# CSC116 Authentication /Hash

# Multi-Factor Authentication

Three types:

1. Something you have, e.g., PC/phone
2. Something you know, e.g., passcode/password
3. Something you are, e.g., fingerprint

1. **Something you have**

Email Account,<br>
**Personal PC,**<br>
**Campus id card,**<br>
**Moblie Phone,**<br>
**iPad**, etc.

# Smart card is a token （Physical Token）

A smart card can be considered a type of token, specifically a security token, as it contains an embedded chip that stores sensitive information and can be used for authentication purposes like logging into systems or making secure transactions, effectively acting as a digital key or "token" to access services.

1. **Something you know**

Password
Passcode
SMS code
Authenticator code
Personal questions
, etc.

# 3 Biometrics — something you are

**Ear Shape Recognition**

**Voice Recognition**

# AI for Authentications

Facial Recognition Authentication

Behavioral Biometrics Authentication

Anomaly Detection in Authentication

Deep Learning for Phishing Detection

AI-Generated One-Time Passwords (OTP)

# Computer Vision for Facial Recognition

A **Computer Vision (CV) model** is an AI-based system that enables computers to **interpret, analyze, and understand visual data** (images, videos, or real-world scenes). These models process visual inputs to perform tasks such as object detection, facial recognition, image classification, segmentation, and motion tracking.

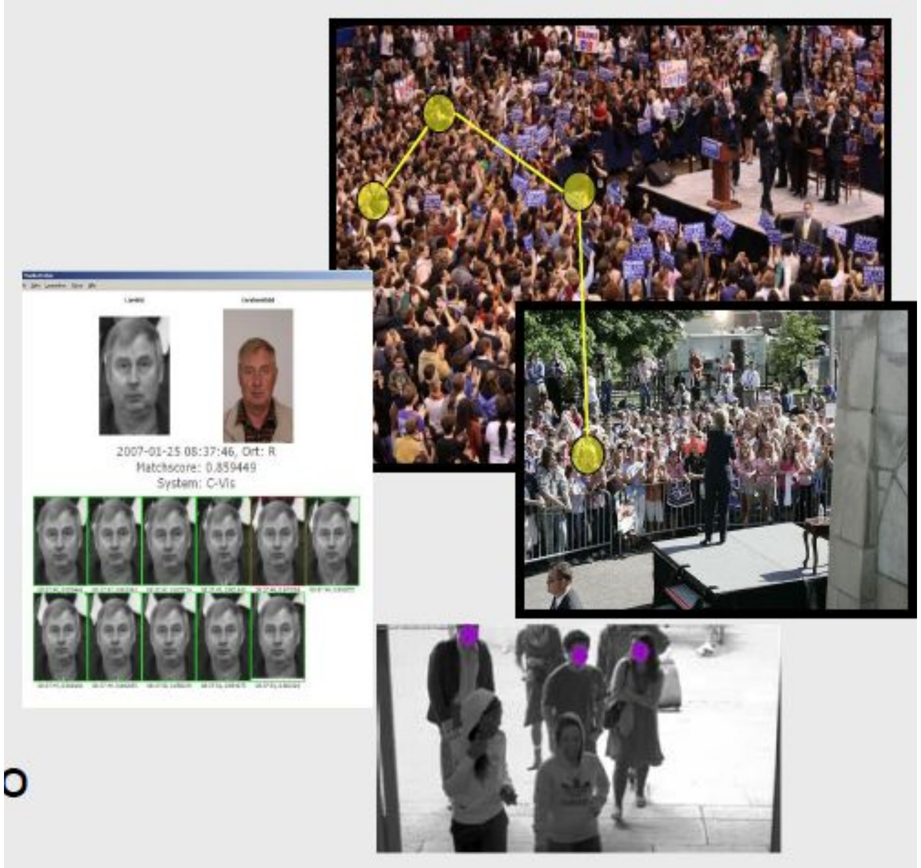
# Emotion Recognition

🔹 **How it works?**

- Analyzes facial expressions to detect emotions (e.g., happy, sad, angry).
- Uses CNNs trained on labeled facial datasets.

https://www.faceplusplus.com/demo/v2.html?module=FaceEmotionRecognition&language=en

# Next Generation Identification



2007-01-25 08:37:46, Ort: R
Matchscore: 0.859449
System: C-Vis

# Cashier-Free Checkout System

https://www.youtube.com/watch?v=NrmMk1Myrxc

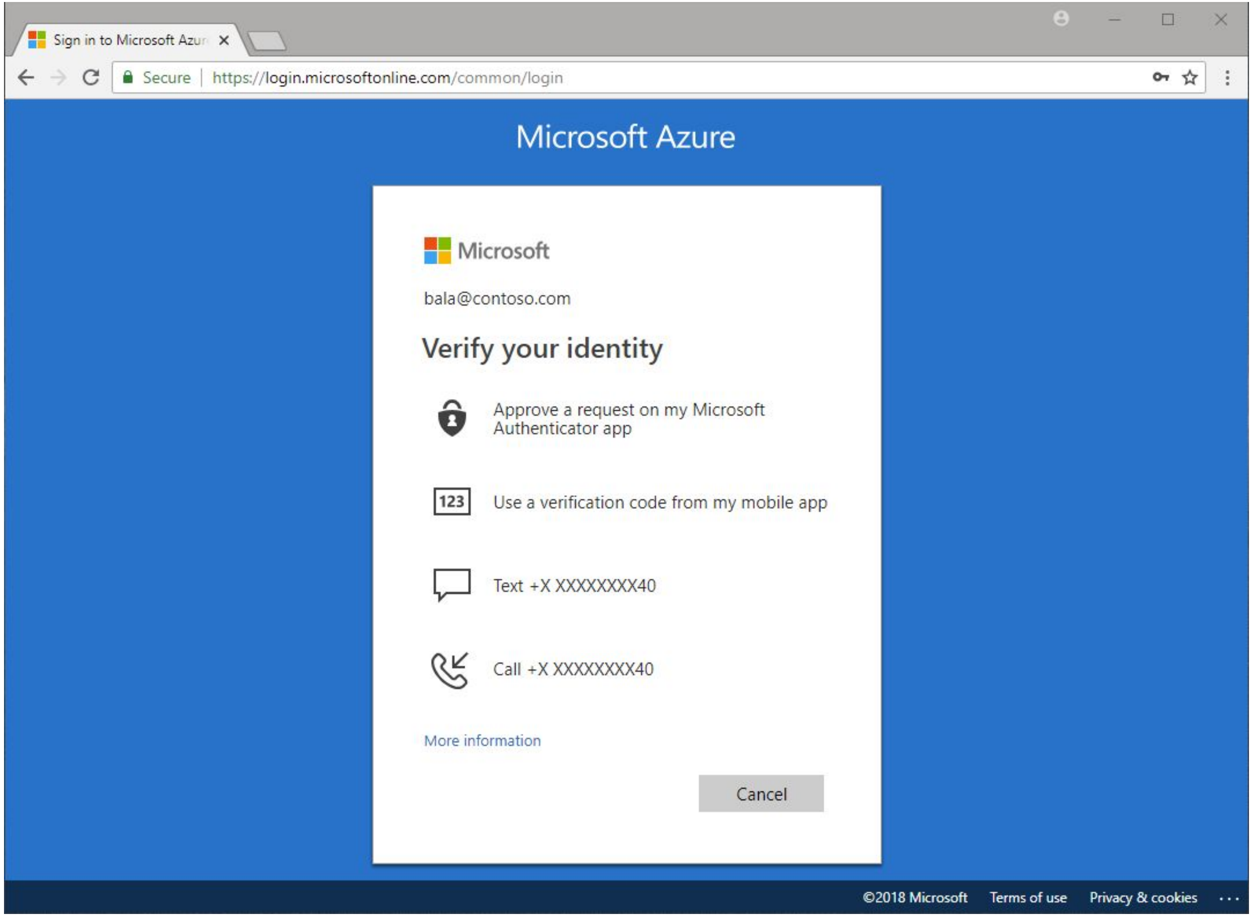
Cashier-free checkout systems (e.g., Amazon Go, AiFi, Grabango) rely on a combination of **AI, computer vision, sensors, and RFID** (Radio Frequency Identification) tag to track what a user picks up and purchases.

1. Use Password + Passcode (send to your email account) to log in ?

2. Use Password + Answer a personal question to log in ?

3. Use Password + SMS codes ?

4. Use Password + ID card ?



Sign in to Microsoft Azur
Secure
https://login.microsoftonline.com/common/login

Microsoft Azure

Microsoft

bala@contoso.com

Verify your identity

Approve a request on my Microsoft Authenticator app

123 Use a verification code from my mobile app

Text +X XXXXXXXX40

Call +X XXXXXXXX40

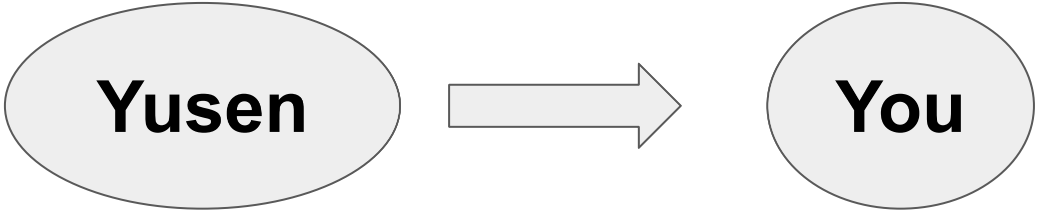
More information

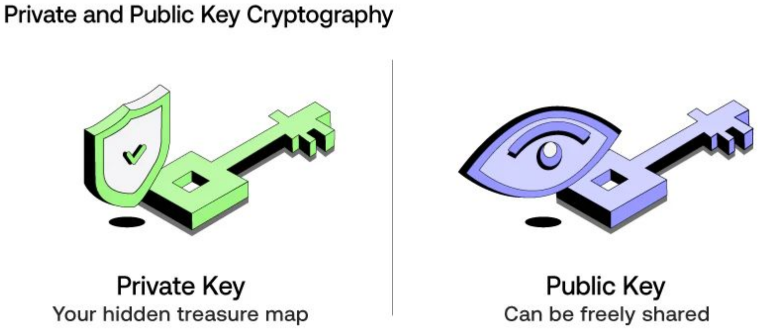
Cancel

©2018 Microsoft Terms of use Privacy & cookies ...

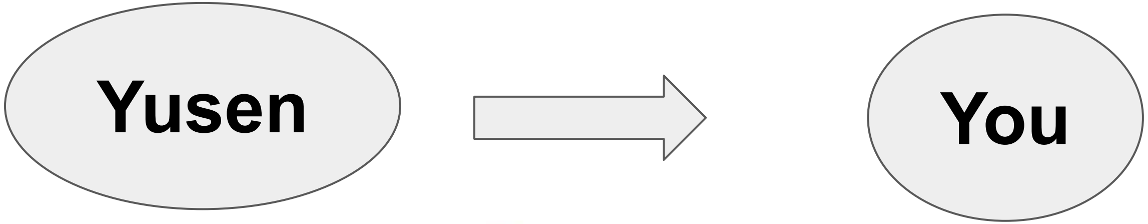
Question?

# Answer an challenging Question also can authenticate who you are.





# Answer an challenging Question also can authenticate who you are.

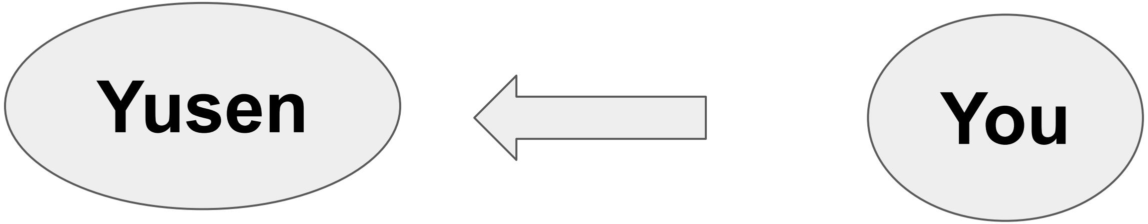


**Yusen**

**You**

Public
Key

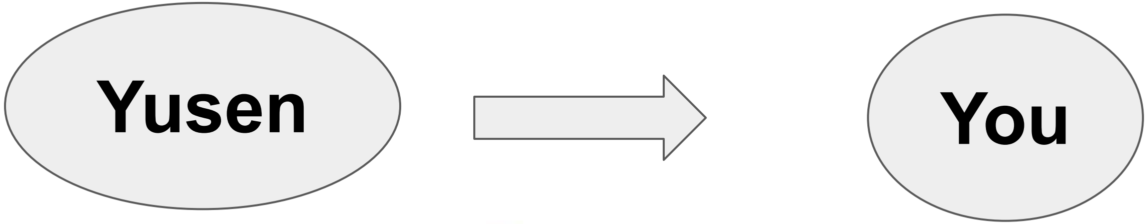
# Answer an challenging Question also can **authenticate** who you are.



Ciphertext

```
hQIMAw3Jn/nLK/38ARAAsSXLDhCtzUYKMptNxZImJXwhhIRm3QxfuyHjJ93ASylE
e+6ABkuyFLJhiKryxp/JmS/alMPfF7hx2aTgovagaPzTwTV1jo6If2mhdCl6keed
1Iz7C0f6jHIqq9d8g0bWDyvELEipn5LNDTX3Xp2Csx5ojRB2wckrUt1l1Xyj8G0H
4DQUYbINRmJVulJJC/acGvgOze66pHuRgSCxxHDscefjXenh/XejSYTo7aMi+Es7
DCcD49zH6ZLDQN6BlN9q2oFI8QIhQ2y1QJbat1dWi/4yYWlKZcLKRSm8eo/gNCdL
h9MncXBBSfgbvbu67CDZ9GO5geZOn3LzQOpJ8hrZq/6K/uMcUKeZjW3RCo0T754f
E5zYe1wUgtwS/lmQ2w5PQF/89bpshtDSYuL1fZgzrsE6DwophuCri5zwCGbEKlsI
g6REIETFbZ2aCL4N2pZVunCIEuoP0zgEB6+M9egdpyxMsMqEBVg3AH7Sa1AtEguP
T/MCxI0bZHCUhPupEKT8slbSrDNxTWMUXQt3XpL0bGCCrDMKLSoWYfDiNnRkFbWK
iiqw9hx4Q9CJg7xX7JRnVgwOeREiFnMYSbFlvPSxEOu6FdBYhdqSefKin4Wnkmdw
qrSl8fjIW/kZ2v72uz0buEKkY9ubBox76yjlRo9KUQMs3em03kc64959gTDiZ0qF
AgwDrosDPQ2BeYQBD/9H5VKFw0an5j5MX1JpOSBAqNGKWq2bcEFnwJfk0DDlhyHD
owHiG7gDowCS+5y/pf56v36HkzpJZATKqoRyKVxmQOxU9l3YnPc5fw8iFhxlrfcG
ywzkJh/BRDQ/uy5fhGc/PbSm6iLv/SkkWTK8PSUD+g1yZyK0W7WkMh9QYS2OE7lQ
qbwpNiy57reWkUWCoE4QmKqqpe7NXXM0eLT9l2D0hG2lthyvTvspkpxszl8+HMJv
M2LMcY2FmmZWAJSdxsQSq9NQdyvCJX2D8oa89WQyXmp7mPXL7BQfoQNPndmn6Obi
0EQojoeMRNh14XNhMjPjxW7m34rH2gtvdN3Dg8iFrtocoVJqXqU3N+9T2sNe/bS8
```

# For communication only, you can not use you private key to encrypt a message



Yusen

You

**Private Key**

But **Digital Signature**
needs it

# Hash function (SHA-256 Hashing)

A **hash function** is a mathematical algorithm that converts any input (such as patient records, medical notes, or passwords) **into a fixed-length string** of characters, called a **hash value or hash code.**

# Demo

https://guggero.github.io/blockchain-demo/#!/hash

# Hash collision

https://colab.research.google.com/drive/1R6MktlqvXBRpoQBWRi1mJjeIhpKzrnjJ?usp=sharing

**If you remember the moment when, after many years of hard work and a long voyage**

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

**You stand in the center of your room**

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

**For CSer: How to solve the Collision?: https://www.youtube.com/watch?v=td0h7cv4cc0**

# Features of Hash function

1 The same input will always produce the same hash value.

2 No matter how long or short the input is, the output hash is always of fixed length.

3 It is **impossible** to reverse-engineer the original input from the hash value.

4 Different inputs should produce different hash values.

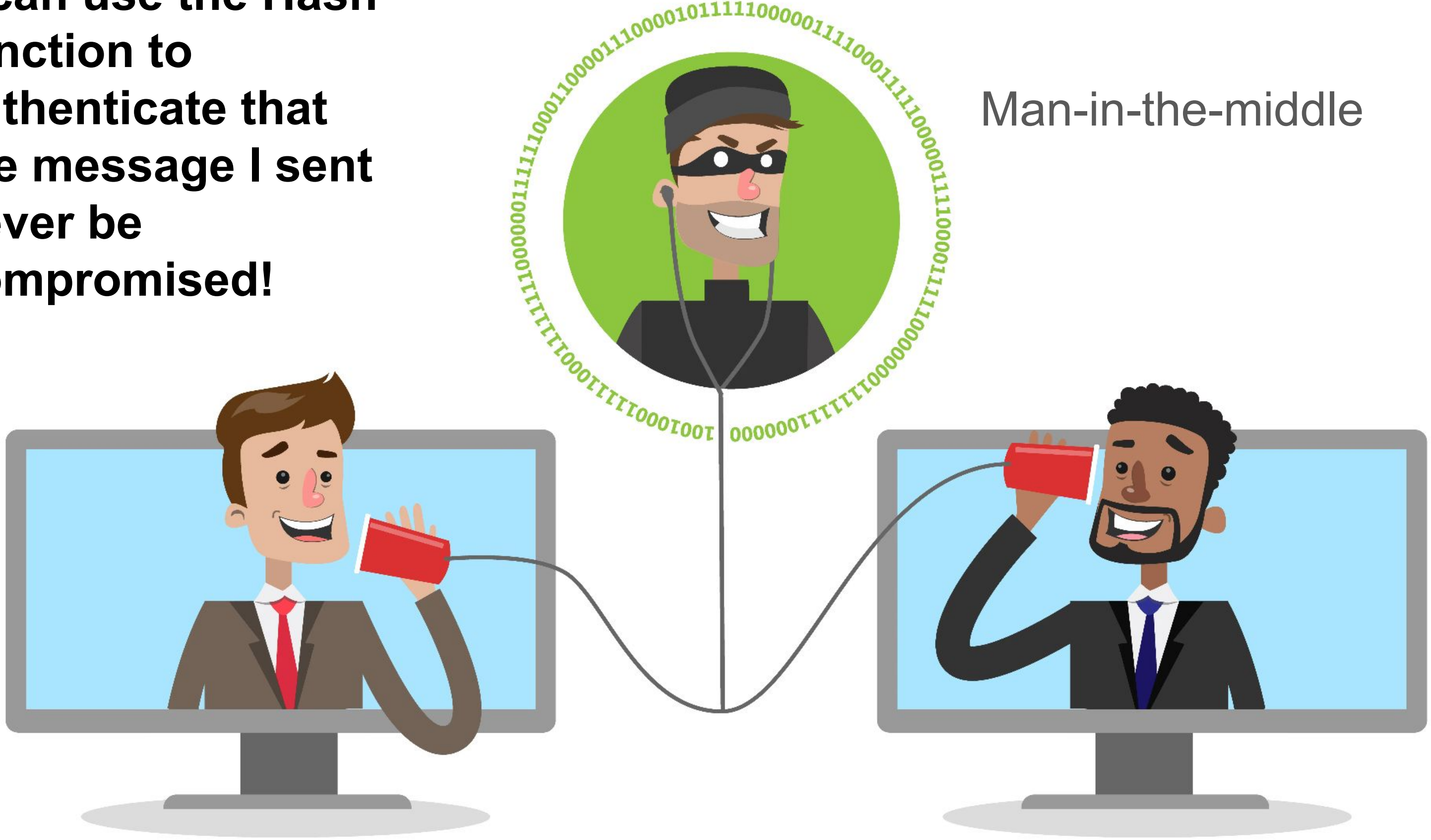
5 Hash functions are designed to compute hashes quickly, even for large amounts of data.

6 Hash functions allow for quick verification of data integrity.

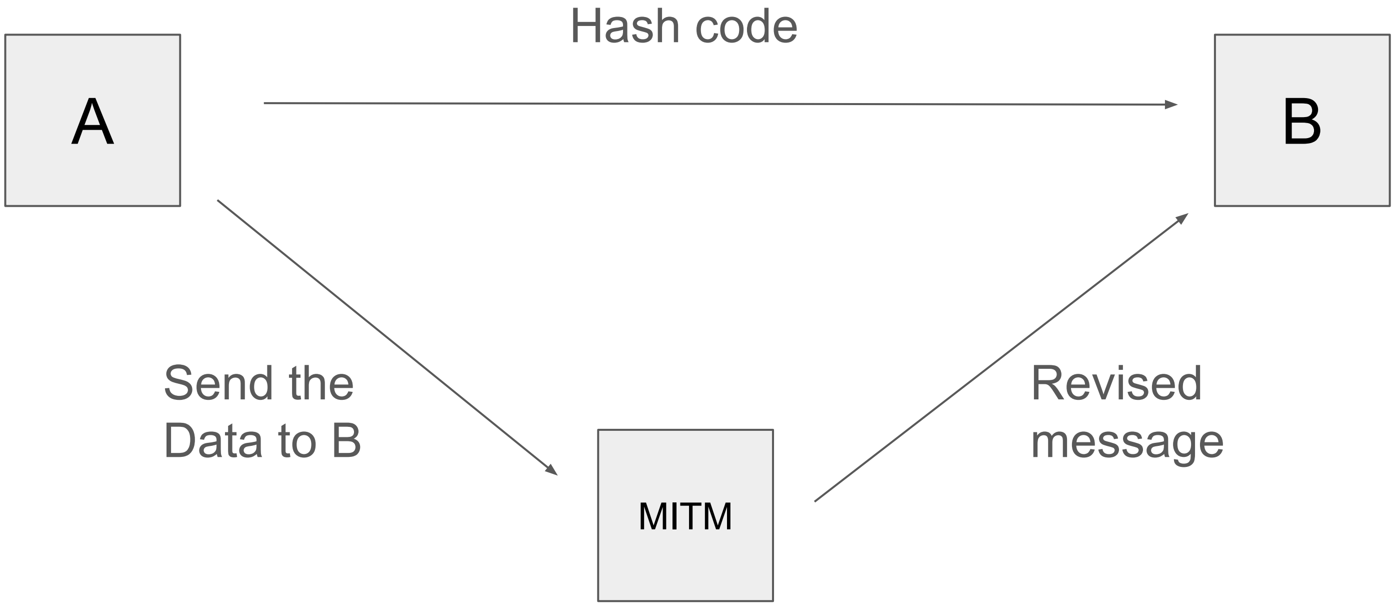
7 A small change in the input results in a huge change in the hash code.

Hash Code can be used for Authenticate the messages

**I  can use the Hash function to authenticate that the message I sent never be compromised!**



Man-in-the-middle


Hash code
A
B
Send the Data to B
MITM
Revised message

## Current systems now all use hash Password

Store raw password is dangerous!

# Hash Password

Storing passwords **in plaintext** is highly insecure. If a database is leaked or compromised, all user passwords are immediately exposed.

To improve security, we store **hashed passwords** instead of plaintext passwords. The idea is:

1. When a user creates a password, it is hashed and stored in the database.
2. When the user logs in, the entered password is hashed again and compared to the stored hash.
3. If the two hashes match, authentication is successful.

# Rainbow Table Attack 🌈

- Attackers use **precomputed hash databases** to reverse hashes back into original passwords.
- If a database contains `MD5("123456")`, an attacker can quickly find that hash and determine the password.

# Demo

https://guggero.github.io/blockchain-demo/#!/hash

```
password123
qwerty
letmein
```

```
Generate a strong
password please!
```

**Digital Signature** needs to use private key to encrypt your name.

# CSC 116 Digital Signature

https://www.adobe.com/acrobat/online/sign-pdf.html

If someone scans and modifies it, how can we prove it’s real?

# What is a digital signature?

A digital signature is an electronic, encrypted, stamp of authentication on digital information such as email messages, or electronic documents. A signature confirms that the information originated from the signer and has not been altered.

# Digital Signature Assurances

- **Authenticity** The signer is confirmed as the signer.
- **Integrity** The content has not been changed or tampered with since it was digitally signed.
- **Non-repudiation** Proves to all parties the origin of the signed content. Repudiation refers to the act of a signer denying any association with the signed content.
- **Notarization** Notarization is the official process of verifying the authenticity of the signature a notary public, a legally authorized official.

Signed by:

Joe Echevarria

1C03B78BEAD7410...

Joseph J. Echevarria
President, University of Miami
Chief Executive Officer, UHealth

Signed by:

Joe Echevarria

1C03B78BFAD7410...

Joseph J. Echevarria
President, University of Miami
Chief Executive Officer, UHealth

DocuSigned by:

Dipen Parekh

7AC89B6F5ABA40E...

Dipen J. Parekh, M.D.
Chief Executive Officer of UHealth
Executive Vice President of Health Affairs
of the University of Miami
Founding Director, Desai Sethi Urology Institute
Professor, Department of Urology
Dr. Victor A. Politano Endowed Chair in Clinical Urology
University of Miami, Leonard M. Miller School of Medicine

Signed by:

Henri Ford

305E62C689B2426...

Henri R. Ford, M.D., M.H.A.
Dean and Chief Academic Officer
University of Miami, Leonard M. Miller School of Medicine

DocuSigned by:

Jose Romano, M.D.

6327346A77F34B3...

Jose Romano, M.D.
Professor of Neurology
Chair, Department of Neurology
University of Miami, Leonard M. Miller School of Medicine

Agreed to and accepted:

Signed by:

Yusen Wu, Ph.D.

E3601B156A404EE...

8/5/2025

Yusen Wu, Ph.D. Date

# How to implement!

## Key Generation（Step 1）

- The sender (signer) generates a **key pair** consisting of:
    - **Private Key** – Used to create the digital signature.
    - **Public Key** – Used by recipients to verify the signature.
- This key pair is generated using cryptographic algorithms such as **RSA** or **ECDSA**.

# Document Hashing（Step 2）

- The sender selects the document or message to be signed (e.g., a medical record or e-prescription).
- A **hash function** (e.g., SHA-256) is applied to the document, producing a **unique hash value**
- The hash value represents the content in a **fixed-size format**, ensuring any modification will change the hash.

# Digital Signature Creation (Step 3)

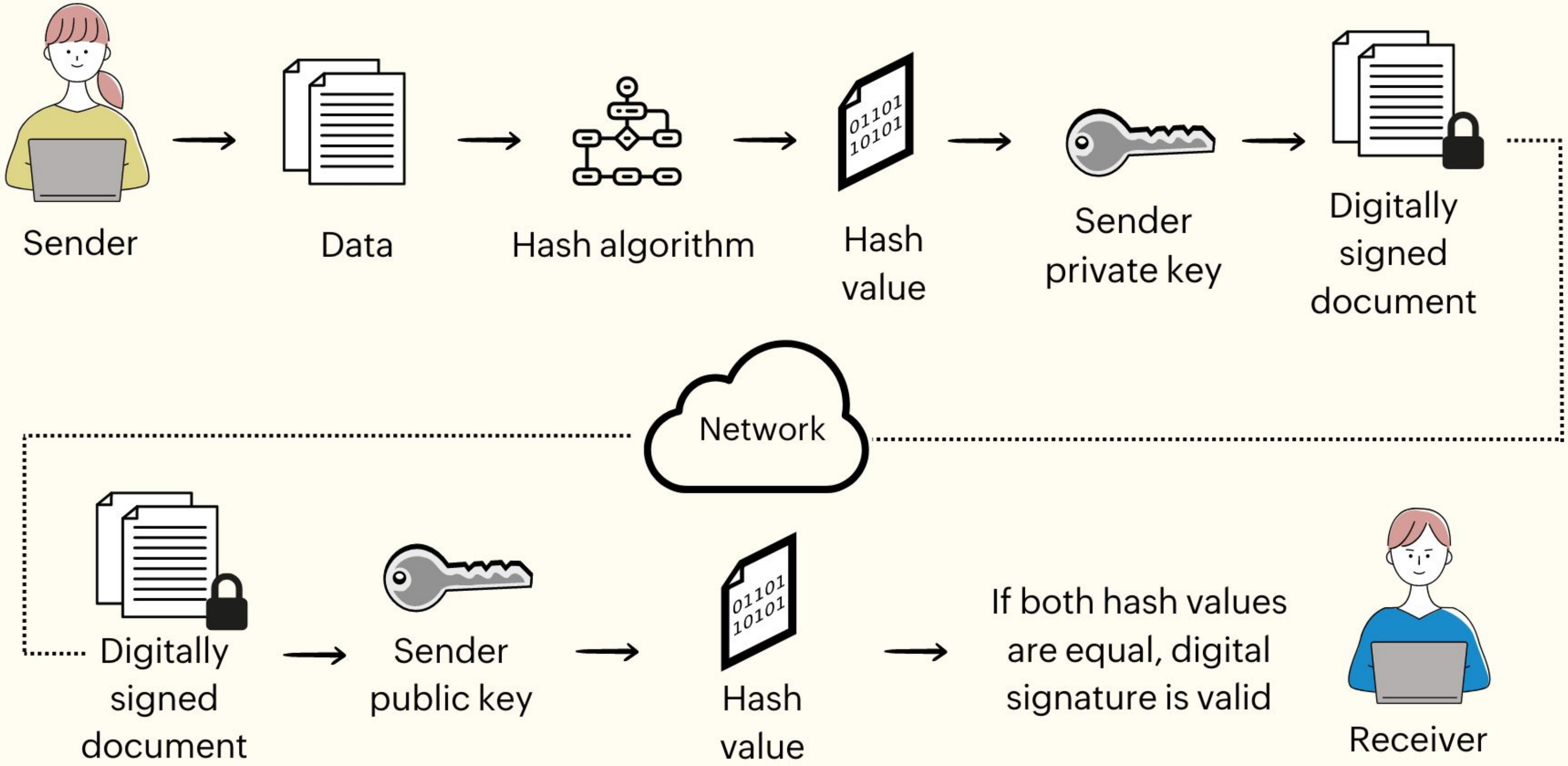
- The sender encrypts the **hash value** using their **private key** to generate the **digital signature**.
- This encrypted hash, along with the original document, is sent to the recipient.

## Signature Transmission（Step 4）

- The **digitally signed document** (original document + digital signature) is sent to the recipient.

You cannot use your private key to encrypt a secret.

However, if someone can successfully decrypt a ciphertext with your public key, it proves that the ciphertext was generated using your private key and therefore came from you.


Sender
Data
Hash algorithm
01101
10101
Hash value
Sender private key
Digitally signed document
Network
Digitally signed document
Sender public key
01101
10101
Hash value
If both hash values are equal, digital signature is valid
Receiver

If you want to use private key to encrypt a message, it is not allowed, as your public key is public.

Private key encryption only used for digital signature to encrypt hash code.