



PARSHVANATH CHARITABLE TRUST'S

**A. P. SHAH INSTITUTE OF TECHNOLOGY**

(All Branches NBA Accredited)



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: Vishal Bangar

Student ID: 20104084

### 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**

Department of Information Technology |



The screenshot shows the "Hash Demonstration" window with the title bar "MD5 (128 bits) Hash of RSA (MD5) signature of < RSA (MD5) sign...". The interface includes:

- Description:** A box explaining that users choose a hash function and change the copy of the original file to see how the hash value changes.
- Selection of hash function:** A dropdown menu set to "MD5 (128 bits)".
- Base of hash values:** Radio buttons for hexadecimal (selected), decimal, and binary.
- Modified document (copied from the original file):** A text area containing a modified RSA message. The modification includes a "SideChannelAttack" key and a "PIN=1234" message, along with a version family update from 1.x to CT1.
- Hash value of the original file:** A text field displaying the hex string: 72 A0 72 BC 92 B3 70 6E B3 71 3C E8 86 0F 2B 2C.
- Hash value of the modified file:** A text field displaying the same hex string: 72 A0 72 BC 92 B3 70 6E B3 71 3C E8 86 0F 2B 2C.
- Difference between the hash values:** A text area showing that all 128 bits are identical, resulting in a longest identical bit sequence of offset 0 and length 128.
- Buttons:** "Close" at the bottom right.



## 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: [Signature data]  
Signature length: 304  
Algorithm: RSA Hash function: MD5  
Key: [Sameer][Dev][RSA-304]  
[1539155622] Message: Signature:  
iO!UE[NZ]`OaZiE[A7]A[AfUyJK|`KjV>2L[A]ZuE\z2  
{'A[[]@[,.) 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-Notebook: ~/Music
apsit@apsit-HP-Notebook:~$ cd /home/apsit/Music
apsit@apsit-HP-Notebook:~/Music$ echo This is demo of md5sum>example.txt
apsit@apsit-HP-Notebook:~/Music$ md5sum example.txt
2bdb073a79fa278cb34a466d94ac784c  example.txt
apsit@apsit-HP-Notebook:~/Music$ echo This is to check message integrity >example.txt
apsit@apsit-HP-Notebook:~/Music$ cat example.txt
This is to check message integrity
apsit@apsit-HP-Notebook:~/Music$ md5sum example.txt
458209d843ab0d8c41358d26311737d0  example.txt
apsit@apsit-HP-Notebook:~/Music$
```

**sha1sum:**

**sha256sum/sha224sum/sha512sum/sha384sum**

:

```
apsit@apsit-HP-Notebook: ~/Music
apsit@apsit-HP-Notebook:~/Music$ sha256sum example.txt
ecc28c251bf3522e66157bdc5c43617d37a3c05e58ac48204d67c660b38666c0  example.txt
apsit@apsit-HP-Notebook:~/Music$ sha224sum example.txt
da33a14765ebc7c7288234e617b91d2af7c508f17b12d744d6f9ed21  example.txt
apsit@apsit-HP-Notebook:~/Music$ sha512sum example.txt
4aeb20fd4e0cbdf8c4b0664e954a519256d3226eb84fbf245cd09507c0e125a006d7757ec241a47
9729a87531a54c4d1eb4d672ea9163047d639ba373295727  example.txt
apsit@apsit-HP-Notebook:~/Music$ sha384sum example.txt
7f6bda478d1f3dfd1cd4b0ba5ca5f85fcb5b94ffe24614ad20689afb2aae4ed3ca6044b4cc48c242
0b206d4458e7c517  example.txt
apsit@apsit-HP-Notebook:~/Music$
```

**Department of Information Technology |**

**AP****SIT**





PARSHVANATH CHARITABLE TRUST'S

**A. P. SHAH INSTITUTE OF TECHNOLOGY**

(All Branches NBA Accredited)



---

checking integrity of downloaded iso :

```
apsit@apsit-HP-Notebook: ~/Music
apsit@apsit-HP-Notebook:~/Music$ sha1sum example.txt
a1617450c7b5e21efa3b1b76724fa4569121e60d  example.txt
apsit@apsit-HP-Notebook:~/Music$ echo testing sha1 >example.txt
apsit@apsit-HP-Notebook:~/Music$ sha1sum example.txt
d9a786e86480cd108a912abea3069cf9e369d602  example.txt
apsit@apsit-HP-Notebook:~/Music$
```

Department of Information Technology |



PARSHVANATH CHARITABLE TRUST'S

# A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)



```
apsit@apsit-HP-Notebook: ~/Music
apsit@apsit-HP-Notebook:~/Music$ ls
example.txt  ubuntu-14.04.5-desktop-amd64.iso
apsit@apsit-HP-Notebook:~/Music$ md5sum ubuntu-14.04.5-desktop-amd64.iso
0abc200fd4b84a1e8881287d70dfb822  ubuntu-14.04.5-desktop-amd64.iso
apsit@apsit-HP-Notebook:~/Music$
```

  

releases.ubuntu.com/trusty/MD5SUMS

```
0abc200fd4b84a1e8881287d70dfb822 *ubuntu-14.04.5-desktop-amd64.iso
22616fb5b597deb059d18606e7ad78bb *ubuntu-14.04.5-desktop-i386.iso
dd54dc8cfc2a655053d19813c2f9aa9f *ubuntu-14.04.5-server-amd64.iso
812ac191b8898b33aed4aef9ab066b5a *ubuntu-14.04.5-server-i386.iso
b31731ea6cdbebe1d02f8193db429886 *wubi.exe
```

Department of Information Technology |