



Parshvanath Charitable Trust's
A. P. SHAH INSTITUTE OF TECHNOLOGY
(Approved by AICTE New Delhi & Govt. of Maharashtra, Affiliated to University of Mumbai)
(Religious Jain Minority)

Department of Information Technology

Semester: V

Academic Year: 2022-23

Class / Branch: TE IT

Subject: Security Lab (SL)

Name of Instructor: Prof. Apeksha Mohite

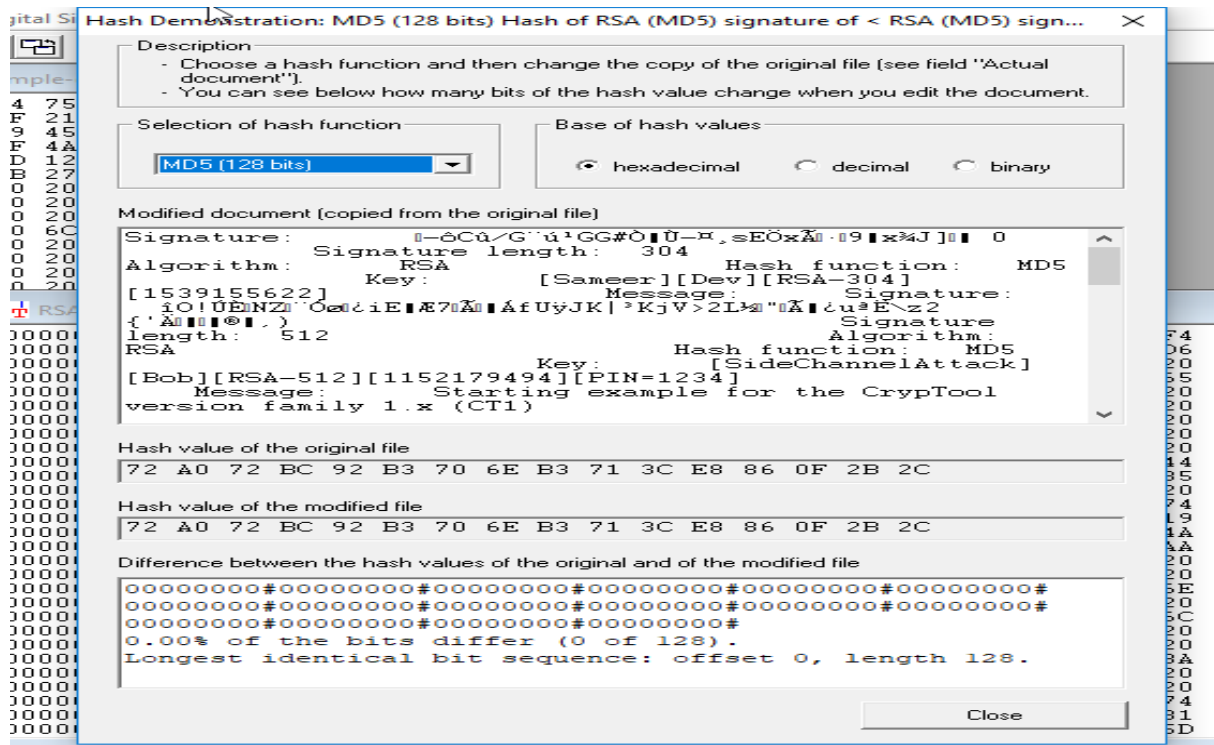
Name of Student: Shreyash Ghute

Student ID: 20104051

EXPERIMENT NO. 10

Aim: To study and test message integrity by using MD-5, SHA-1 for varying message sizes

1) Original File in MD5 hash





2) % change in differing bits of MD5

Hash Demonstration: MD5 (128 bits) Hash of RSA (MD5) signature of < RSA (MD5) sign... X

Description

- Choose a hash function and then change the copy of the original file (see field "Actual document").
- You can see below how many bits of the hash value change when you edit the document.

Selection of hash function

MD5 (128 bits)

Base of hash values

☒ hexadecimal ☐ decimal ☐ binary

Modified document (copied from the original file)

sameer

Hash value of the original file

72 A0 72 BC 92 B3 70 6E B3 71 3C E8 86 0F 2B 2C

Hash value of the modified file

D5 24 81 35 36 B7 16 39 99 9B A1 2B DB 36 21 A8

Difference between the hash values of the original and of the modified file

10100111#10000100#11110011#10001001#10100100#00000100#
01100110#01010111#00101010#11101010#10011101#11000011#
01011101#00111001#00001010#10000100#
46.09% of the bits differ (59 of 128).
Longest identical bit sequence: offset 38, length 7.

Close



3) Original File in SHA-1 hash

Hash Demonstration: SHA-1 (160 bits) Hash of RSA (MD5) signature of < RSA (MD5) sig... X

Description

- Choose a hash function and then change the copy of the original file [see field "Actual document"].
- You can see below how many bits of the hash value change when you edit the document.

Selection of hash function

SHA-1 (160 bits)

Base of hash values

☒ hexadecimal
 ☐ decimal
 ☐ binary

Modified document (copied from the original file)

```
Signature:    [-ôCû/G'ú¹GG#Ô||Û-¤,sEÖxÃ·09|x%J]|| 0
Signature length: 304
Algorithm:    RSA                                Hash function: MD5
Key:          [Sameer][Dev][RSA-304]
[1539155622] Message:                            Signature:
io|ÜB|NZI`ÖæöiiE|Æ7|Ã||ÁfUÿJK|³KjV>2L¾|"iÃ||ü³E\z2
{'Ã||@||,)                                         Signature
length: 512                                       Algorithm:
RSA                                                Hash function: MD5
                                                    Key:          [SideChannelAttack]
[Bob][RSA-512][1152179494][PIN=1234]
Message: Starting example for the Cryptool
version family 1.x (CT1)
```

Hash value of the original file

9E	7B	0A	54	F6	90	59	B5	10	CE	F8	42	26	A3	8C	57	C9	72	9B	1
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	---

Hash value of the modified file

9E	7B	0A	54	F6	90	59	B5	10	CE	F8	42	26	A3	8C	57	C9	72	9B	1
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	---

Difference between the hash values of the original and of the modified file

```
00000000#00000000#00000000#00000000#00000000#00000000#
00000000#00000000#00000000#00000000#00000000#00000000#
00000000#00000000#00000000#00000000#00000000#00000000#
00000000#00000000#
0.00% of the bits differ (0 of 160).
Longest identical bit sequence: offset 0, length 160.
```

Close



4) % change in differing bits of SHA-1

Hash Demonstration: SHA-1 (160 bits) Hash of RSA (MD5) signature of < RSA (MD5) sig... X

Description

- Choose a hash function and then change the copy of the original file (see field "Actual document").
- You can see below how many bits of the hash value change when you edit the document.

Selection of hash function

SHA-1 (160 bits)

Base of hash values

☒ hexadecimal ☐ decimal ☐ binary

Modified document (copied from the original file)

sameer

Hash value of the original file

9E 7B 0A 54 F6 90 59 B5 10 CE F8 42 26 A3 8C 57 C9 72 9B 1

Hash value of the modified file

DA 4A 4E FB 90 7A 17 FA BB 3E 09 28 41 51 1E 7F 24 E2 26 C

Difference between the hash values of the original and of the modified file

```
01000100#00110001#01000100#10101111#01100110#11101010#
01001110#01001111#10101011#11110000#11110001#01101010#
01100111#11110010#10010010#00101000#11101101#10010000#
10111101#11011010#
51.88% of the bits differ (83 of 160).
Longest identical bit sequence: offset 6, length 4.
```

Close



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)



md5sum :

```
apsit@apsit-HP-280-G3-MT: ~/Documents
File Edit View Search Terminal Help
apsit@apsit-HP-280-G3-MT:~/Documents$ echo Im from IT department>shreyash.txt
apsit@apsit-HP-280-G3-MT:~/Documents$ cat shreyash.txt
Im from IT department
apsit@apsit-HP-280-G3-MT:~/Documents$ md5sum shreyash.txt
fab8935e6ca611ca6380a97b06e82c8d shreyash.txt
apsit@apsit-HP-280-G3-MT:~/Documents$ echo Happy Navratri>shreyash.txt
apsit@apsit-HP-280-G3-MT:~/Documents$ md5sum shreyash.txt
e6b0096de04d0de0925c6fe89513cc22 shreyash.txt
apsit@apsit-HP-280-G3-MT:~/Documents$
```

sha1sum:

```
apsit@apsit-HP-280-G3-MT:~/Documents$ sha1sum shreyash.txt
3f550ac564be14d4e7e9944286d874dba11f0d3a shreyash.txt
apsit@apsit-HP-280-G3-MT:~/Documents$ echo Happy Diwali>shreyash.txt
apsit@apsit-HP-280-G3-MT:~/Documents$ sha1sum shreyash.txt
\e91e05c0e6ce5b091c670bd027c32afbed4e5a4b shreyash.txt
apsit@apsit-HP-280-G3-MT:~/Documents$
```

Department of Information Technology |

APSIT



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)



sha256sum/sha224sum/sha512sum/sha384sum :

```
apsit@apsit-HP-280-G3-MT:~/Documents$ sha256sum shreyash.txt
c88484ff13c8e00ac930514f9958c087e9ad0691294077e485cb6ccecd6b6fda shreyash.txt
apsit@apsit-HP-280-G3-MT:~/Documents$ sha224sum shreyash.txt
0cbe93f5aba252a3e7d4c978ea23a0617b2a49bd68f18e194221deb0 shreyash.txt
apsit@apsit-HP-280-G3-MT:~/Documents$ sha512sum shreyash.txt
faf960c2931db31c3b4fa858002c79d622bb5fa8c7caaac79693ebd09ac8de27ca7755c29b6dfadb313ef413758f8cbbc99e085e17df364a33826f0965f73f6 shreyash.txt
apsit@apsit-HP-280-G3-MT:~/Documents$ sha384sum shreyash.txt
a606259278f7f1bc4b8a145db86f14892c25d9a7db85f895e417a9d22b72d48c7a478ac392d1aaa3d101dc2be49d8cf0 shreyash.txt
apsit@apsit-HP-280-G3-MT:~/Documents$
```

checking integrity of downloaded iso :

```
apsit@apsit-HP-280-G3-MT: ~/Videos
File Edit View Search Terminal Help
apsit@apsit-HP-280-G3-MT:~/Documents$ cd
apsit@apsit-HP-280-G3-MT:~$ cd Videos
apsit@apsit-HP-280-G3-MT:~/Videos$ ls
ubuntu-14.04.6-desktop-amd64.iso
apsit@apsit-HP-280-G3-MT:~/Videos$ md5sum ubuntu-14.04.6-desktop-amd64.iso
401e9a5528bdae53b85f63996ae83773  ubuntu-14.04.6-desktop-amd64.iso
apsit@apsit-HP-280-G3-MT:~/Videos$
```



```
releases.ubuntu.com/14.04
+
Not secure | releases.ubuntu.com/14.04/MD5SUMS
401e9a5528bdae53b85f63996ae83773 *ubuntu-14.04.6-desktop-amd64.iso
c16ec8b927849cbbba7b900d25eb49bfd *ubuntu-14.04.6-desktop-i386.iso
e750536067b6fff7f9934a13466fe2db *ubuntu-14.04.6-server-amd64.iso
8634a4626a056907e227b7be636f05f8 *ubuntu-14.04.6-server-i386.iso
b31731ea6cdbebe1d02f8193db420886 *wubi.exe
```

Department of Information Technology |

APSIT



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)



Department of Information Technology |

AP**S****IT**



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)



Department of Information Technology |

AP**S****IT**