# DIGITAL SIGNATURES

PRESENTED BY
:S.K.D

# Why Digital Signatures?

- To provide Authenticity, Integrity and Non - repudiation to electronic documents
- To use the Internet as the safe and secure medium for e-Governance and e-Commerce

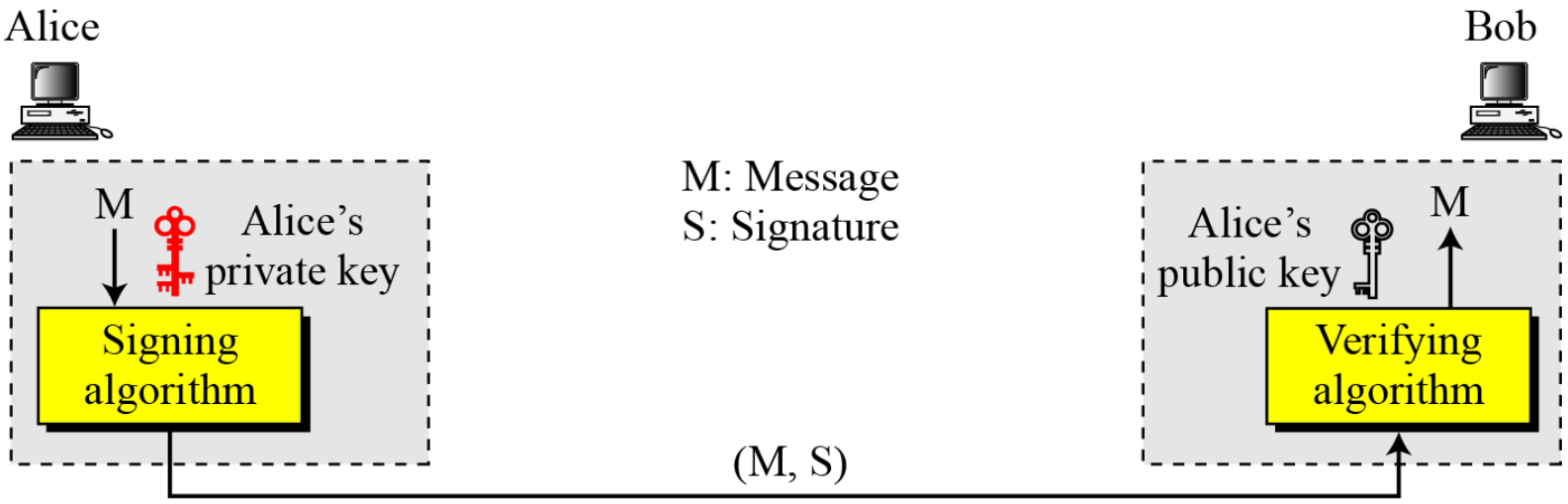
# What is Digital Signature?

- Mathematical scheme for demonstrating the authenticity
- Easily transportable
- Signing key
- Verification key
- Asymmetric cryptography

# The Scheme typically consists of three Algorithms

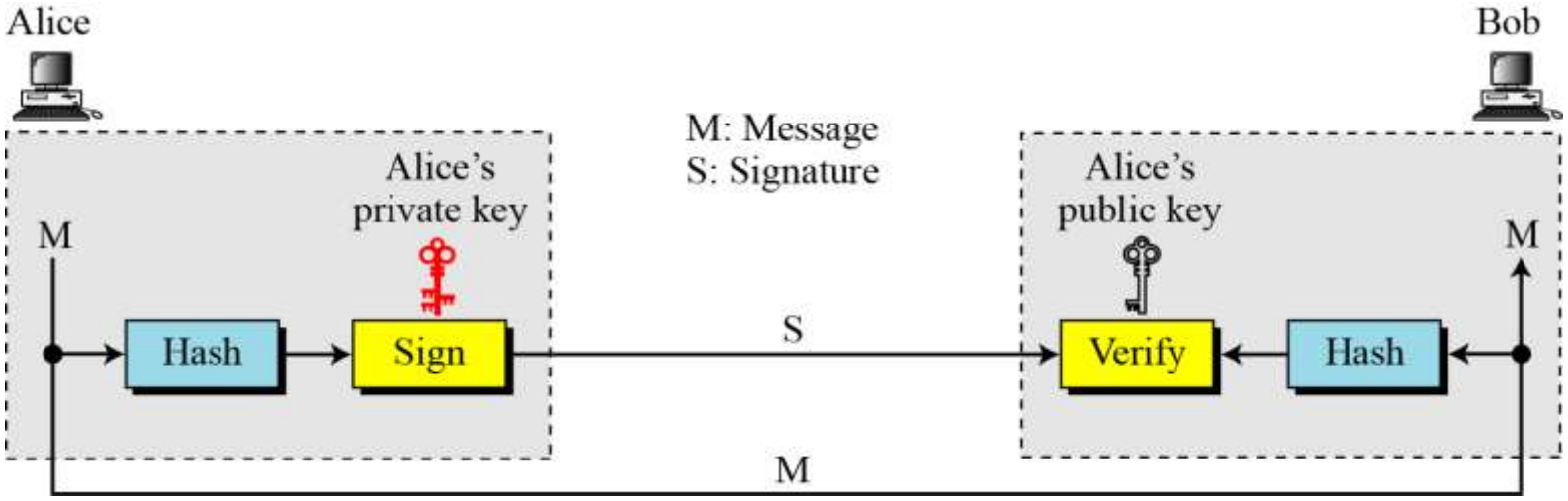
- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A signing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity

# Digital signature process



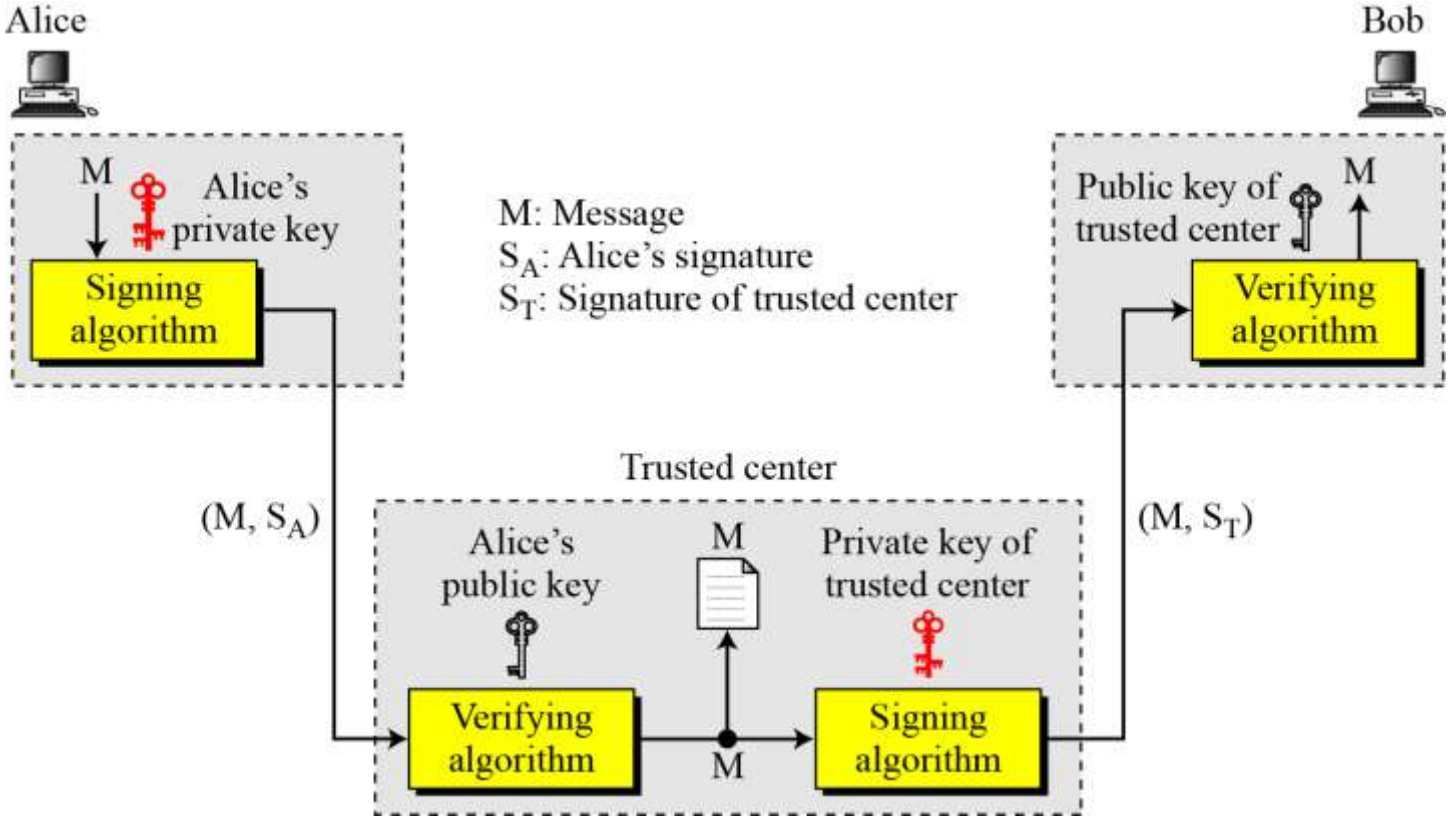
# Signing the digest

- For efficiency
- For compatibility
- For integrity



# Services

- Authentication
- Integrity
- Non-repudiation



# Attacks on digital signature

## Key-Only Attack

the attacker is only given the public verification key

## Known-Message Attack

the attacker is given valid signatures for a variety of messages known by the attacker but not chosen by the attacker.

## Chosen-Message Attack

the attacker first learns signatures on arbitrary messages of the attacker's choice.

# Forgery types

## Existential forgery

Existential forgery is the creation (by an adversary) of any message/signature pair (m,σ), where σ was not produced by the legitimate signer.

## Selective forgery

Selective forgery is the creation (by an adversary) of a message/signature pair (*m*,σ) where *m* has been *chosen* by the adversary prior to the attack.

# Hardware Tokens

iKey


Smart Card