



PARSHVANATH CHARITABLE TRUST'S

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

Department of Information Technology

(NBA Accredited)



Academic Year: 2025-26

Semester: V

Class / Branch/ Div: TEIT-C

Subject: Security Lab

Name of Student: Suyash Y Mane

Student ID: 24204008

Roll No. 10

Date of Submission: 14/08/2025

## Experiment No: 12

**Aim:** To study and test message integrity by using MD5, SHA-1 for varying message sizes.

### Outputs:

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ cd /home/apsit/Downloads
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads$ mkdir Suyash
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads$ cd Suyash
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ pwd
/home/apsit/Downloads/Suyash
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ echo This is VB sirs best batch>example.txt
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ cat example.txt
This is VB sirs best batch
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ md5sum example.txt
95db13aef1d4de03645d15dded0db8e4 example.txt
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ sudo nano example.txt
[sudo] password for apsit:
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ md5sum example.txt
ae53206f07c52fa24c29c783472df5c2 example.txt
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ sha1sum example.txt
8d058d70dc0a4da8268ef71264646111a99558d1 example.txt
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ sha256sum example.txt
f35aa2e761ba25a9435ebd2f994751e4e4ba34b60ed1679df174ab5771f71363 example.txt
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ sha512sum example.txt
fd718a07742ec8dace75fa1f49b34acefd351139ba75ac312b93c8967c77f6a8f89ad297b2373bdf96758d9621401285ba6708a268550a6fc50ff8f125c40 example.txt
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ ls
example.txt  ubuntu-14.04.6-desktop-amd64.iso
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ md5sum ubuntu-14.04.6-desktop-amd64.iso
401e9a5528bdae53b85f63996ae83773 ubuntu-14.04.6-desktop-amd64.iso
```

```
← → ↻ 📄 releases.ubuntu.com/14.04.6/MD5SUMS
401e9a5528bdae53b85f63996ae83773 *ubuntu-14.04.6-desktop-amd64.iso
c16ecbb927849cbba7b908d25eb49bfd *ubuntu-14.04.6-desktop-1386.iso
e75053606786ffff79934a13466f62db *ubuntu-14.04.6-server-amd64.iso
8634e4626a095607e2277b6e636f65f8 *ubuntu-14.04.6-server-1386.iso
b31731ea6cdebe1d02f8193db420886 *wubi.exe
```



PARSHVANATH CHARITABLE TRUST'S

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

**Department of Information Technology**

**(NBA Accredited)**



```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ sha1sum ubuntu-14.04.6-desktop-amd64.iso
2d3675f14a6884bb42917838a5c4246916fe73b5  ubuntu-14.04.6-desktop-amd64.iso
```

```
< → releases.ubuntu.com/14.04.6/SHA1SUMS
2d3675f14a6884bb42917838a5c4246916fe73b5 *ubuntu-14.04.6-desktop-amd64.iso
91a72f4b623b3bc38a3698eed30e6241b42c8cfd *ubuntu-14.04.6-desktop-i386.iso
13bfe163ca8ad8a6e5676b0460ce6d03387ec24 *ubuntu-14.04.6-server-amd64.iso
17297306e47b63f5393826e4726b5604280aba3 *ubuntu-14.04.6-server-i386.iso
bfc1ff3446b8cb49b6481372a2edf1c3861ba727 *wubi.exe
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~/Downloads/Suyash$ sha256sum ubuntu-14.04.6-desktop-amd64.iso
bcc02554c37d438545658be7964e1bc05bdb11289ae16bfbf94626b80d42656f  ubuntu-14.04.6-desktop-amd64.iso
```

```
< → releases.ubuntu.com/14.04.6/SHA256SUMS
bcc02554c37d438545658be7964e1bc05bdb11289ae16bfbf94626b80d42656f *ubuntu-14.04.6-desktop-amd64.iso
0a704ba33285558a76a88ef79dcf7fbaf1455c4889ab69939875ccc21bf3696d *ubuntu-14.04.6-desktop-i386.iso
b17d7c1e9d0321ad5810ba77b69aef43f0f29a5422b08120e6ee0576c4527c0e *ubuntu-14.04.6-server-amd64.iso
c3b0e016e77e6bfc608ab3e3d2aa33367fc83e3bf645014ecf36689fe330b80 *ubuntu-14.04.6-server-i386.iso
bc3b20ad00f19d0169206af0df5a4186c61ed08812262c55dbca3b7b1fc4a0b *wubi.exe
```

## Conclusion:

In this experiment, we learnt and understood to study and test message integrity by using MD5, SHA-1 for varying message sizes.