Index no – 18020552

University of Colombo School of Computing

IS2109 Information Systems Security – Practical 9

Cryptography

Checking Integrity

1.

```
PS C:\java-workspace\Files-20210107> Get-FileHash C:\java-workspace\Files-20210107\Text1.txt -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             398F19F9B33CA038B7A5CCFCFB258DD0                                       C:\java-workspace\Files-20210...


PS C:\java-workspace\Files-20210107> Get-FileHash C:\java-workspace\Files-20210107\Text1.txt -Algorithm SHA1

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA1            B50054919C56A60975EA9427B9221F3092D29683                               C:\java-workspace\Files-20210...


PS C:\java-workspace\Files-20210107>
```

2.

```
PS C:\java-workspace\Files-20210107> Get-ChildItem | Get-FileHash -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             9CDC00C301F4DC635A8555EBF782E45B                                       C:\java-workspace\Files-20210...
MD5             6AC0F17DB3972E027DEE6969B02E80FC                                       C:\java-workspace\Files-20210...
MD5             398F19F9B33CA038B7A5CCFCFB258DD0                                       C:\java-workspace\Files-20210...
MD5             0068D1B6FB20610F9634C6E1E4F88283                                       C:\java-workspace\Files-20210...


PS C:\java-workspace\Files-20210107>
```

3.

Added some text to Text1.txt and checked integrity and it has been changed.

```
PS C:\java-workspace\Files-20210107> Get-ChildItem | Get-FileHash -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             9CDC00C301F4DC635A8555EBF782E45B                                       C:\java-workspace\Files-20210...
MD5             6AC0F17DB3972E027DEE6969B02E80FC                                       C:\java-workspace\Files-20210...
MD5             048A1FD6135901878FC84AD833324220                                       C:\java-workspace\Files-20210...
MD5             0068D1B6FB20610F9634C6E1E4F88283                                       C:\java-workspace\Files-20210...


PS C:\java-workspace\Files-20210107>
```

Collisions in MD5 and SHA-1

1.

```
PS C:\java-workspace\Files-20210107> Get-FileHash C:\java-workspace\Files-20210107\flowers.jpg -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             9CDC00C301F4DC635A8555EBF782E45B                                       C:\java-workspace\Files-20210...


PS C:\java-workspace\Files-20210107> Get-FileHash C:\java-workspace\Files-20210107\rabbit.jpg -Algorithm MD5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             6AC0F17DB3972E027DEE6969B02E80FC                                       C:\java-workspace\Files-20210...


PS C:\java-workspace\Files-20210107>
```

2.

The hash value is available so that we can check it after downloading. After downloading when we check the hash value of that, and if it is different from the provided hash value, that means that some content is missing in the downloaded file or that someone has changed the file intentionally.

3.

Shattered-1.pdf and shattered-2.pdf both give the same SHA-1 value.

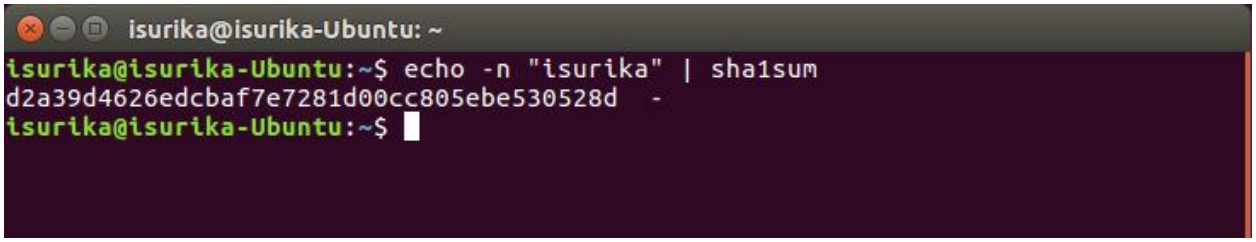
```
PS C:\java-workspace\Files-20210107> Get-FileHash C:\java-workspace\shattered-1.pdf -Algorithm SHA1

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA1            38762CF7F55934B34D179AE6A4C80CADCCBB7F0A                               C:\java-workspace\shattered-1...


PS C:\java-workspace\Files-20210107> Get-FileHash C:\java-workspace\shattered-2.pdf -Algorithm SHA1

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA1            38762CF7F55934B34D179AE6A4C80CADCCBB7F0A                               C:\java-workspace\shattered-2...
```

Reverse Hashing

1. The old password can be already known by someone. If we use the same old password, they can also log in as that user. To avoid that, setting a new password is better.

2. 5d41402abc4b2a76b9719d911017c592

3.



The hash value for the name could not be reversed.

4.

These websites generate hashes for a very large number of strings and store them in a table called rainbow table. When we search for the reversed hash, the data stored in those tables are searched and the relevant string is displayed.

5.

Use strong passwords which has uppercase and lowercase letters, numbers, and symbols.

Long passwords which are uncommon.

Use passwords that are suggested by google.