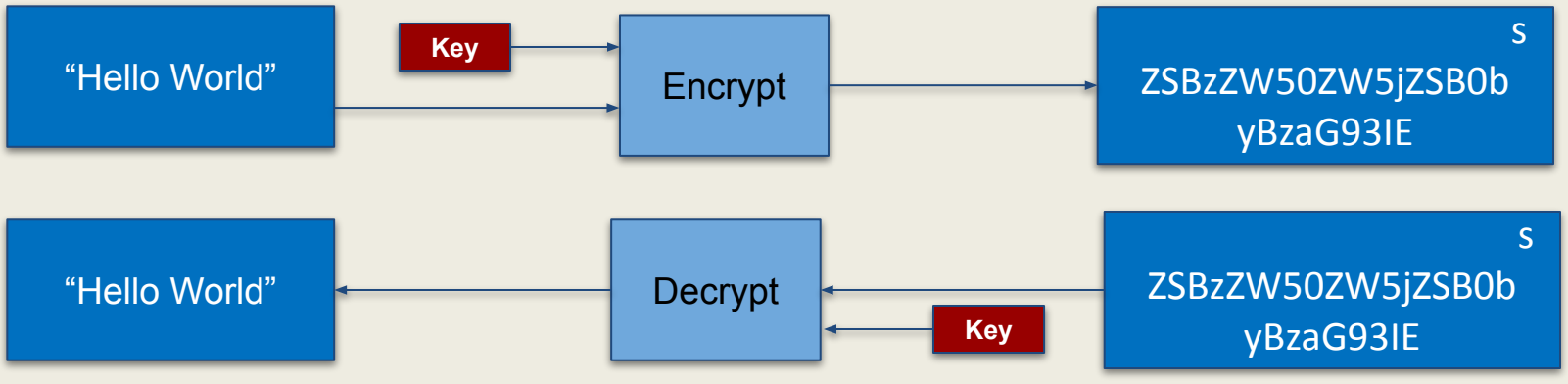
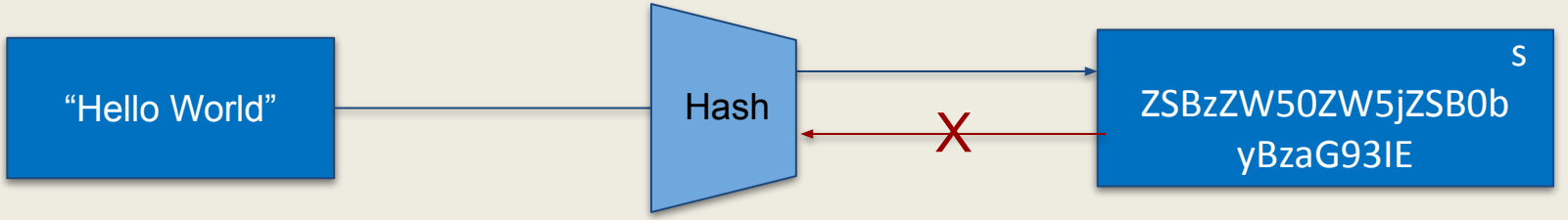
AUBURN

Cryptographic Hashing & File Validation

Hashing vs. Encryption

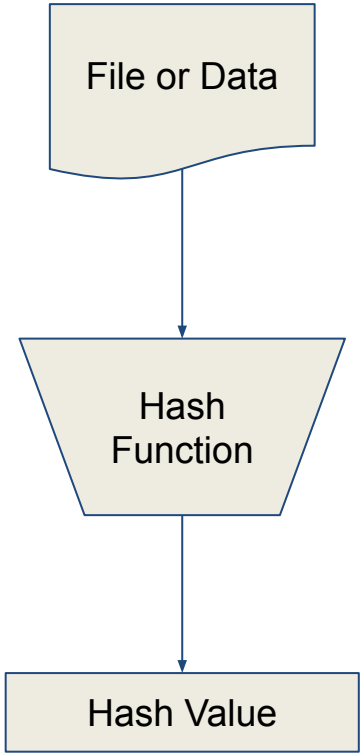


Encryption is two way, and requires a key to encrypt/decrypt



Hashing is one-way.

Cryptographic Hash Function



“Hello World”

648a6a6ffffdaa0badb23b8baf90b6168dd16b3a

Hash Function Features

AUBURN

- Fixed Length Output (Hash Value)
- Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as hashing the data.
- Hash value is much smaller than the input data
  - Hash functions can be called compression functions
  - Hash value is a smaller representation of a larger data and sometimes referred to as a **digest**
- Hash Function Naming
  - N bit output is referred to as an N-bit hash function
  - Represented in Hexadecimal to be readable
  - Common hash functions generate values between 160 and 512 bits

Hash Function Key Properties

AUBURN

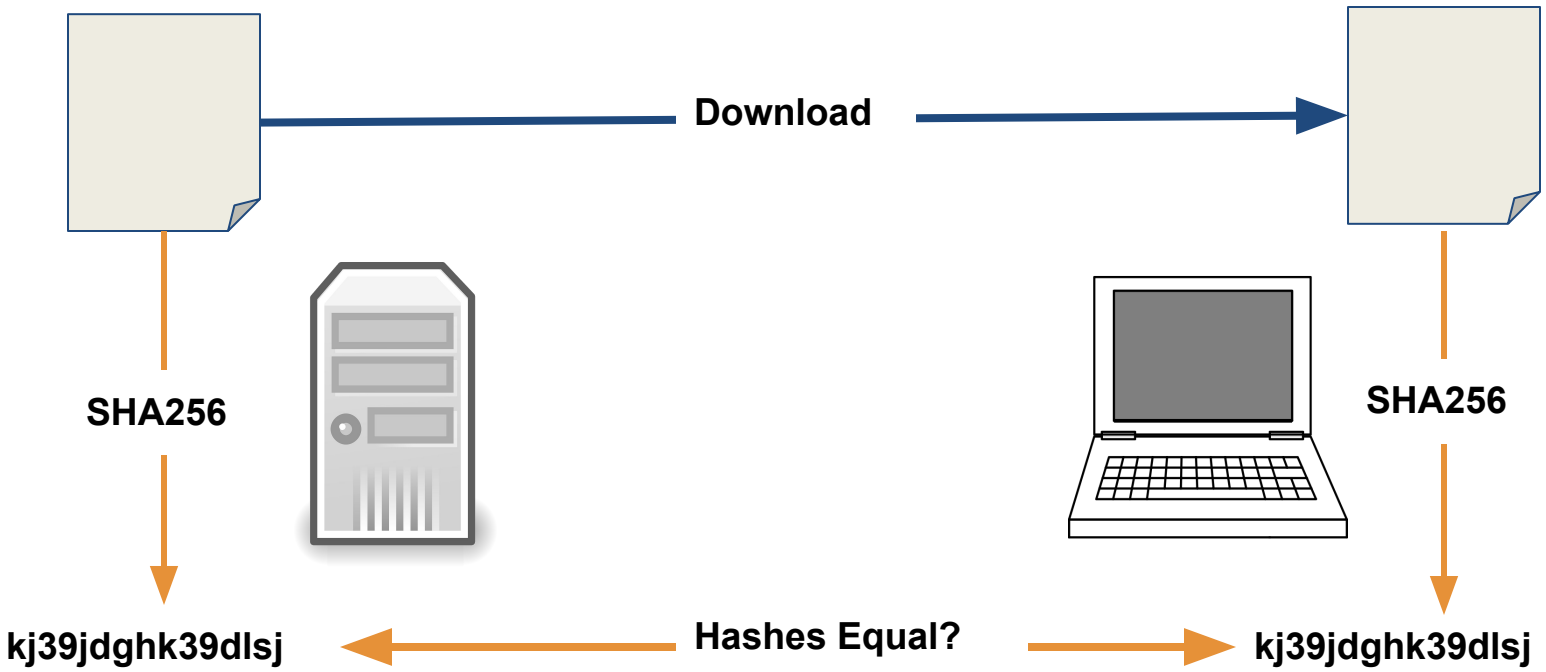
- **Deterministic**
  - The same message always results in the same hash.
- **One-Way Function**
  - You cannot reverse the cryptographic hash function to get to the data.
- **Collision Resistance**
  - It should be hard to find two different messages that hash to the same enciphered text.
- **Diffusion or Avalanche Effect**
  - Change a single bit or character and the output of hashed message should change significantly and unpredictably
- **Calculation Speed**
  - Fast, but no too fast

Uses of Cryptographic Hash Functions

AUBURN

- Password Encryption
- Cryptocurrency
- Digital Signatures
- Digital Certificates
- SSL/TLS
- **File Integrity Validation**

File Integrity Validation



AUBURN UNIVERSITY