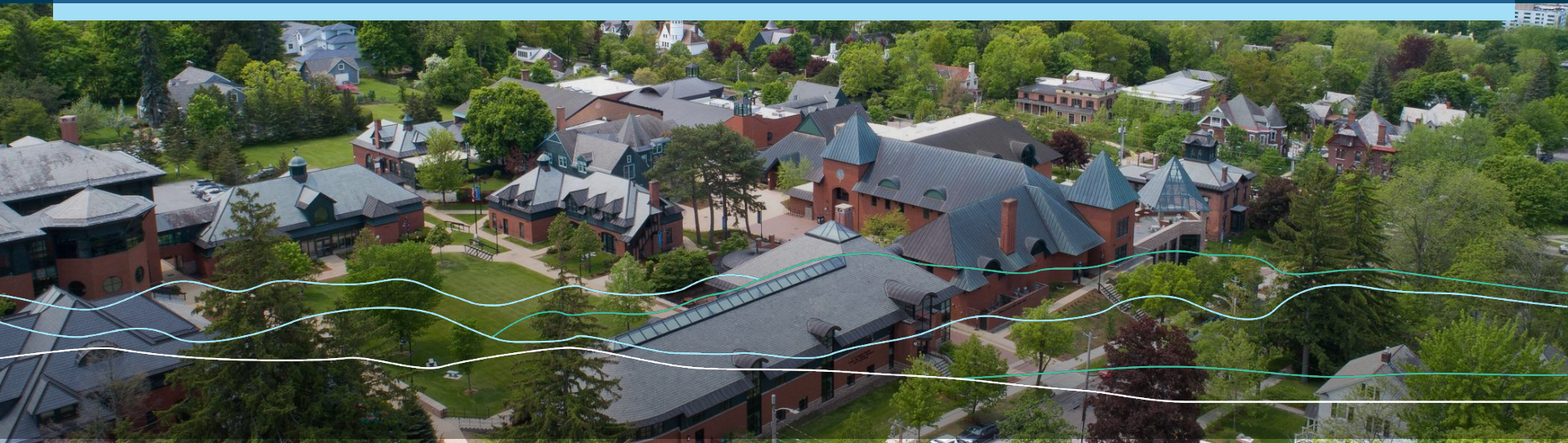
CHAMPLAIN COLLEGE

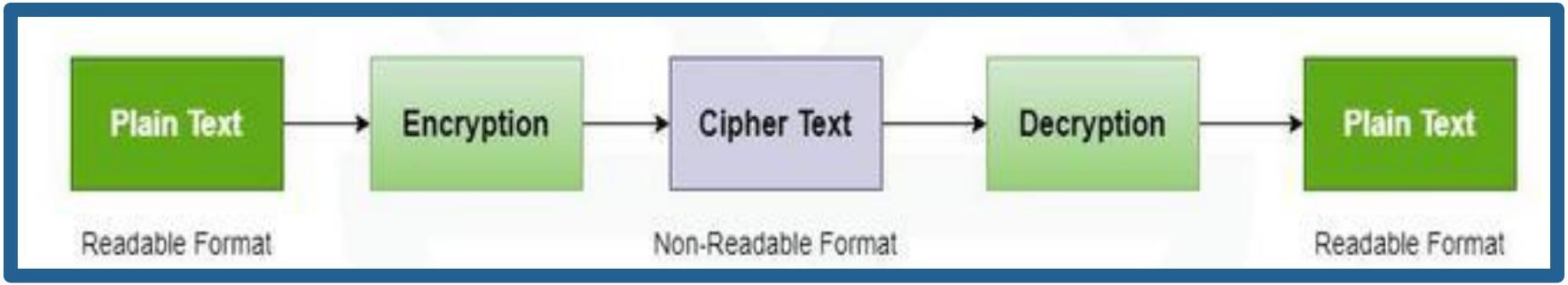
Mod 7 – Cryptography Basics

SEC-110



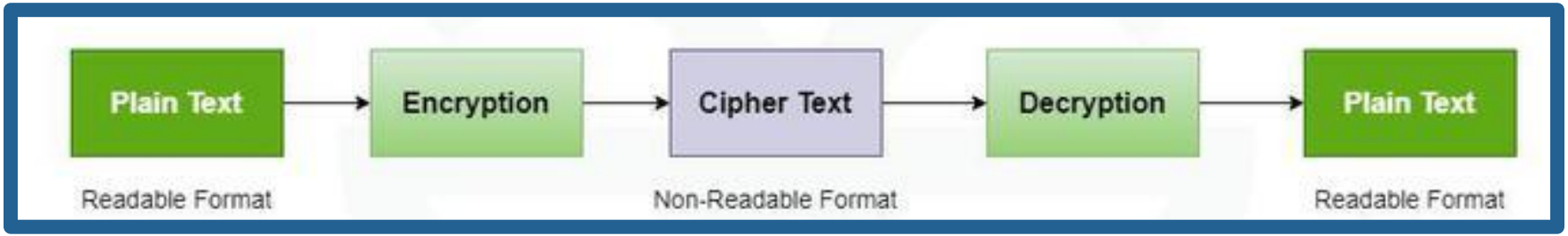
Cryptology Terms

- **Cryptography:** The art of writing and solving codes
- **Cryptology:** The study of cryptography
- **Cipher:** Method/code used to disguise text



Cryptology Terms

- **Plaintext:** the original text
- **Encrypt/Encode:** the process of disguising
- **Ciphertext:** the disguised text
- **Decrypt/Decode:** Remove disguise



New CIA Terms

CIA + NR in Cryptography

- **Confidentiality:** Using cryptography to keep data private
- **Integrity:** Using cryptography to ensure that data has not been altered
- **Availability:** Timely and ready access to information
- **Authentication:** Verifying that user is who they claim
- **Non-repudiation:** Ensure that user performed activity by proof that they cannot deny

Multi-Factor Authentication

How do you verify that user or system is who they claim?

Multi-Factor Authentication uses 2 out of 3 of the following:

- **What you know**
  - Username, password, pin, security question, etc.
- **What you have**
  - Key card, USB, smart phone, email address, etc.
- **What you are (biometric)**
  - Fingerprint, facial recognition, voice recognition, retina scan, etc.

Is it Multi-Factor?

1. **Username/password and a code sent via SMS to phone?**

   Yes

2. **Password and a security question?**

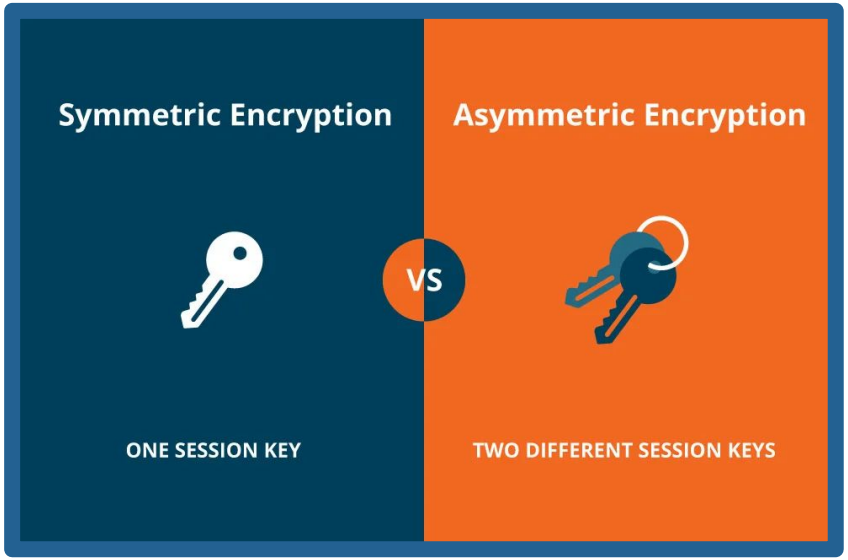
   No - both what you know

3. **Thumbprint scan to login to system?**

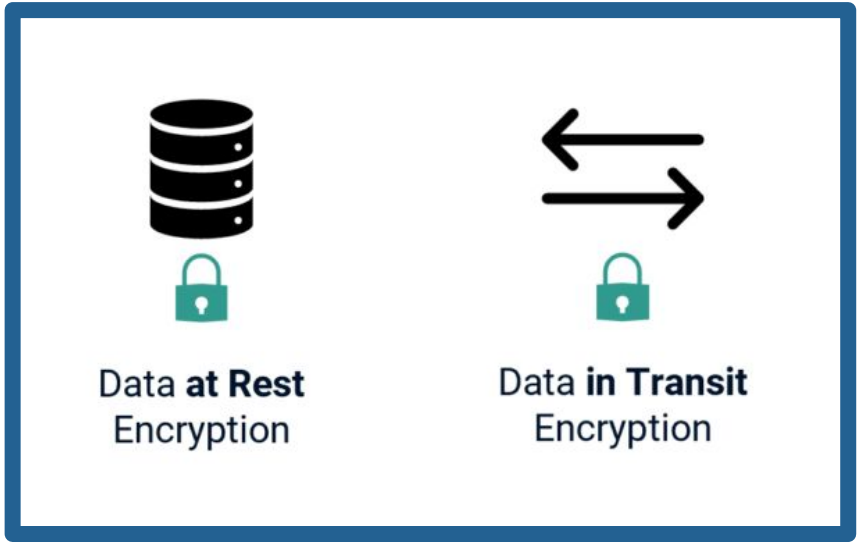
   No - single factor

Cryptography Methods Overview

Two Basic Methods:

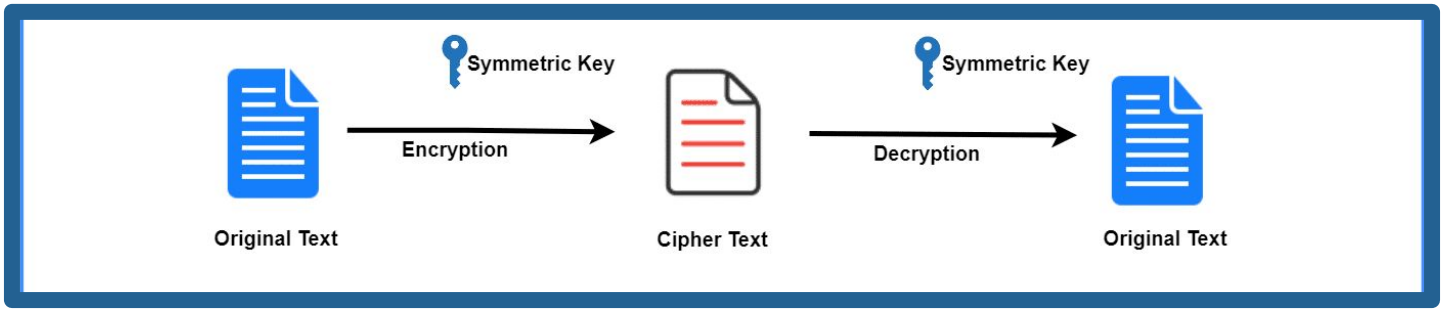


Two Common Applications:



Symmetric Encryption

- **One secret key**
  - Applied to a message to change the content in a particular way
  - If sender and recipient know the secret key, they can encrypt and decrypt messages

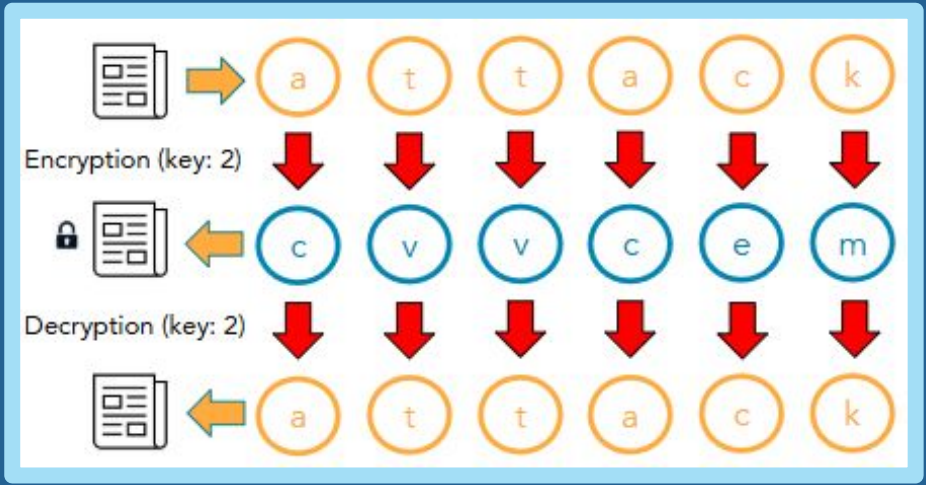


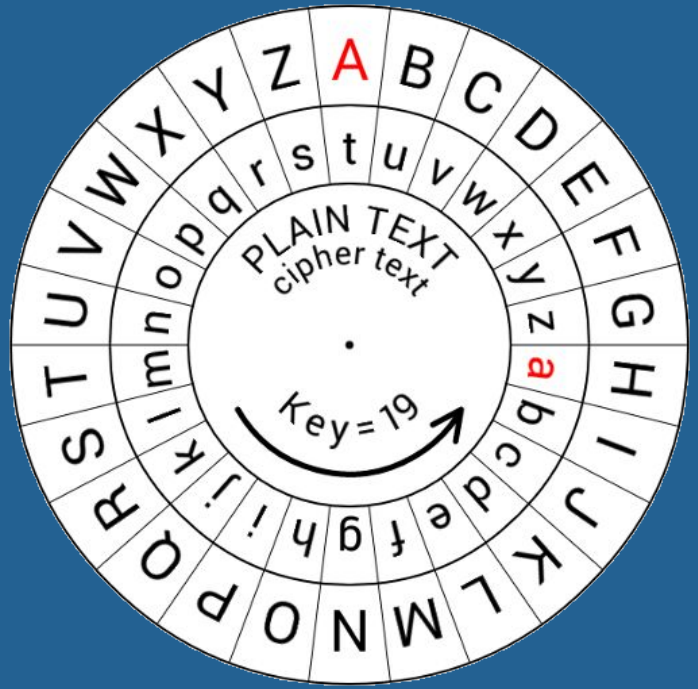
Atbash Cipher

Atbash Cipher is a cipher that simply works by reversing the alphabet. It is also known as the mirror code. For instance, the word "**Apple**" would be decoded to "**Zkkov**" as the letters in it matches each other when reversed. Such as the letter "**A**" becoming "**Z**" when Atbash Cipher is applied. Here's table example of what the conversion would look like;

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

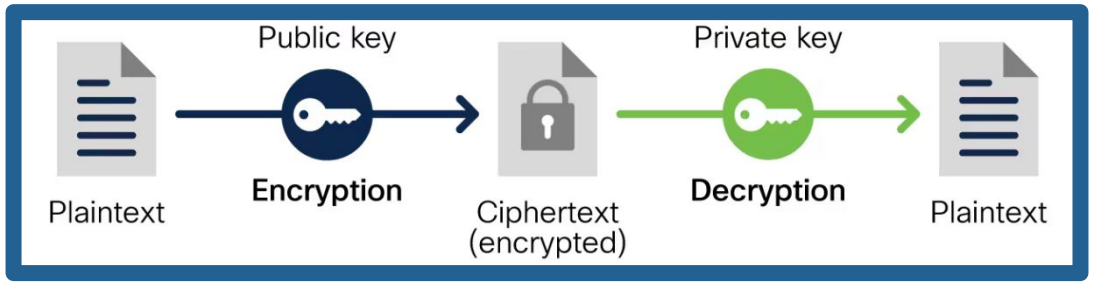
Caesar Cipher



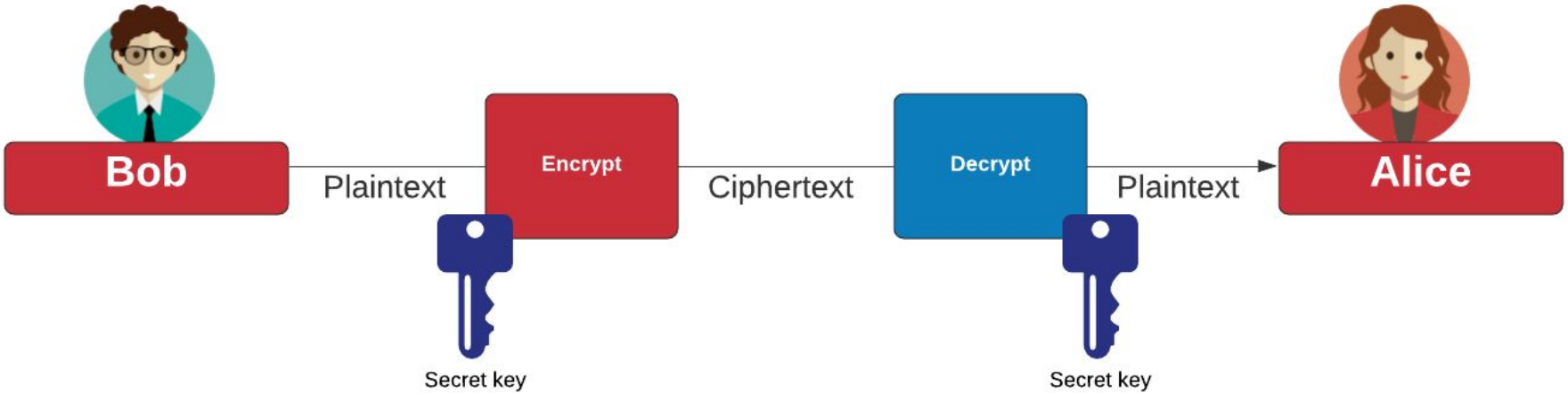


Asymmetric Encryption

- **Uses key pairs**
  - **Public key** – A key made available to anyone
  - **Private key** – Only the key owner knows
- Any message encrypted using the **public key** can only be decrypted by the matching **private key.**
- Any message encrypted using the **private key** can only be decrypted by the matching **public key.**



Asymmetric Encryption Example



Pros of Asymmetric Encryption: no need to exchange keys

Cons of Asymmetric Encryption: slow, requires more processing

Data in Transit/At Rest

Data in Transit:

Modern techniques use asymmetric encryption to start a communication and share a symmetric key going forward.

Relevant Protocols:

- SSL(Secure Sockets Layer)
- TLS (Transport Layer Security)
- SSH (Secure Shell)

Data at Rest:

Can apply to whole disk, volume, or file encryption, usually using symmetric encryption.

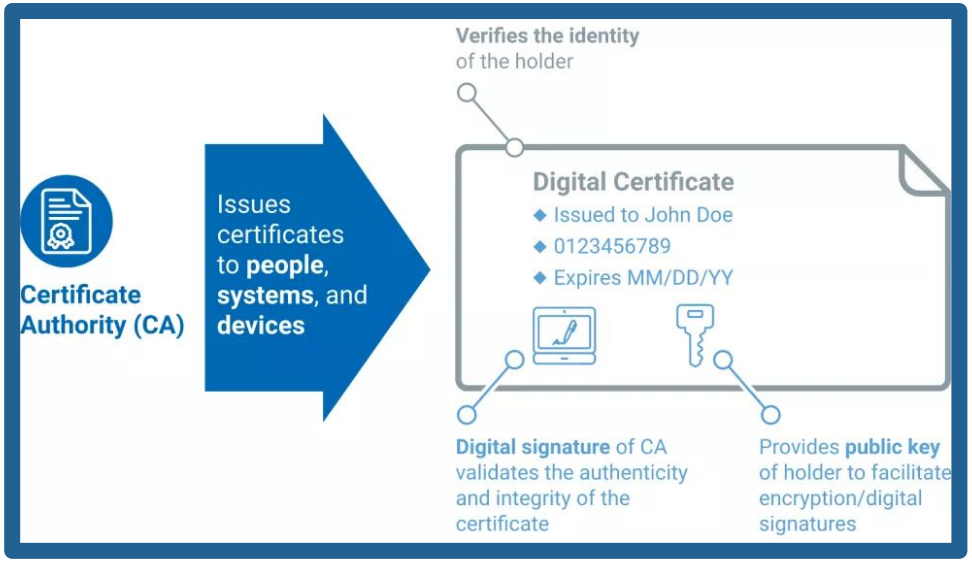
Relevant Algorithms:

- AES (Advanced Encryption Standard)

Digital Certificates

A **digital certificate** is an electronic file that verifies the identity of of a user, device, or website.

- Contains the **public key** for the connection
- **Signed by a certificate authority** (a trusted source for creating and issuing certificates)
- Systems **exchange certificates or public keys using SSL/TLS** to establish an encrypted connection



Hash Functions

Hash Function: An algorithm that computes a fixed-bit-length string from a block of data and used to test the integrity of a file

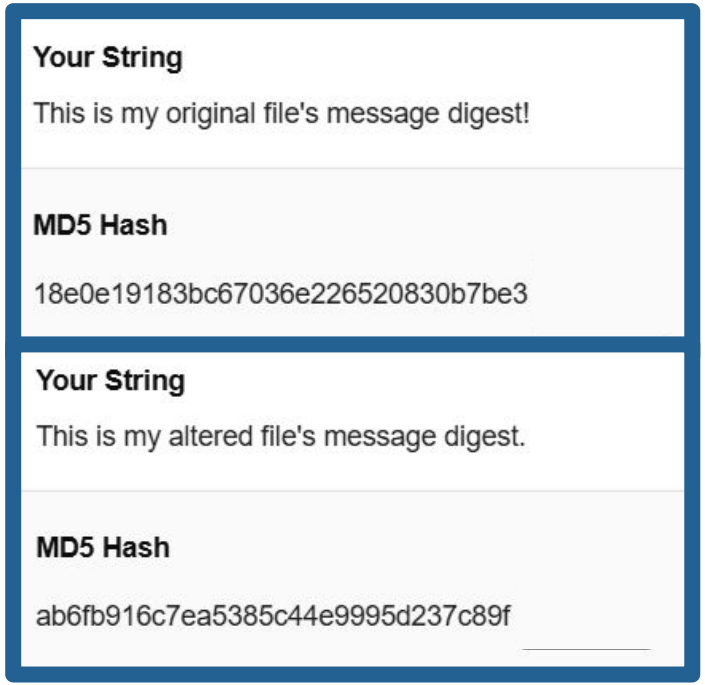
- **Message:** the data
- **Message Digest** or **Hash**: the fixed-bit string output

Popular hashing algorithms:

MD5 – creates 128-bit message digest

SHA-1: Creates 160-bit message digest

SHA-2: 256 and 512-bit message digests



Digital Signatures

Ensure that a party cannot deny the sending of a message that they originated.

- a “virtual fingerprint” unique to a person or entity
- use both **Digital Certificates** and **Hashes**