 9

cryptography



IS2109 Information Systems Security - Practical 9

Cryptography

Checking integrity

1.

```
hansi@ubuntu: ~/Downloads/ISS
File Edit View Search Terminal Help
hansi@ubuntu:~/Downloads/ISS$ md5sum Text1.txt
398f19f9b33ca038b7a5ccfcfb258dd0 Text1.txt
hansi@ubuntu:~/Downloads/ISS$ sha1sum Text1.txt
b50054919c56a60975ea9427b9221f3092d29683 Text1.txt
hansi@ubuntu:~/Downloads/ISS$
```

2.

```
hansi@ubuntu: ~/Downloads/ISS
File Edit View Search Terminal Help
hansi@ubuntu:~/Downloads/ISS$ md5sum * > ../integritymd5
hansi@ubuntu:~/Downloads/ISS$ cat ../integritymd5
9cdc00c301f4dc635a8555ebf782e45b flowers.jpg
6ac0f17db3972e027dee6969b02e80fc rabbit.jpg
398f19f9b33ca038b7a5ccfcfb258dd0 Text1.txt
0068d1b6fb20610f9634c6e1e4f88283 Text2.txt
hansi@ubuntu:~/Downloads/ISS$
```

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.

```
hansi@ubuntu: ~/Downloads/ISS
File Edit View Search Terminal Help
hansi@ubuntu:~/Downloads/ISS$ md5sum * > ../integritymd5
hansi@ubuntu:~/Downloads/ISS$ cat ../integritymd5
9cdc00c301f4dc635a8555ebf782e45b flowers.jpg
6ac0f17db3972e027dee6969b02e80fc rabbit.jpg
27504e750d16fbb8102d7fefaaf13f03 Text1.txt
df693fcdcf819d18cc7dae8d6cc2b6ca Text2.txt
hansi@ubuntu:~/Downloads/ISS$
```

Collisions in MD5 and SHA-1

1.

```
hansi@ubuntu: ~/Downloads/ISS
File Edit View Search Terminal Help
hansi@ubuntu:~/Downloads/ISS$ md5sum flowers.jpg
9cdc00c301f4dc635a8555ebf782e45b  flowers.jpg
hansi@ubuntu:~/Downloads/ISS$ md5sum rabbit.jpg
6ac0f17db3972e027dee6969b02e80fc  rabbit.jpg
hansi@ubuntu:~/Downloads/ISS$
```

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.

```
hansi@ubuntu: ~/Desktop
File Edit View Search Terminal Help
hansi@ubuntu:~/Desktop$ sha1sum sh1.pdf sh2.pdf
88762cf7f55934b34d179ae6a4c80cadccbb7f0a  sh1.pdf
88762cf7f55934b34d179ae6a4c80cadccbb7f0a  sh2.pdf
hansi@ubuntu:~/Desktop$
```

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.

```
hansi@ubuntu: ~/Desktop
File Edit View Search Terminal Help
hansi@ubuntu:~/Desktop$ md5sum <<<"hello"
b1946ac92492d2347c6235b4d2611184 -
hansi@ubuntu:~/Desktop$
```

I googled it and it reversed successfully.

Md5 hash digest
b1946ac92492d2347c6235b4d2611184
 Copy Hash

Md5 digest unhashed, decoded, decrypted, reversed value:
hello
 Copy Value

3.

```
hansi@ubuntu: ~/Desktop
File Edit View Search Terminal Help
hansi@ubuntu:~/Desktop$ sha1sum <<<"Medani Gunathilaka"
7030d27cb77642ee0c947e1b71e69202ca43dc7a -
hansi@ubuntu:~/Desktop$
```

Reverse decryption is failed here.

Reverse **sha1** lookup, unhash, decrypt and search

Hash String

7030d27cb77642ee0c947e1b71e69202ca43dc7a

Enable **mass-decrypt** mode

Google-powered search

Reverse decryption is failed. No match found. Try to search via "by all hash types" option, "Google-powered" search, or try later. Sorry... :(

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.