

# Applications of One-Way Hash Functions

- Integrity Verification — Detecting when data has been altered
- Commitments — Committing a secret without telling it
- Password Verification — Verifying a password without storing the plaintext

# Integrity Verification

Changing one bit of the original data changes the hash value

```
$ echo -n "Hello World" | sha256sum
a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e -

$ echo -n "Hallo World" | sha256sum
d87774ec4a1052afb269355d6151cbd39946d3fe16716ff5bec4a7a631c6a7a8 -
```

Examples:

- Detect changes in system files
- Detect if file downloaded from website is corrupted (e.g., SEED VM!)

```
$ md5sum SEEDUbuntu-16.04-32bit-15-31-57-662.zip
12c48542c29c233580a23589b72b71b8 SEEDUbuntu-16.04-32bit-15-31-57-662.zip
```

SEED Ubuntu16.04 VM (32-bit): This VM was built in June 2019

- Download the image from one of the following servers:
  - Google Drive: [SEEDUbuntu-16.04-32bit.zip](#)
  - DigitalOcean: [SEEDUbuntu-16.04-32bit.zip](#)
  - Cybersecurity.com: [SEEDUbuntu-16.04-32bit.zip](#)
  - Syracuse University (New York, US): [SEEDUbuntu-16.04-32bit.zip](#)
  - Zhejiang University (Zhejiang, China): [SEEDUbuntu-16.04-32bit.zip](#)
  - MD5 value: 12c48542c29c233580a23589b72b71b8