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.

How to use Computer Science Solutions to Ensure These 4 Features?

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** (digest).
- 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）

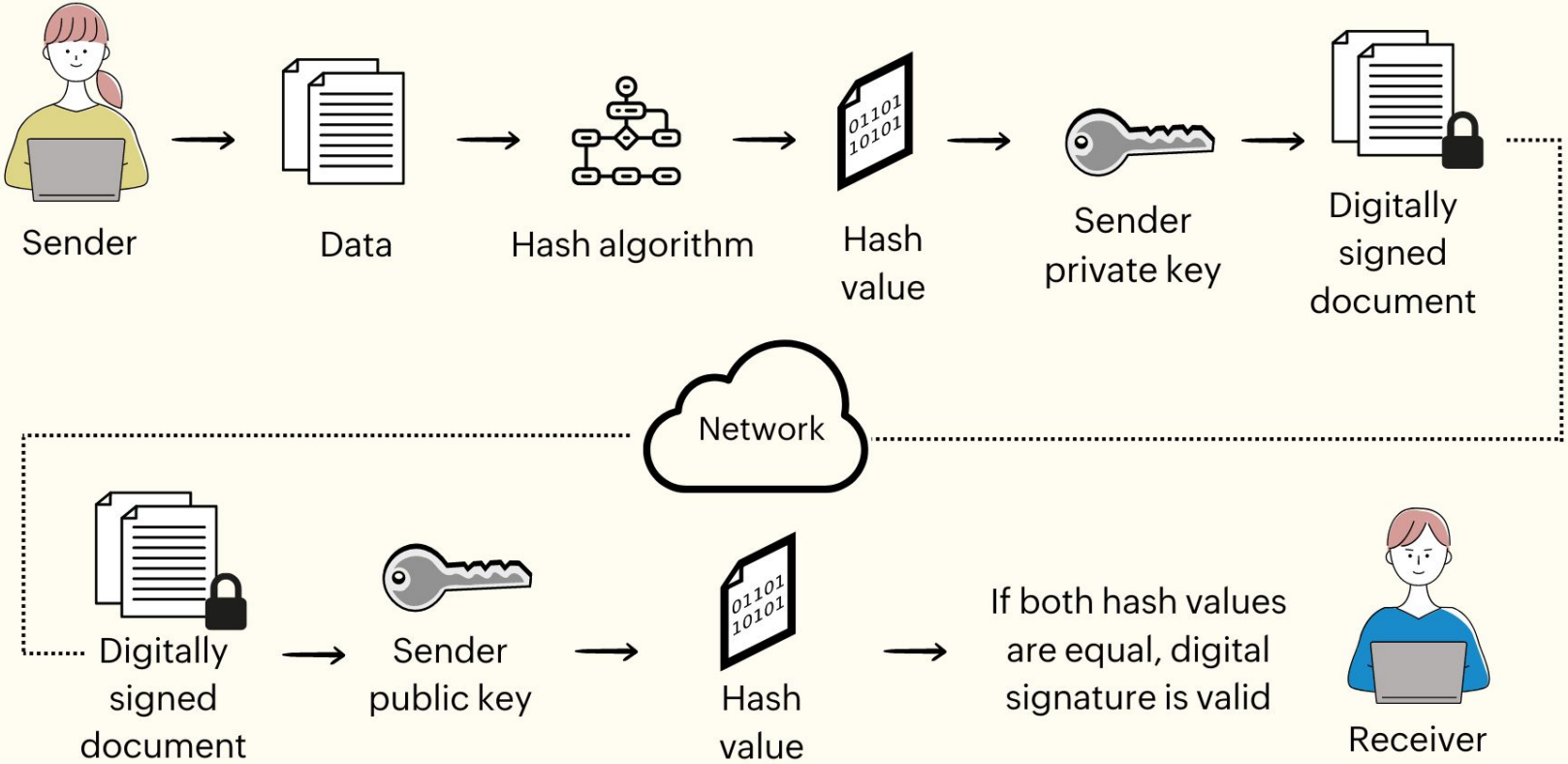
- The **digitally signed document** (original document + digital signature) is sent to the recipient.
- The sender may also attach their **public key** or a **digital certificate** issued by a **Certificate Authority (CA)**.

Signature Verification（Step 5）

- The recipient:
  1. **Applies the same hash function** to the received document to generate a new hash value.
  2. **Decrypts the received digital signature** using the sender's **public key** to retrieve the original hash.
  3. **Compares both hash values**:
     - ✅ **If hashes match:** The document is **authentic and untampered**.
     - ❌ **If hashes do not match:** The document has been **modified or forged**.

Document Acceptance or Rejection (Step 6)

- If the signature is **valid**, the recipient **trusts and accepts** the document.
- If the signature is **invalid**, the recipient **rejects** the document and may request a **resend** or **report fraud**.


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

Signature Style

- **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.

1. **Encryption with a Public Key, Decryption with a Private Key**:

$$\text{Ciphertext} = \text{Encrypt}(\text{Message}, \text{Public Key})$$

$$\text{Message} = \text{Decrypt}(\text{Ciphertext}, \text{Private Key})$$

   - This is used for **confidential communication**, ensuring that only the intended recipient (who owns the private key) can decrypt the message.

2. **Signing with a Private Key, Verification with a Public Key**:

$$\text{Signature} = \text{Encrypt}(\text{Hash}(\text{Message}), \text{Private Key})$$

$$\text{Hash}(\text{Message}) = \text{Decrypt}(\text{Signature}, \text{Public Key})$$

- This is used for **digital signatures**, allowing anyone with the public key to verify that the message was signed by the corresponding private key owner.

Why not use your private key to encrypt the messages？

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

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

Where Digital Signature Can be Applied?

Healthcare & Medical Industry

Electronic Health Records (EHRs) – Ensures that medical records remain unaltered.
E-Prescriptions – Doctors digitally sign prescriptions, preventing fraud.
Consent Forms – Patients can sign treatment agreements digitally.

Education & Academic Institutions

Digital Diplomas & Transcripts – Universities issue digitally signed certificates.
Student Enrollment Verification – Securely verifies student records.
Online Learning Certificates – Platforms like Coursera and Udemy use digital signatures for course completion certificates.

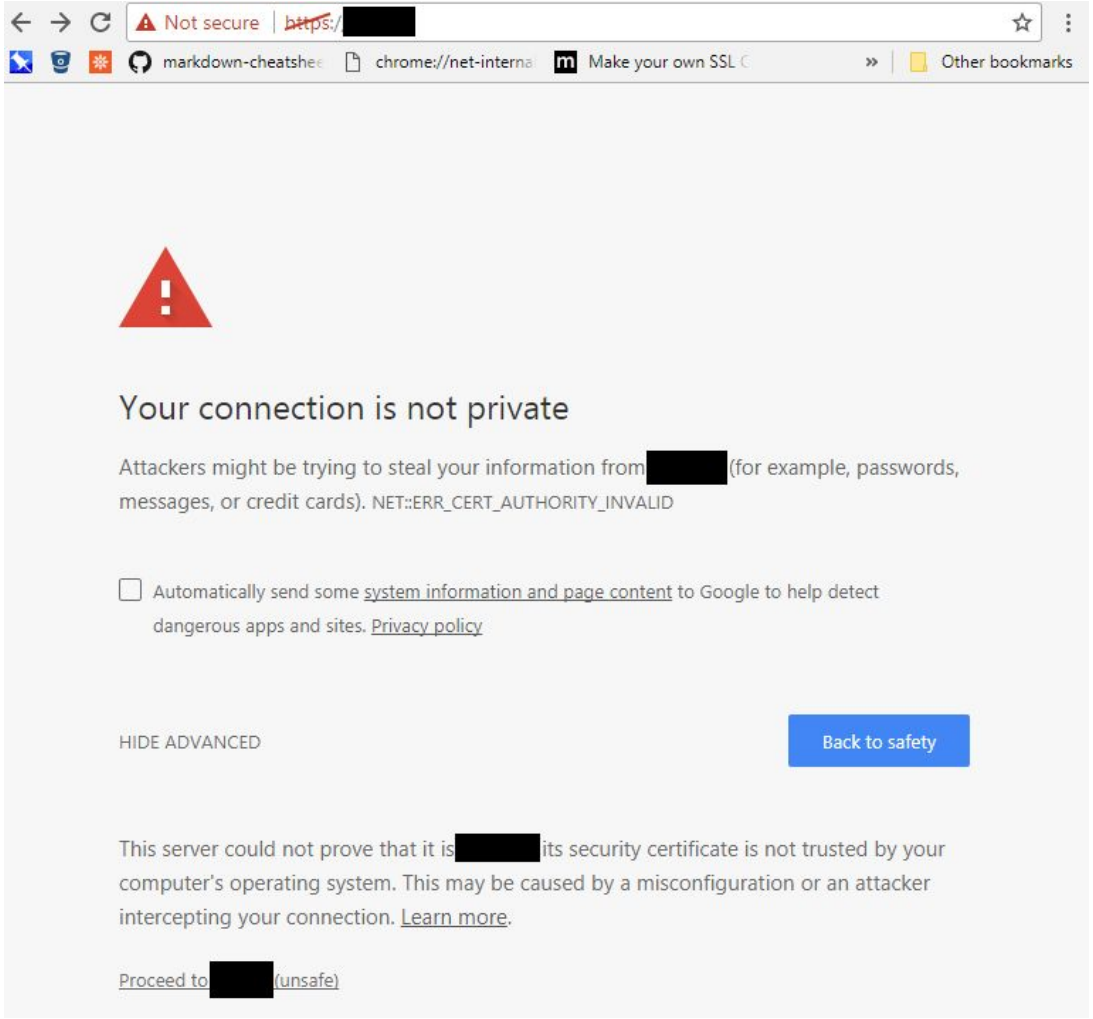
Conclusion

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

Certificates

A **certificate** is like a **website’s ID card** that proves its identity and ensures secure communication. It is issued by a trusted organization (Certificate Authority, CA) and helps protect users from fake or dangerous websites.

Certificate Authority (CA)	Description
Let's Encrypt (free)	A free, automated CA used by millions of websites.
DigiCert	One of the most popular commercial CAs.
GlobalSign	Provides SSL certificates for enterprises.
Sectigo (formerly Comodo)	A major provider of website security.
Google Trust Services	Google's own CA for securing Google services.



The website **does not use HTTPS** (only HTTP, which is not secure).
The certificate is **expired or untrusted**.
The website could be **a fake or phishing site**.

Key Technologies Behind Certificates

Public Key Infrastructure (PKI)

Asymmetric Encryption
(Public-Key Cryptography)

X.509 Certificate Standard

📜 **X.509** is the **international standard** for digital certificates.

Thanks