

# CS458: Introduction to Information Security

## Notes 5: Digital Signatures

Yousef M. Elmehdwi

Department of Computer Science

Illinois Institute of Technology

[yelmehdwi@iit.edu](mailto:yelmehdwi@iit.edu)

February 21<sup>st</sup> 2024

Slides: Modified from [Christof Paar and Jan Pelzl](#) & Cryptography and Network by Behrouz Forouzan, the McGraw-Hill Companies

- Security services
- The principle of digital signatures
  - *The principles of digital signatures encompass verifying the sender's identity (authentication), ensuring the message's integrity (integrity), and preventing the sender from denying their involvement (non-repudiation). These principles collectively contribute to secure and trustworthy communication in digital transactions and exchanges.*
- The RSA digital signature scheme

# Attacks, Services and Mechanisms

- Security Attack

- Any action that compromises the security of information.

- Security Mechanisms

- A mechanism that is designed to detect, prevent, or recover from a security attack.
- A mechanism might operate by itself, or with others, to provide a particular service.
- Examples of common security mechanisms:
  - Cryptography, Message digests and digital signatures, Digital certificates, Public Key Infrastructure (PKI)

- Security Services

- Refer to the different services available for maintaining the security and safety of an organization
- Intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.
- They help in preventing any potential risks to security
- Implement security policies and are implemented by security mechanisms.

# Core Security Services

- The objectives of security system are called security services.
  1. **Confidentiality**: Information is kept secret from all but authorized parties
  2. **Message/Data Integrity**: Ensures that a message has not been modified in transit.
  3. **Message/Data Origin Authentication**: Ensures that the sender of a message is authentic.
  4. **Non-repudiation**: Ensures that the sender of a message can not deny the creation of the message. (e.g., order of a pink car)
- **Confidentiality** is provided by using primarily symmetric ciphers and less frequently asymmetric encryption.
- **Integrity** and **message authentication** are provided by digital signatures and message authentication codes.
- **Non-repudiation** can be achieved with digital signatures.

# Additional Security Services

5. Identification/Peer entity authentication:
  - Establishing and verifying the identity of an entity, such as a person or a computer.
  - *who are you?*
6. Access control/Authorization:
  - Restricting access to resources to privileged entities.
  - *Deciding who can do what.*
7. Auditing:
  - Provides evidences of security-relevant activities
  - Keeping logs of certain events.
  - *Providing a proof of who did what*
8. Availability:
  - Ensuring the system is accessible and usable on demand by authorized users according to the intended goal.
9. Physical security:
  - Providing protection against physical tampering.
  - Responding to physical tampering attempts.
10. Anonymity/privacy:
  - Providing protection against the discovery and misuse of identity.
  - Addressing the question of *what happens when we do not want to be identified.*

# Introduction to Digital Signatures

- Goal:
  - Signature-like function for the electronic world that mimic the conventional (paper) signature
- Conventional (paper) Signature
  - In the physical world, it is common to use handwritten signatures on handwritten or typed messages.
  - They are used to bind signatory to the message.
- Digital Signatures
  - Similarly, a digital signature is a technique that binds a person/entity to the digital data.
  - This binding can be independently verified by receiver as well as any third party.
- *Digital signatures are cryptographic tools serve as the electronic equivalent of handwritten signatures and provide the same level of authentication, integrity, and non-repudiation in electronic transactions and communications.*

# Motivation

- Consider the real-life example where a person pays by credit card and signs a bill; the seller verifies that the signature on the bill is the same with the signature on the card.
  - *the signature on the bill serves as evidence that the person authorized the transaction and cannot later deny their involvement*
- Contracts are valid if they are signed.
  - *handwritten signatures serve as evidence of a party's intent to be bound by the terms of the agreement*
- Signatures provide non-repudiation.
  - ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract.
- *Can we have a similar service in the electronic world?*

# Motivation

- *Why not use symmetric cryptography?*
- A setting in which symmetric cryptography fails to provide a desirable security function:
- Odd Colors for Cars
  - **Bob** orders a pink car from the car dealer **Alice**
  - After seeing the pink car, **Bob** states that he has never ordered it
  - How can **Alice** prove towards a judge that **Bob** has ordered a pink car?  
(And that she did not fabricate the order herself)
    - Symmetric cryptography fails because both **Alice** and **Bob** can be malicious
    - Can be achieved with public-key cryptography



# Comparison

- Conventional signatures and digital signatures are two methods of authenticating documents or messages, but they differ in several key ways.
- Let us begin by looking at the differences between conventional signatures and digital signatures.
  - Inclusion
  - Verification Method
  - Relationship
  - Duplicity

# Comparison: Inclusion

- A conventional signature is included in the document; it is part of the document.
  - include message and signature in the same document.
- But when we sign a document digitally, we send the signature as a separate document.
  - i.e., digital signature: the signature will be attached to the document, is not a part of the document
- *Conventional signatures are physically included on a document or message, whereas digital signatures are added as a digital code that is embedded in the document or message.*

# Comparison: Verification Method

- For a conventional signature, when the recipient receives a document, she compares the signature on the document with the signature on file.
- For a digital signature
  - The recipient receives the message and the signature.
  - The recipient needs to apply a verification technique to the combination of the message and the signature to verify the authenticity.
- *Conventional signatures are typically verified by examining the physical signature and comparing it to a known sample, while digital signatures are verified by using a mathematical algorithm that checks the signature against the original document or message.*

# Comparison: Relationship

- Compare based on the relationship between the signature and the documents.
- For a conventional signature, there is normally a one-to-many relationship between a signature and documents.
  - i.e., all documents would have the same signature if it signed by the same person/entity
- For a digital signature, there is a one-to-one relationship between a signature and a message.
  - if we modify even one bit, we will have a different signature for this message.

# Comparison: Duplicity

- In conventional signature, a copy of the signed document can be indeed distinguished from the original based on physical characteristics such as ink, paper, or other unique features.
  - *These physical attributes can help determine the authenticity of the signature.*
- Unlike conventional signatures, digital signatures do not rely on physical characteristics. Instead, they utilize advanced encryption technology to provide integrity, authenticity, and non-repudiation of digital documents.
- In general, digital signatures are considered to be more difficult to duplicate or tamper with than conventional signatures due to the advanced encryption technology used.
- *Conventional signatures can be easily duplicated or forged, while digital signatures are very difficult to forge or tamper with due to the complex encryption technology used.*

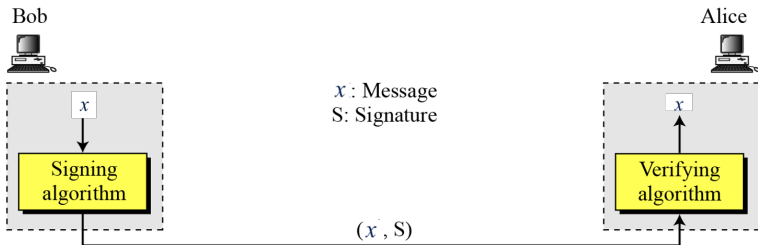
# Digital Signatures

- Aim of a signature
  - Prove to anyone that a message originated at (or is approved by) a particular user
- Symmetric key cryptography
  - Two users, **Alice** and **Bob**, share a secret key **K**
  - Receiver of message (user **Alice**) can verify that message came from the other user (**Bob**)
  - User **C** cannot prove that the message came from **Bob** (it may also have came from **Alice**)
- Public key cryptography can provide signature
  - Only one user has the private key

# Digital signature process

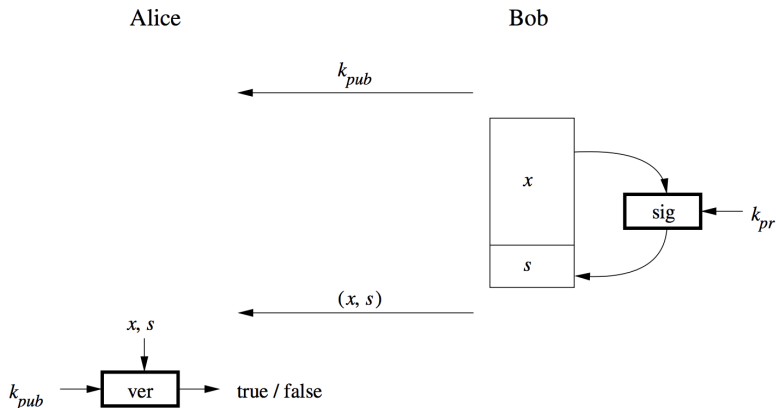
- The sender uses a **signing algorithm** to sign the message.
- The message and the signature are sent to the receiver.
- The receiver receives the message and the signature and applies the **verifying algorithm** to the combination.
  - If the result is true, the message is accepted;
  - otherwise, it is rejected.

# Digital signature process





# Basic Protocol for Digital Signature



- A digital signature needs a public-key system.
- The *signer* signs with their private key; the *verifier* verifies with the signer's public key.
  - *The person who signs the message uses a private key, and the receiving party uses the matching public key.*

# Main Idea

- For a given message  $x$ , a digital signature is appended to the message.
- Only the person with the private key should be able to generate the signature.
- The signature must change for every document.
- The **signature** is realized as a function with the message  $x$  and the private key as input.
- The public key, signature  $s$ , and the message  $x$  are the inputs to the **verification function**.

# Digital Signature Operations (Concept)

- Signing

- Bob signs a message by encrypting with own private key
  - $s = E_{k_{pr,B}}(x)$
- Bob attaches signature to message

- Verification

- Alice verifies a message by decrypting signature with signer's (Bob) public key
  - $x' = D_{k_{pub,B}}(s)$
- Alice then
  - compares received message  $x$  with decrypted  $x'$
  - if identical, signature is verified
  - otherwise, rejected

- We discussed several security services including message confidentiality, message authentication, message integrity, and nonrepudiation.
- A digital signature can directly provide the last three; for message confidentiality we still need encryption/decryption.

# Message Authentication

- A secure digital signature scheme, like a secure conventional signature can provide message authentication.
- *When the verifier validates the digital signature using the public key of the sender, they are assured that the signature has been created only by the sender who possesses the corresponding secret private key and no one else.*

# Message Integrity

- When a digital signature is applied to a message, any modifications made to the message after the signature has been created will result in a different signature.
- This ensures that the integrity of the message can be verified.
- *In case an attacker has access to the data and modifies it, the digital signature verification at the receiver end fails. The digital signature of modified data and the output provided by the verification algorithm will not match.*
  - ⇒ The receiver can safely deny the message assuming that data integrity has been breached*

# Nonrepudiation

- Nonrepudiation is the assurance that someone cannot deny something.
- Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
- Alice can take  $x$ , and signature  $s$  to court and prove that Bob signed  $x$
- *Since it is assumed that only the signer has the knowledge of the signature key, he can only create a unique signature on a given data*  
 *$\Rightarrow$  The receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future*

- A digital signature does not provide data confidentiality.
- If there is a need for confidentiality, another layer of encryption/decryption must be applied.



- Several digital signature schemes have evolved during the last few decades.
  - RSA Digital Signature Scheme
  - ElGamal Digital Signature Scheme
  - Schnorr Digital Signature Scheme
  - Digital Signature Standard (DSS)
  - Elliptic Curve Digital Signature Scheme

# Main idea of the RSA signature scheme

- To generate the private and public key
  - Use the same key generation as RSA encryption.
- To generate the signature
  - “**encrypt**” the message  $x$  with the private key.  
 $s = \text{sig}_{K_{pr}}(x) \equiv x^d \bmod n$
  - Append  $s$  to message  $x$
- To verify the signature
  - “**decrypt**” the signature with the public key
  - $\text{ver}_{K_{pub}}(x, s)$ 
    - $x' \equiv s^e \bmod n$
    - If  $x \equiv x'$ , the signature is valid
    - If  $x \not\equiv x'$ , the signature is invalid

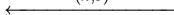
# The RSA signature Protocol

**Alice**

**Bob**

$$k_{pr} = d, k_{pub} = (n, e)$$

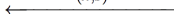
$(n, e)$



compute signature:

$$s = \text{sig}_{k_{pr}}(x) \equiv x^d \pmod n$$

$(x, s)$



verify:  $\text{ver}_{k_{pub}}(x, s)$

$$x' \equiv s^e \pmod n$$

$$x' \begin{cases} \equiv x \pmod n & \implies \text{valid signature} \\ \not\equiv x \pmod n & \implies \text{invalid signature} \end{cases}$$

- Alice can conclude from the valid signature that Bob generated the message and that it was not altered in transit
  - message authentication, non-repudiation and message integrity are given.
- If confidentiality is required, the message  $x$  and signature  $s$  can be encrypted, e.g., using AES.
- *Signature verification is very efficient as a small number can be chosen for the public key.*

# The RSA signature Protocol: Example

**Alice**

**Bob**

1. choose  $p = 3$  and  $q = 11$
2.  $n = p \cdot q = 33$
3.  $\Phi(n) = (3 - 1)(11 - 1) = 20$
4. choose  $e = 3$
5.  $d \equiv e^{-1} \equiv 7 \pmod{20}$

←  $(n,e)=(33,3)$

compute signature for message

$x = 4$ :

$$s = x^d \equiv 4^7 \equiv 16 \pmod{33}$$

←  $(x,s)=(4,16)$

verify:

$$x' = s^e \equiv 16^3 \equiv 4 \pmod{33}$$

$x' \equiv x \pmod{33} \implies$  valid signature

# Existential Forgery Attack

- **Existential forgery** is a type of attack that can occur with digital signatures
- It involves an attacker creating a message that has the same digital signature as a legitimate message, without having access to the private key used to create the signature.
- *Essentially, the attacker is able to create a fake message that appears to be signed by a legitimate source, but is not actually authorized or authenticated.*
- This type of attack can occur when there are weaknesses in the digital signature algorithm or implementation, or when the private key used to create the signature is compromised.

# Existential Forgery Attack Against RSA Digital Signature

- Attacker generates a valid signature for a random message  $x$ .

**Alice**

**Eve**

**Bob**

$$k_{pr} = d$$
$$k_{pub} = (n, e)$$

$$\xleftarrow{(n, e)}$$

$$\xleftarrow{(n, e)}$$

1. choose signature:

$$s \in \mathbb{Z}_n$$

2. compute message:

$$x \equiv s^e \pmod{n}$$

$$\xleftarrow{(x, s)}$$

verification:

$$s^e \equiv x' \pmod{n}$$

since  $x' = x$

$\implies$  valid signature!

# Existential Forgery and Padding

- An attacker can generate valid message-signature pairs  $(x, s)$
- Limitations of this attack
  - Attacker can not directly control the semantics of the message  $x$ 
    - But attacker can only choose signature  $s$  and NOT the message  $x$
    - Attacker cannot generate messages like “Transfer \$1000 into Oscar’s account”
- The fact that an automated verification process does not recognize the forgery is certainly not a desirable feature

# Existential Forgery and Padding

- The fact that an automated verification process does not recognize the forgery is certainly not a desirable feature
- For this reason, schoolbook RSA signature is rarely used in practice, and padding schemes are applied in order to prevent this and other attacks
- **Padding**
  - Technique used in digital signature algorithms to add additional bits to a message before it is signed.
  - This helps to prevent attacks that rely on known plaintext or message length, and makes it more difficult for an attacker to guess the private key used to create the signature.
    - Formatting the message  $x$  according to a padding scheme can be used to make sure that an attacker cannot generate valid  $(x, s)$  pairs.
    - A messages  $x$  generated by an attacker during an Existential Forgery Attack will not coincide with the padding scheme.



# Lessons Learned

- Digital signatures provide message integrity, message authentication and nonrepudiation.
- RSA is currently the most widely used digital signature algorithm.
- Competitors are the Digital Signature Standard (DSA) and the Elliptic Curve Digital Signature Standard (ECDSA).
- RSA verification can be done with short public keys  $e$ . Hence, in practice, RSA verification is usually faster than signing.
- In order to prevent certain attacks, RSA should be used with padding. The modulus of the RSA signature schemes should be at least *2048-bits* long.

- Understanding Cryptography: A Textbook for Students and Practitioners - *available online*
  - Chapter 10: Digital Signatures