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

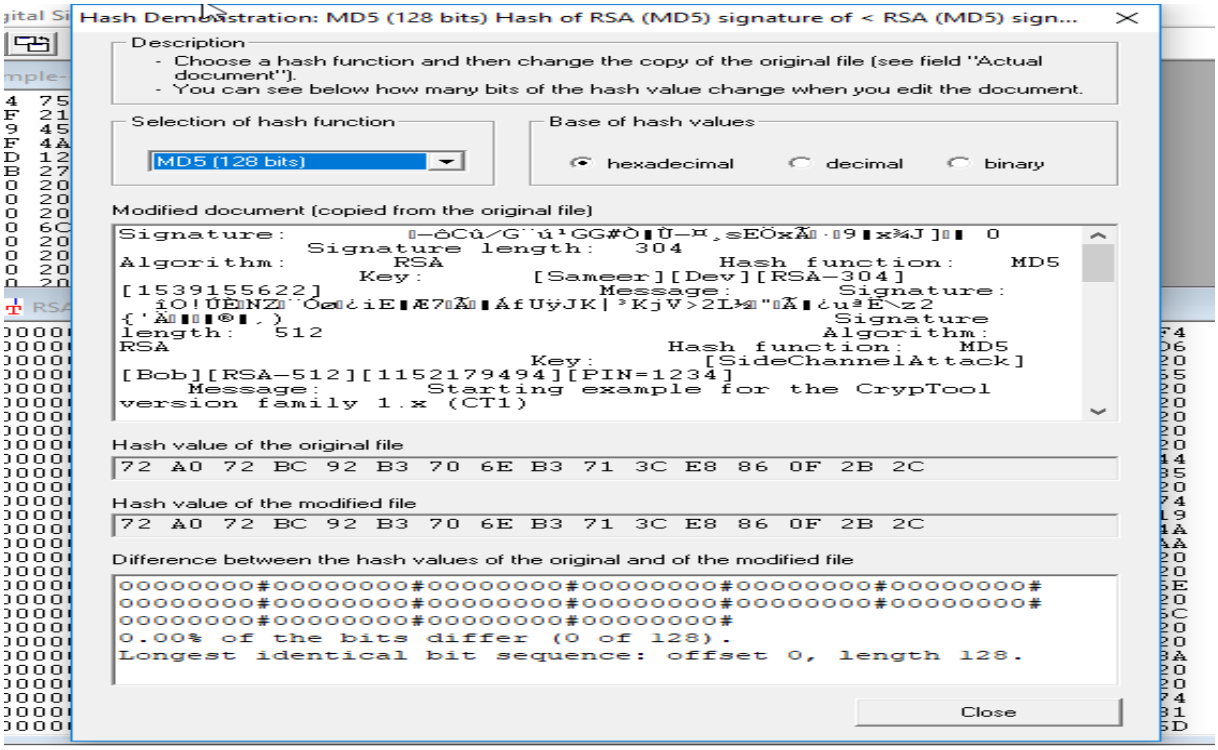
Semester: V
Academic Year: 2022-23
Class / Branch: TE IT
Subject: Security Lab (SL)
Name of Instructor: Prof. Apeksha Mohite

Name of Student:Shreyash Ghute
Student ID:20104051

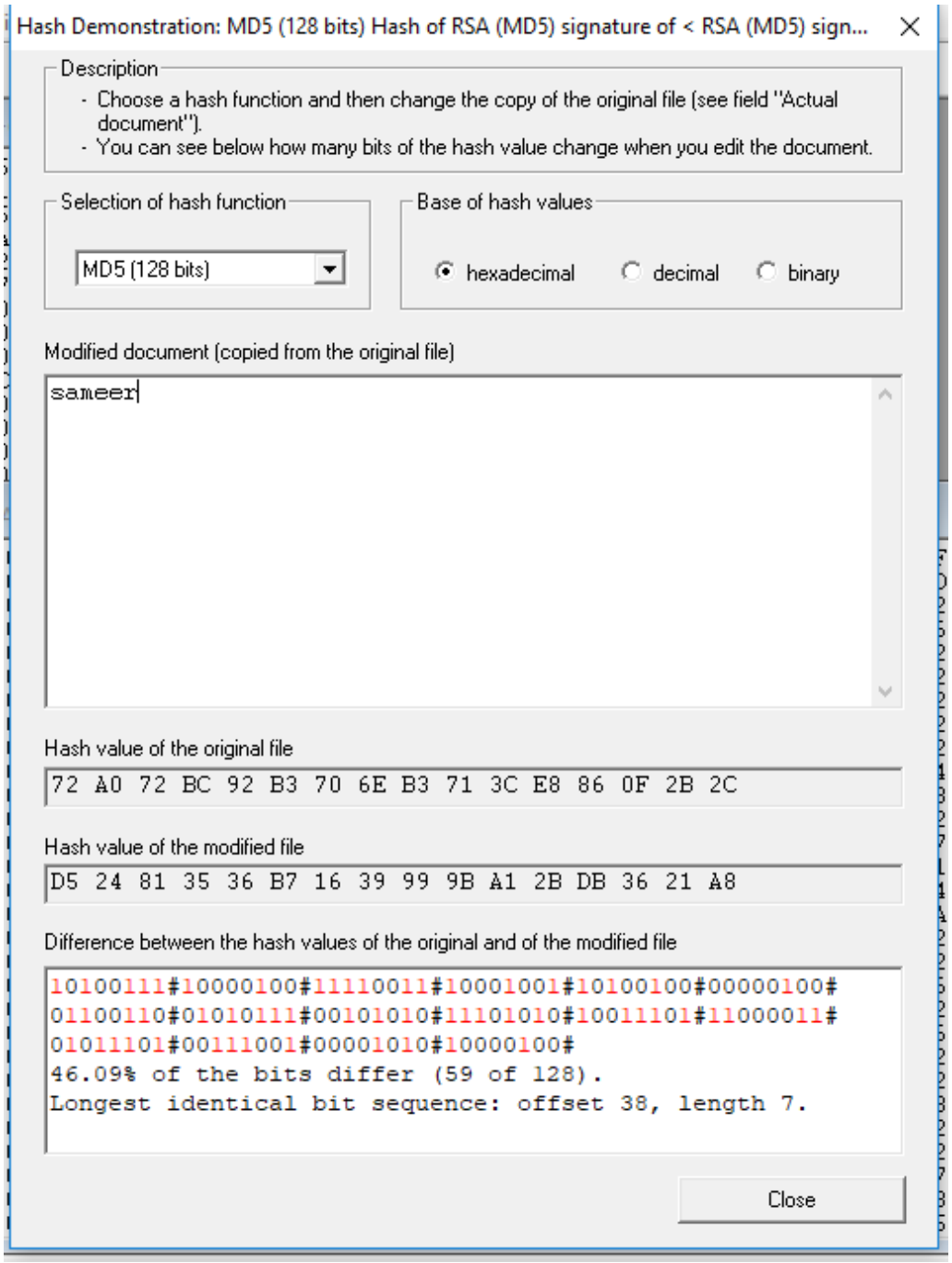
EXPERIMENT NO. 10

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

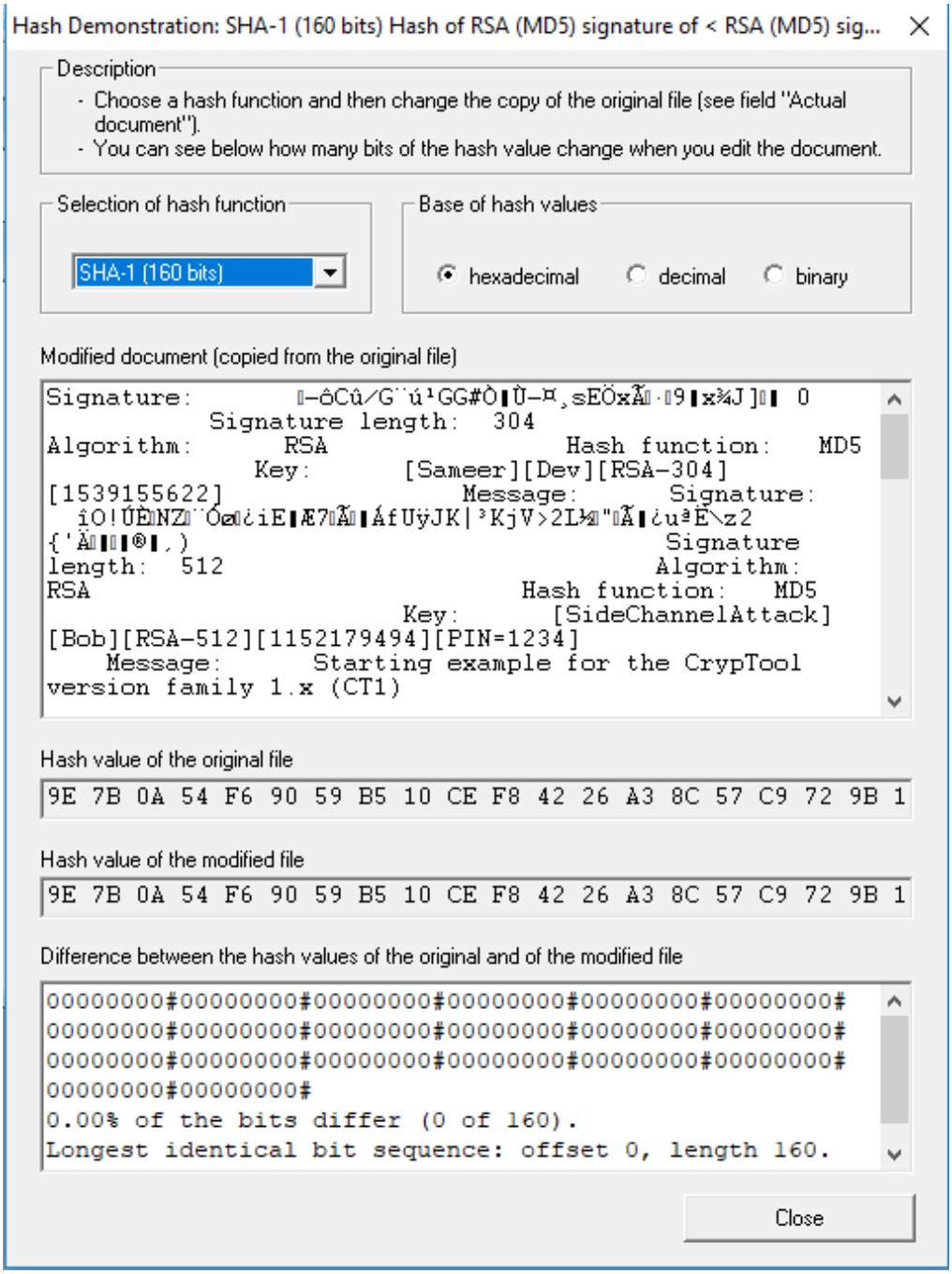
1) Original File in MD5 hash


Hash Demonstration: MD5 (128 bits) Hash of RSA (MD5) signature of < RSA (MD5) sign...
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)
Signature: Signature length: 304
Algorithm: RSA Hash function: MD5
Key: [Sameer][Dev][RSA-304]
[1539155622] Message: Signature:
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
72 A0 72 BC 92 B3 70 6E B3 71 3C E8 86 0F 2B 2C
Hash value of the modified file
72 A0 72 BC 92 B3 70 6E B3 71 3C E8 86 0F 2B 2C
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#
0.00% of the bits differ (0 of 128).
Longest identical bit sequence: offset 0, length 128.
Close

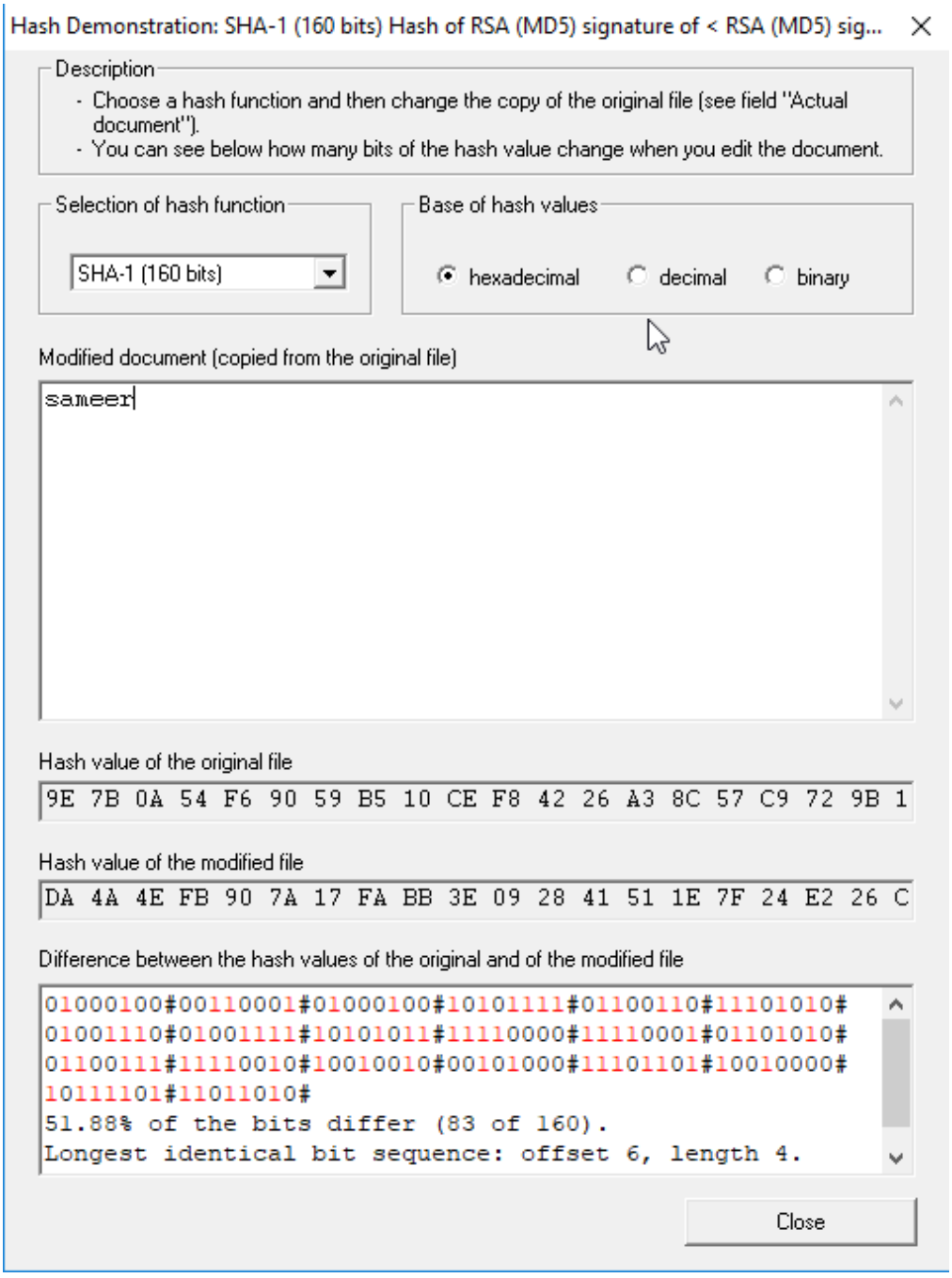
2) % change in differing bits of MD5



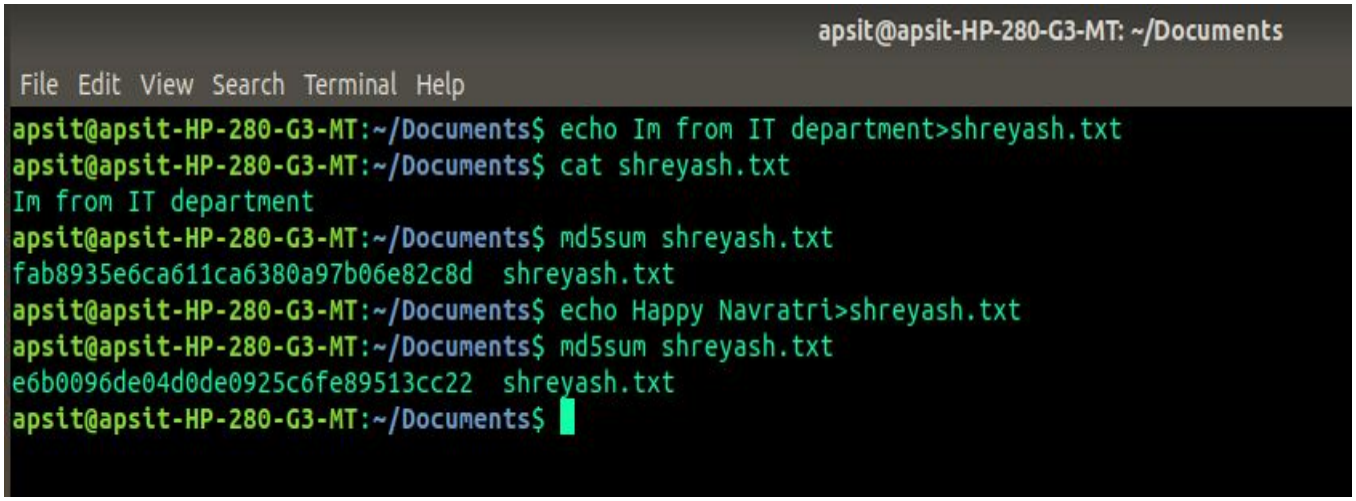
3) Original File in SHA-1 hash



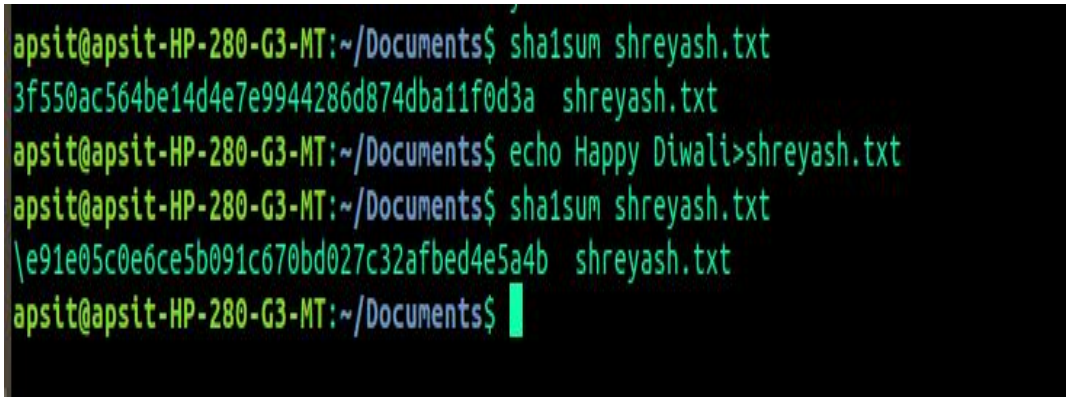
4) % change in differing bits of SHA-1



md5sum :



sha1sum:



sha256sum/sha224sum/sha512sum/sha384sum :

```
apsit@apsit-HP-280-G3-MT:~/Documents$ sha256sum shreyash.txt
c88484ff13c8e00ac930514f9958c087e9ad0691294077e485cb6ccecdbb6fda  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
faf960c2931db31c3b4fa858002c79d622bb5fa8c7caaaac79693ebd09ac8de27ca7755c29b6dfadb313ef413758f8cbbc99e085e17df364a33826f0965f73f6  shreyash.txt
apsit@apsit-HP-280-G3-MT:~/Documents$ sha384sum shreyash.txt
a686259278f7f1bc4b8a145db86f14892c25d9a7db85f895e417a9d22b72d48c7a478ac392d1aaa3d101dc2be49d8cf0  shreyash.txt
apsit@apsit-HP-280-G3-MT:~/Documents$
```

checking integrity of downloaded iso :

```
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.

Not secure | releases.ubuntu.com/14.04/MD5SUMS

```
401e9a5528bdae53b85f63996ae83773 *ubuntu-14.04.6-desktop-amd64.iso
c16ec8b927849cbba7b900d25eb49bfd *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
```