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

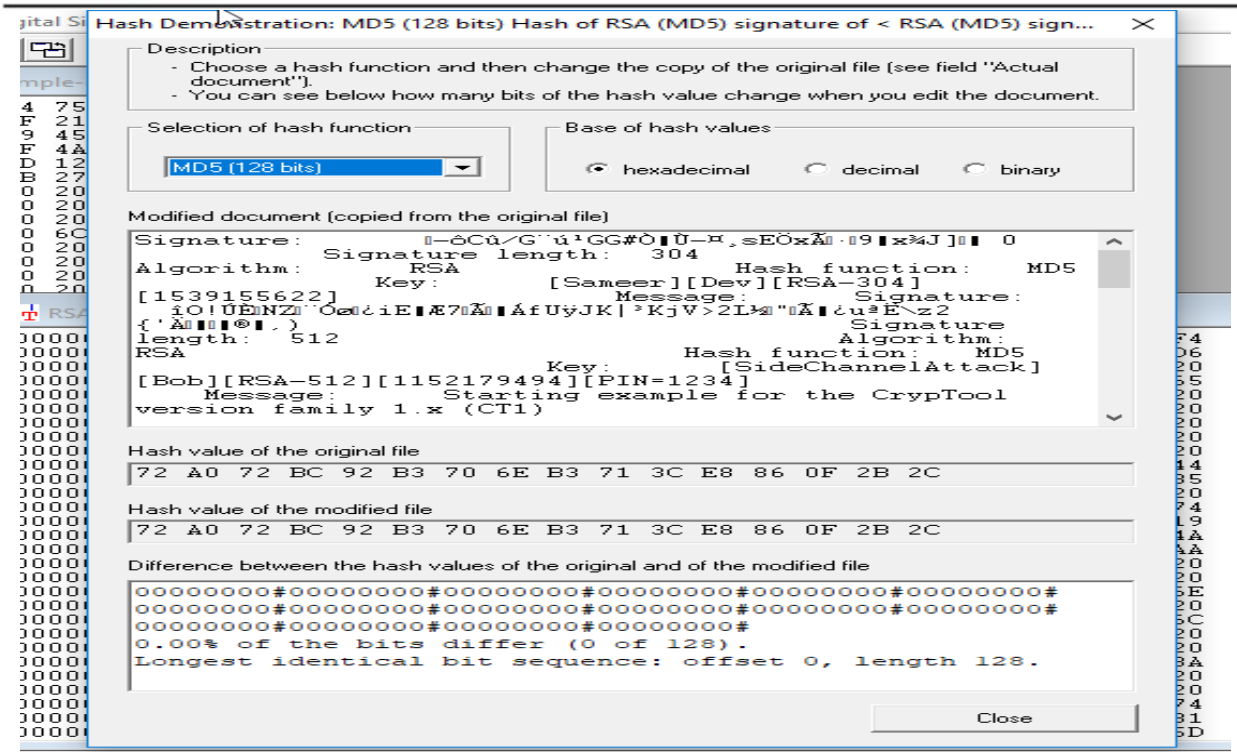
Semester: V
Academic Year: 2022-23
Class / Branch: TE IT
Subject: Security Lab (SL)
Name of Instructor: Prof. Apeksha Mohite

Name of Student: Vishal Bangar
Student ID: 20104084

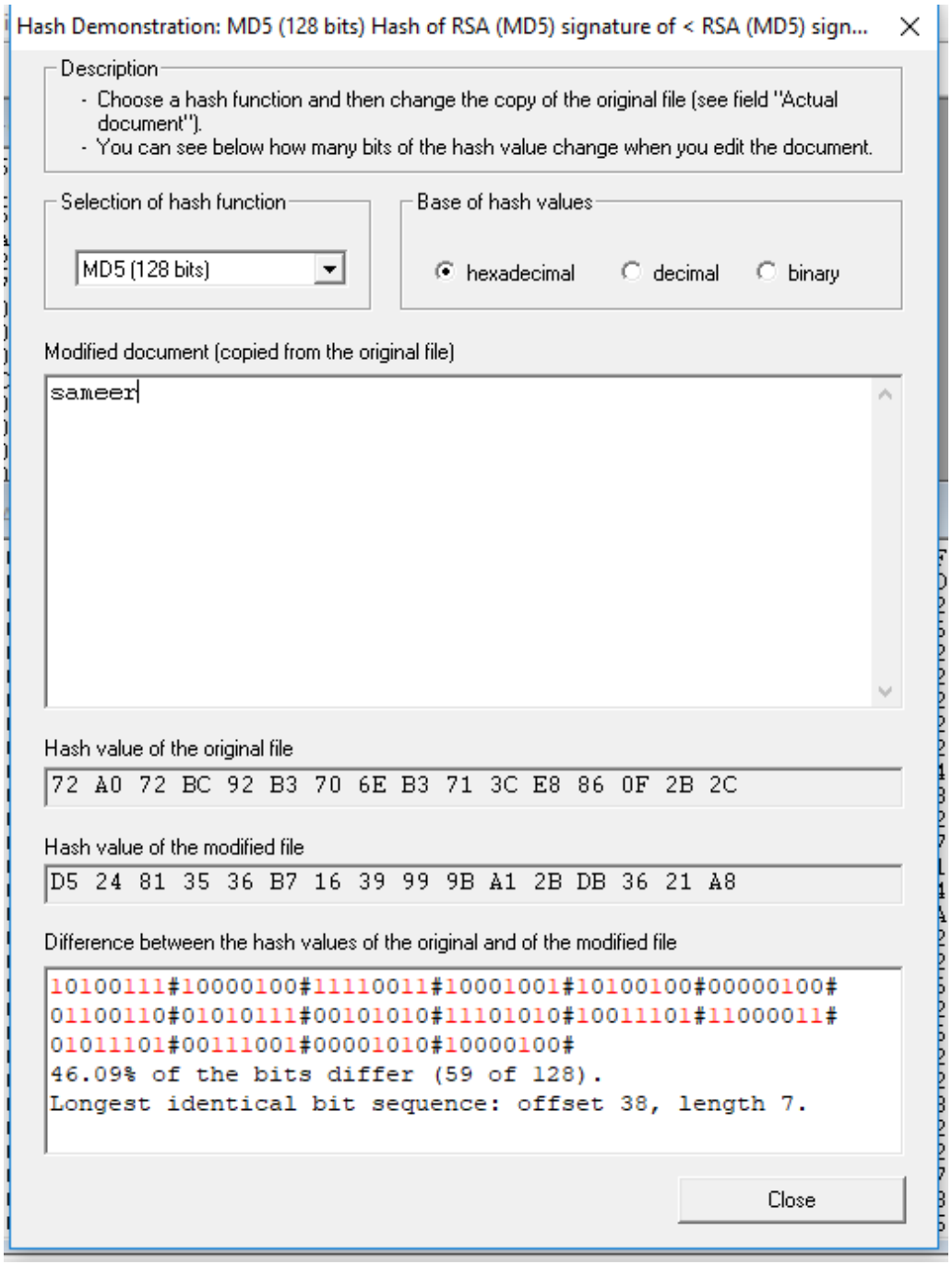
EXPERIMENT NO. 10

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

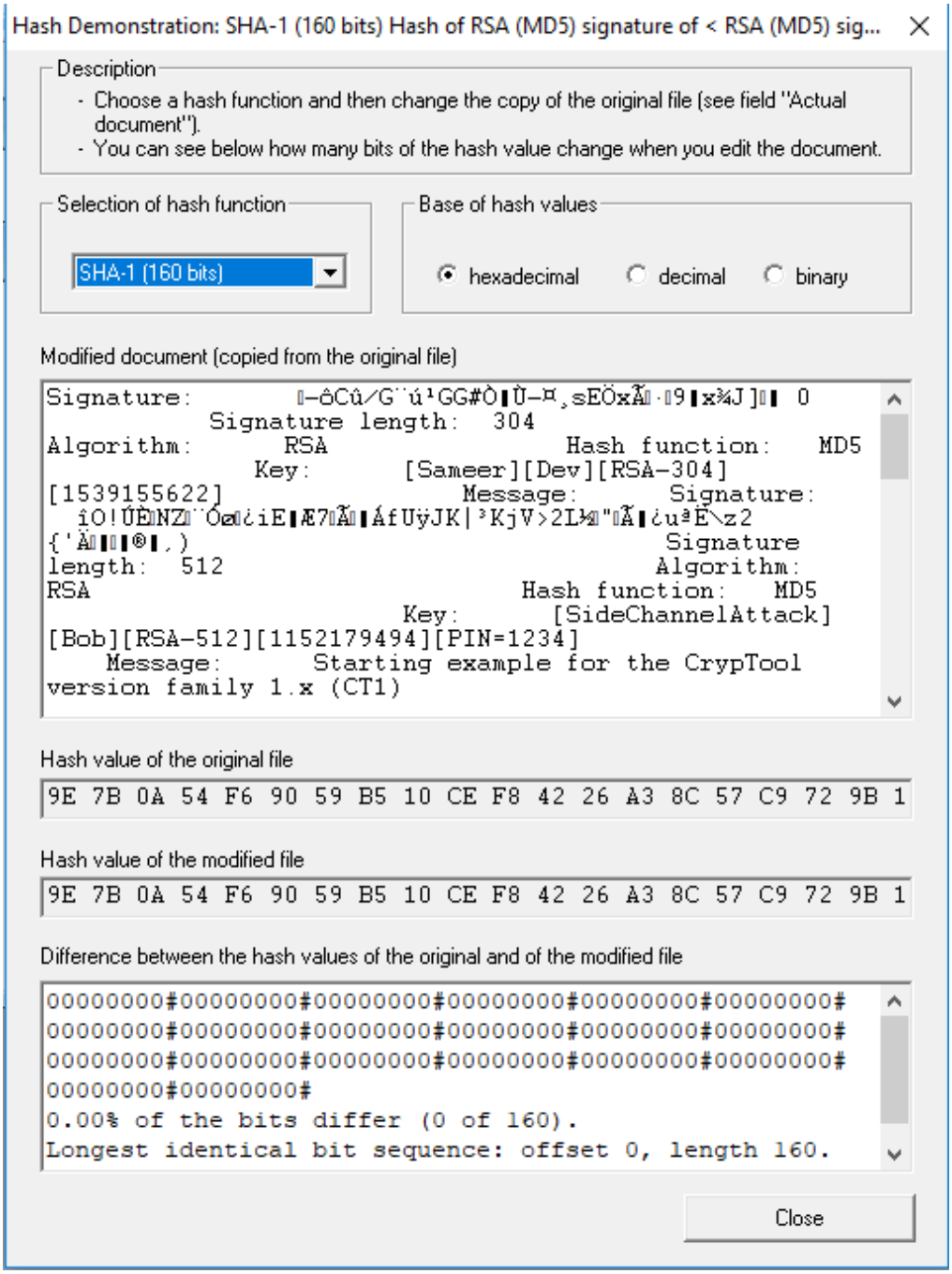
1) Original File in MD5 hash


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

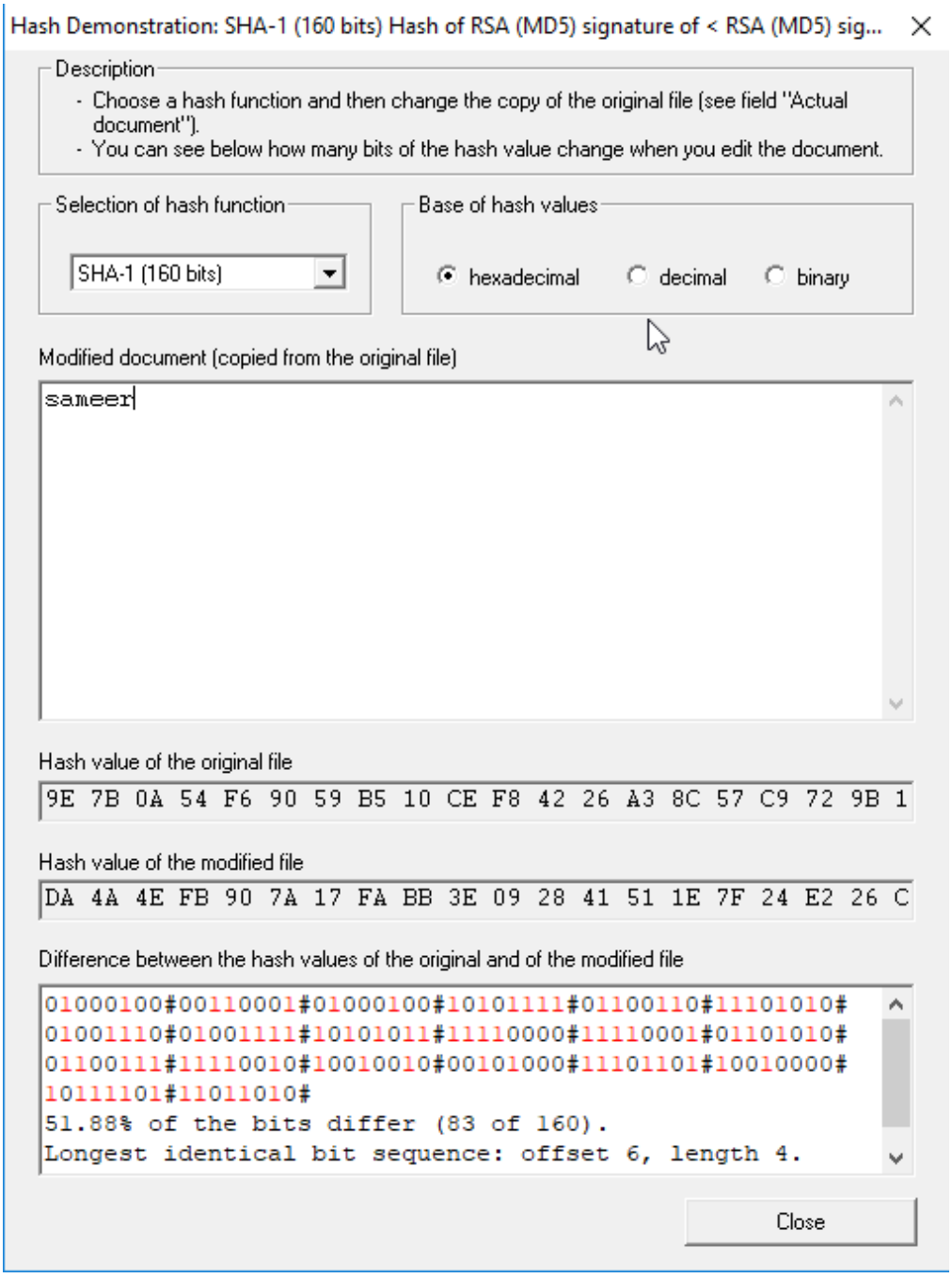
2) % change in differing bits of MD5



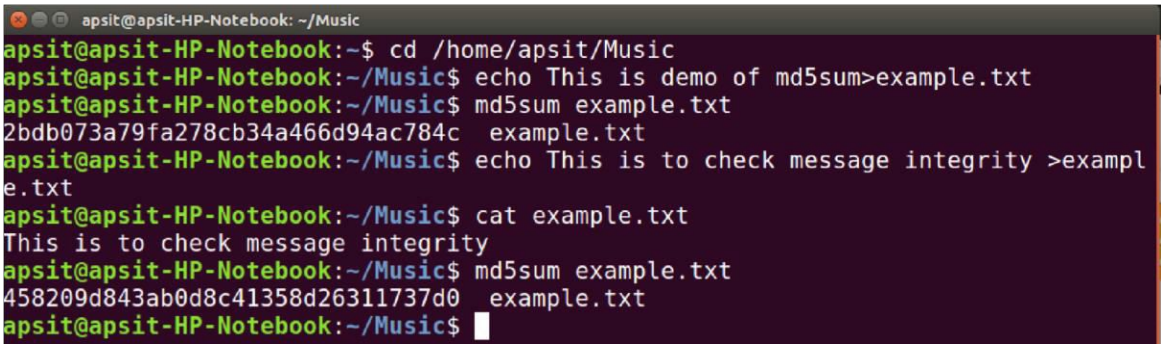
3) Original File in SHA-1 hash



4) % change in differing bits of SHA-1



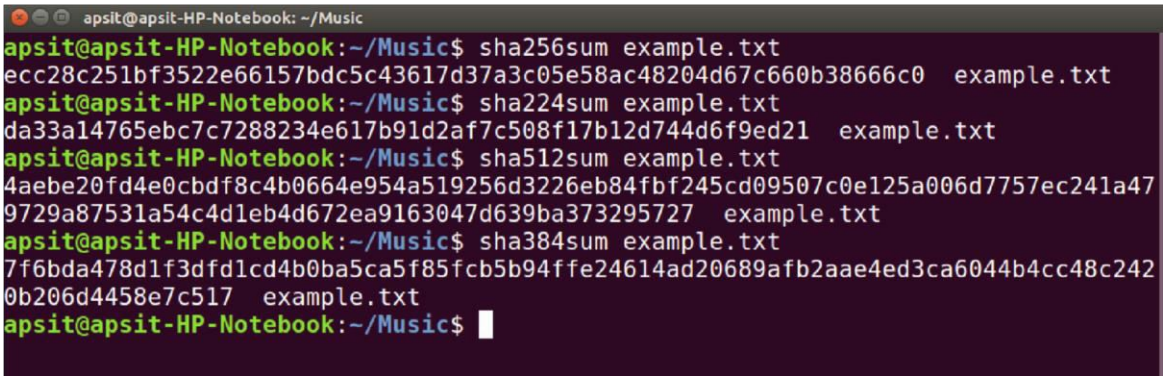
md5sum :



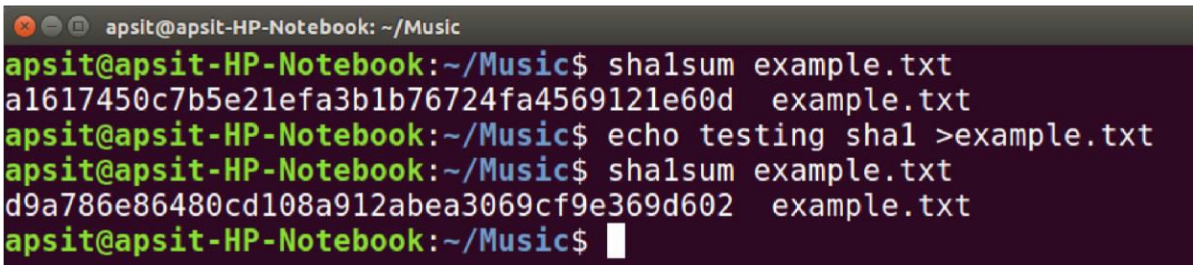
sha1sum:

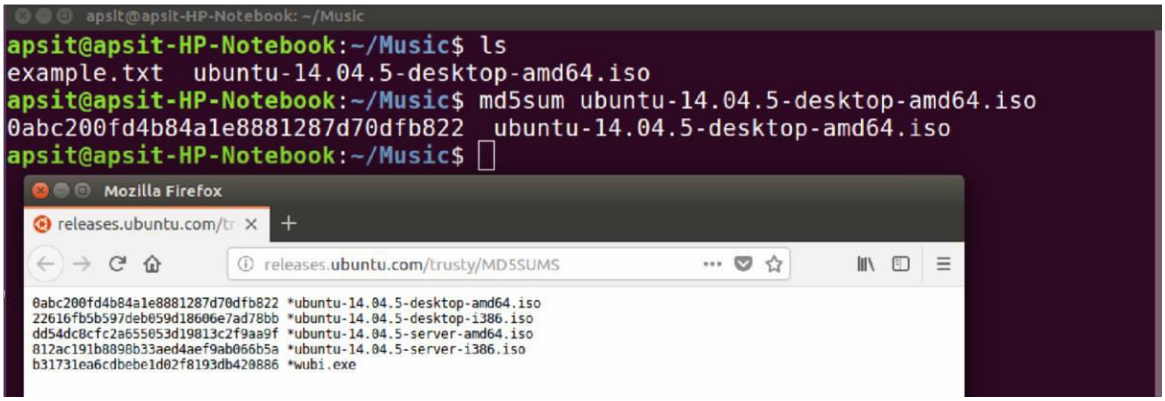
sha256sum/sha224sum/sha512sum/sha384sum

:



checking integrity of downloaded iso :




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$
Mozilla Firefox
releases.ubuntu.com/tr
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
b31731ea6cdbebe1d02f8193db420886 *wubi.exe