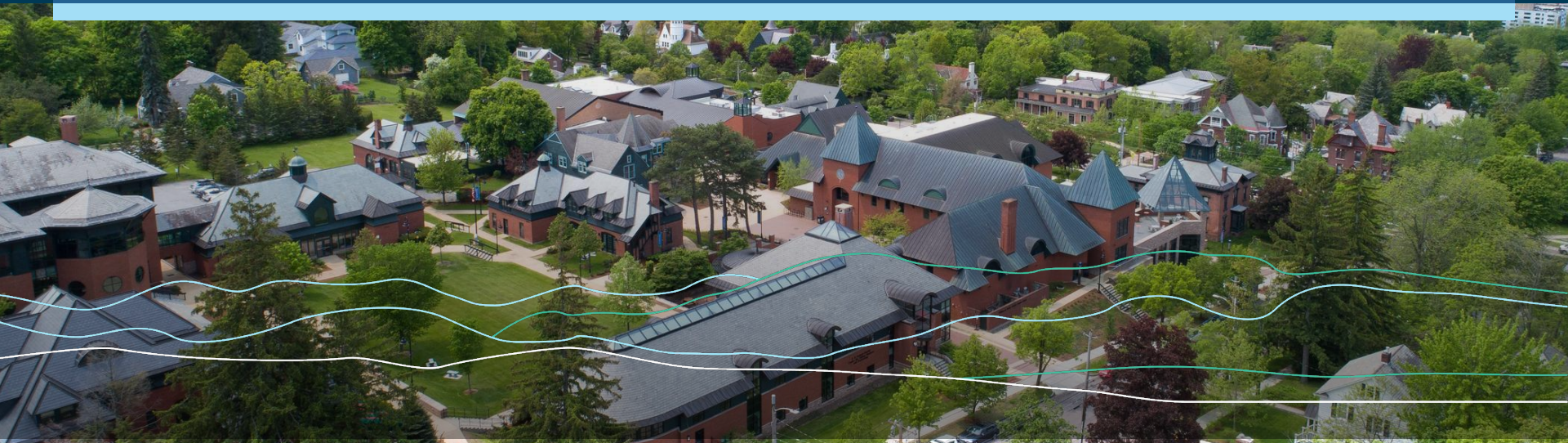
CHAMPLAIN COLLEGE

Mod 8 – Hashing & Modern Ciphers

SEC-110



Week 7 Review

CIA & NR

- **Confidentiality:** Encryption/decryption algorithms
- **Integrity:** Hash functions.
- **Availability:** Time - and workload- efficient security methods
- **Authenticity:** Digital signatures & digital certificates.
- **Non-Repudiation:** Digital signatures, digital certificates.

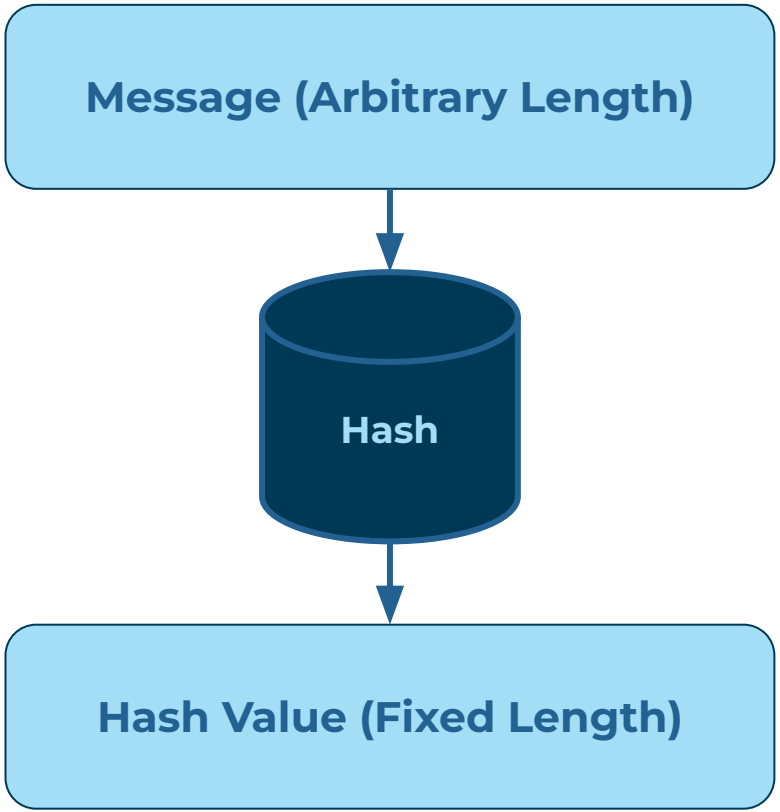
Integrity Problem

How does Bob know that the message or file was not altered in some way in transit?

- Solution: Hash functions.
- Hash functions can also be used to check if the data has been altered at rest (in storage)

Hash Functions Review

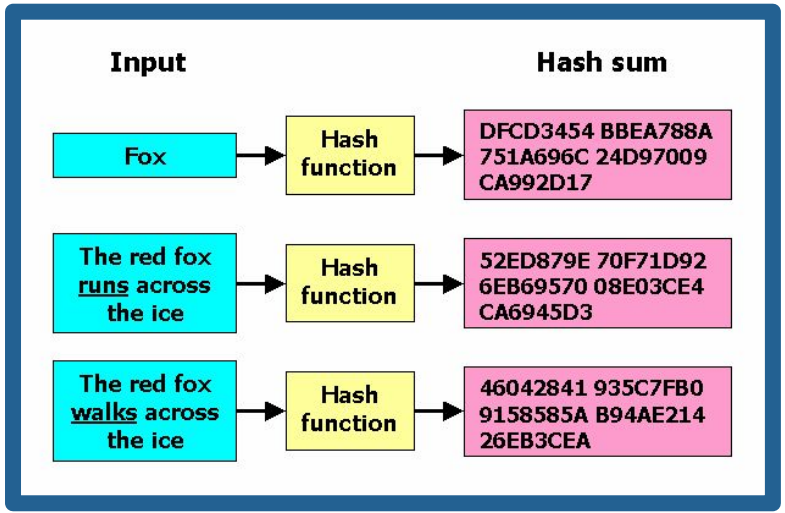
A **hash function** maps digital data of arbitrary size to digital data of **fixed size**. The hash is sometimes called a **message digest**.



Cryptographic Hash Functions

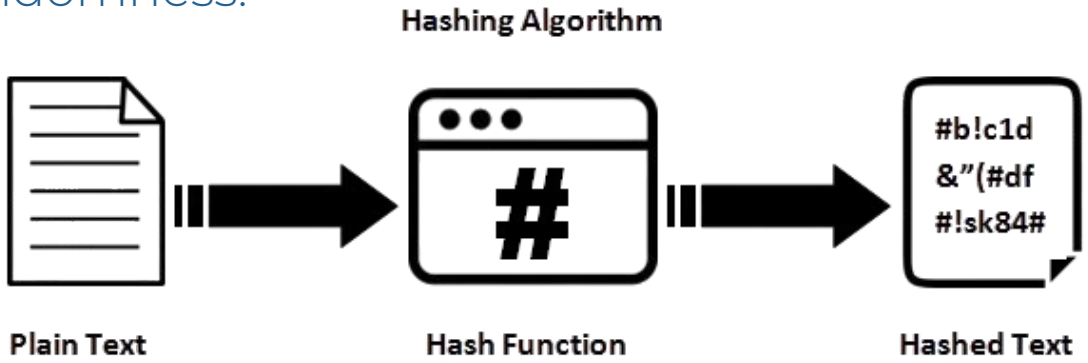
A cryptographic hash function is a hash function that is considered practically **impossible to invert** or find collisions (i.e. two messages with the same hash value).

- **Variable input/Fixed output size:** Can be applied to data of practically any size but the output is always a fixed number of bits.
- **Preimage resistant (not reversible):** Virtually impossible to find the input value for a given hash value



Cryptographic Hash Functions

- **Collision resistant:** Impossible to find two inputs that have the same hash value.
- **Efficiency:** Fast, and simple to compute on hardware and software
- **Pseudorandomness:** The outputs pass tests designed to detect not truly random, but imitating randomness known as pseudorandomness.

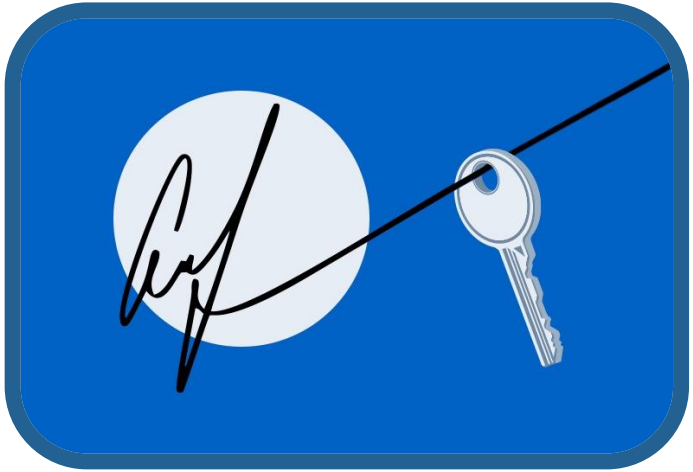


Utilizing Hash Functions

Password Files: Hashes of passwords are stored in password files. No one can see the plain password, this provides an extra layer of security in case the password file is stolen.

Utilizing Hash Functions

Digital Signatures: When you sign messages digitally, the hash value of the message is encrypted instead of the message itself. This allows messages of arbitrary lengths to be signed.



Utilizing Hash Functions

File signature: Related to virus detection, hashes serve as a fingerprint or signature for a file. You can differentiate between one Notepad.exe from another. Hashes are used to verify downloaded files.

Utilizing Hash Functions

Intrusion/Virus Detection: A change in the hash value of a file may indicate an intrusion or a virus.

Utilizing Hash Functions

Pseudorandom number generator: One of the required properties of a cryptographic function is that the output has to pass pseudorandomness tests.

- No detectable pattern or correlations
- Not reversible
- Collision Resistant
- Output distribution even across all possible values

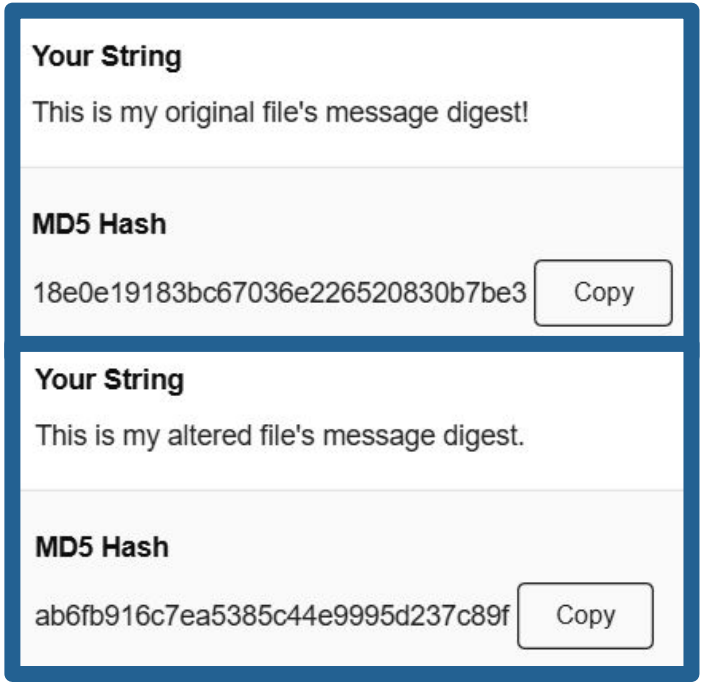
Utilizing Hash Functions

File synchronization:
Whether to upload a file or not for synchronization (for example with cloud storage) can be determined by checking the hash value of the file has changed or not since the last update.

Hash Algorithms

MD - Message Digest Algorithms

- MD4
  - 128 bit digests; used in TLS certificates
- MD5
  - Similar to MD4; security severely compromised, so not suitable for cryptographic use.



Hash Algorithms

- **SHA: Secure Hash Algorithm**
  - SHA-1
    - Designed by NSA
    - Published by NIST in 1993 as Federal Info. Processing Standard
  - SHA-2
    - Designed by NSA
    - Published by NIST in 2001 as Federal Info. Processing Standard

Hash Algorithms Examples

SHA-1 Hashing Example:

Cybersecurity Rocks

950f2e838ba18fe62fd030
b412ec1e4dd2a7b766

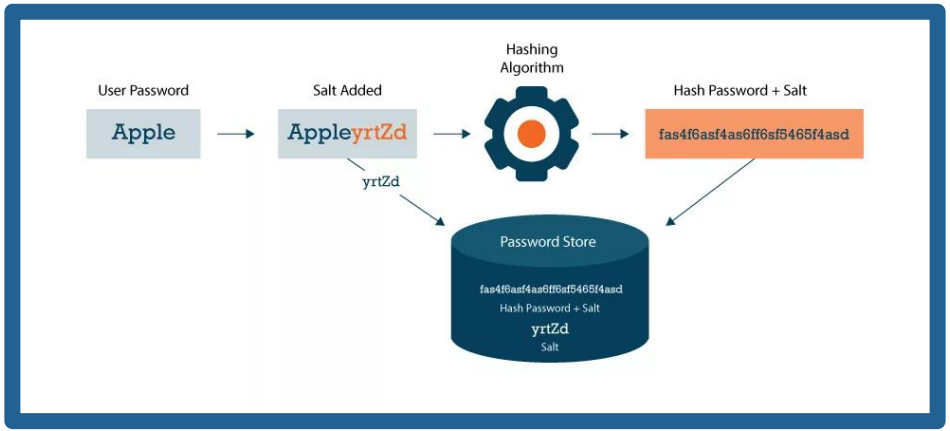
SHA-256 Hashing Example:

Cybersecurity Rocks

8a7e72a3370e27552d8cf7557f
84c64842da9de9e2e4c5713d
3b0c72ececf7fb

Salting

- Another technique used for securing hash functions is the practice of salting.
- The idea of **Cryptographic Salt** is to add a string of random characters to a password before it is hashed and stored to create an extra layer of randomness.



Rainbow Tables

A **rainbow table** is a password-cracking tool that uses a table with precomputed hash values to crack the password hashes in a database.

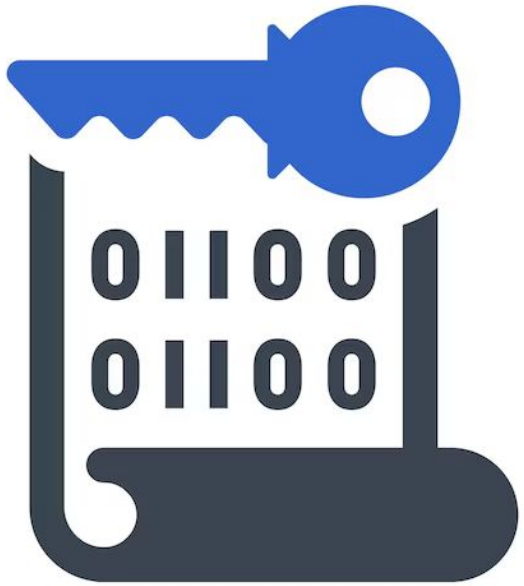
Salting helps prevent rainbow table attacks by ensuring that the same password used by two users **will not return the same value** because of the random salt value.

Modern Cipher Examples

An early concept was the **Caesar Cipher**, which shifted the letter of each word by a fixed number within the alphabet.

In our modern world with computers and tech, we have:

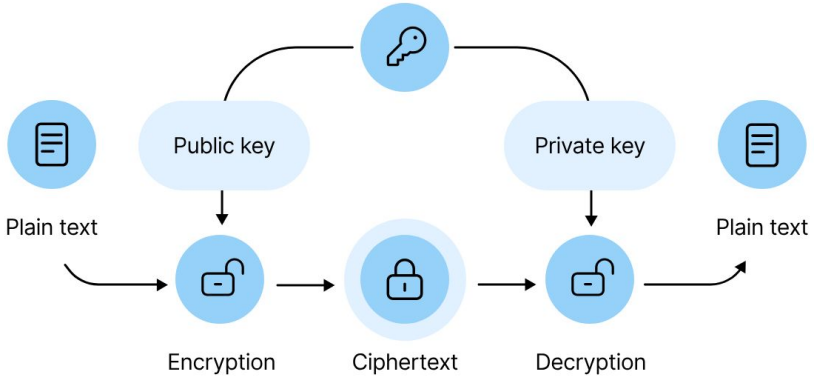
- **RSA Encryption**
- **AES Encryption**



Modern Cipher Examples

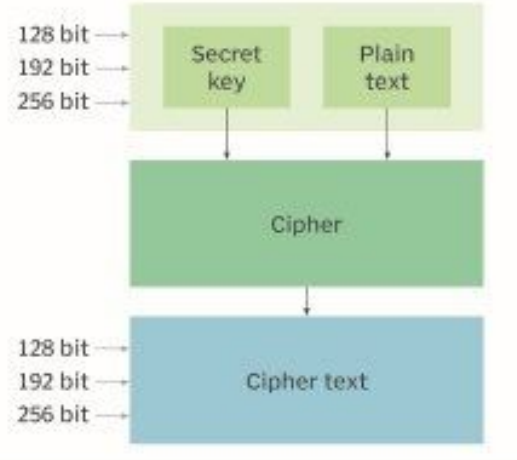
RSA Encryption

A public key system that uses a pair of keys to secure digital communication.



AES Encryption

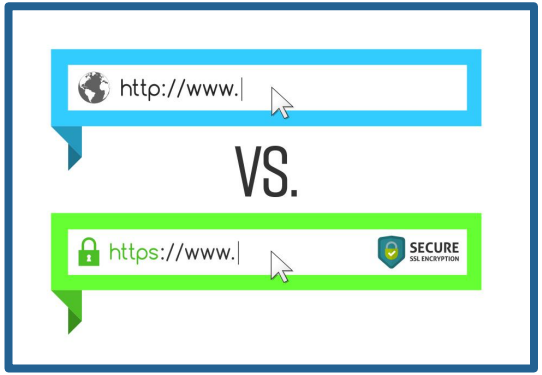
An algorithm that takes a fixed-size input and makes a ciphertext of 128/192/256 bits.

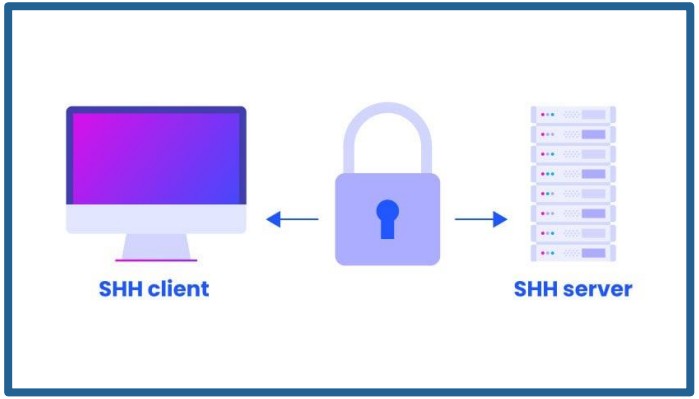


Cipher in the Real World (pt 1)

SSL/TLS Certificates

- Verification for a website's encrypted connections for secure online connection.





SSH Configurations

- Secure Shell to create a secure connection between two machines.

Ciphers in the Real World (pt 2)

Secure Messaging Apps

- End-to-end encryption via built-in apps or apps such as WhatsApp or Signal.

Electronic Money

- Protection of money being sent or transferred online.

Steganography

Steganography is the practice of **concealing** information within another message or physical object to avoid detection.

“Hiding in Plain sight”

- Invisible Ink
- Embedding a picture
- Masking in an audio file
- Inserting data into a video frame
- Hiding text in whitespaces
- Metadata