SOS POLITICAL SCIENCE AND PUBLIC ADMINISTRATION
JIWAJI UNIVERSITY, GWALIOR

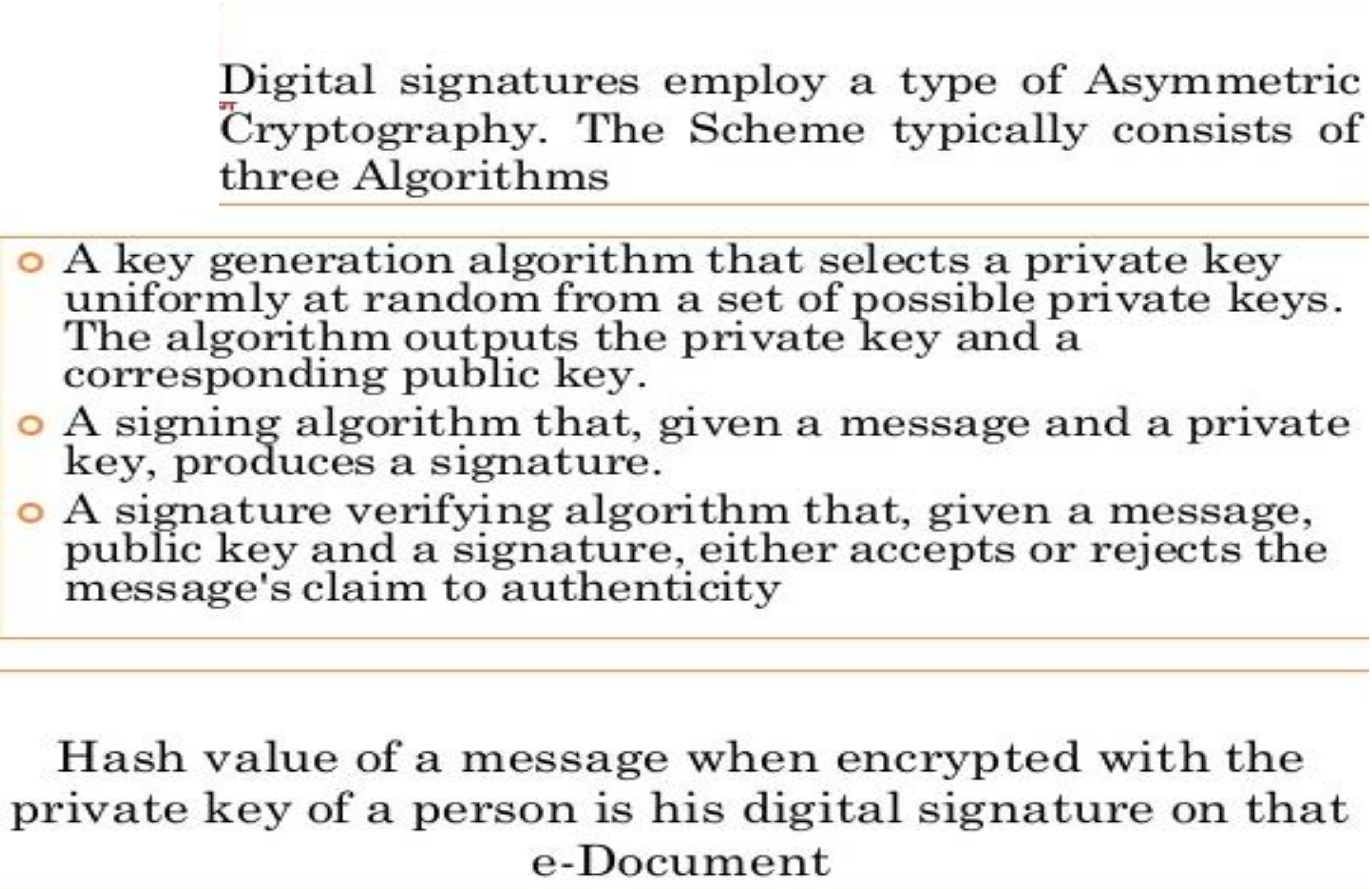
MBA FA IV SEM
PAPER- FA 402
SUBJECT NAME: E-BUSINESS AND CYBER LAW

TOPIC NAME: DIGITAL SIGNATURE

Digital Signature

WHAT IS DIGITAL SIGNATURE?

- A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.
- Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender can not easily repudiate it later.
- The originator of a message uses a signing key (Private Key) to sign the message and send the message and its digital signature to a recipient
- The recipient uses a verification key (Public Key) to verify the origin of the message and that it has not been tampered with while in transit



Digital signatures employ a type of 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

Hash value of a message when encrypted with the private key of a person is his digital signature on that e-Document

What is a digital signature?

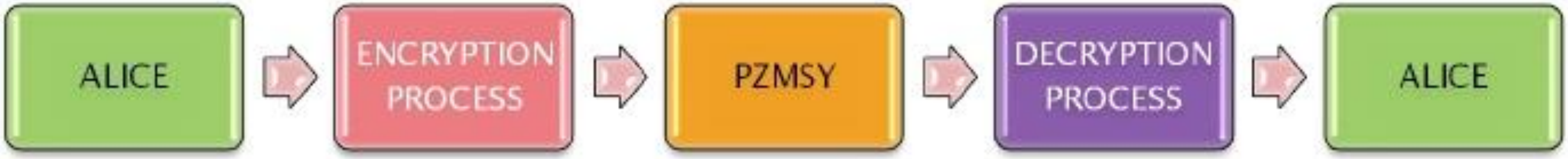
•is a type of **asymmetric cryptography** used to simulate the security properties of a **signature** in digital, rather than written, form. Digital signature schemes normally give two algorithms, one for signing which involves the user's secret or **private key**, and one for verifying signatures which involves the user's **public key**. The output of the signature process is called the "digital signature.“

•is an **electronic signature** that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

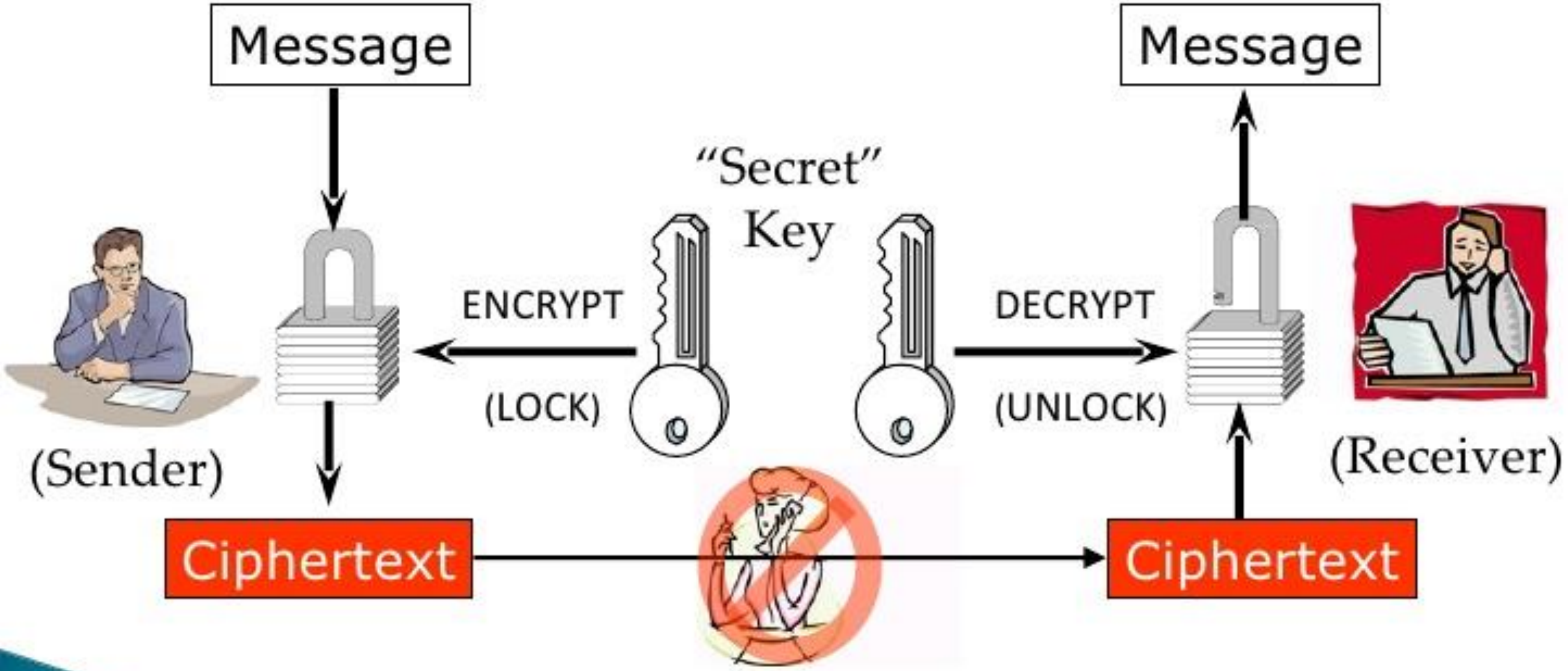
How it works

- The use of digital signatures usually involves two processes, one performed by the signer and the other by the receiver of the digital signature:
- **Digital signature creation** uses a hash result derived from and unique to both the signed message and a given private key. For the hash result to be secure, there must be only a negligible possibility that the same digital signature could be created by the combination of any other message or private key.
- **Digital signature verification** is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.

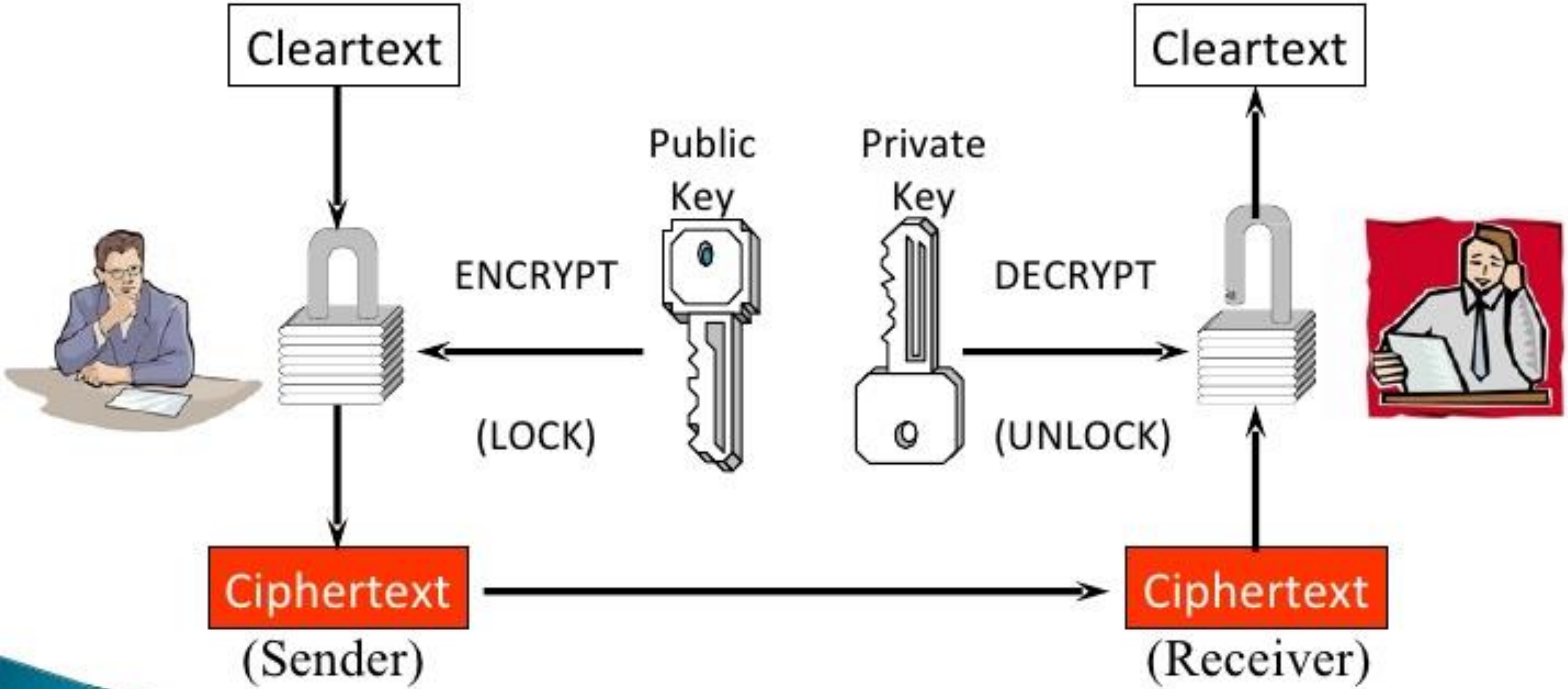
CRYPTOGRAPHY



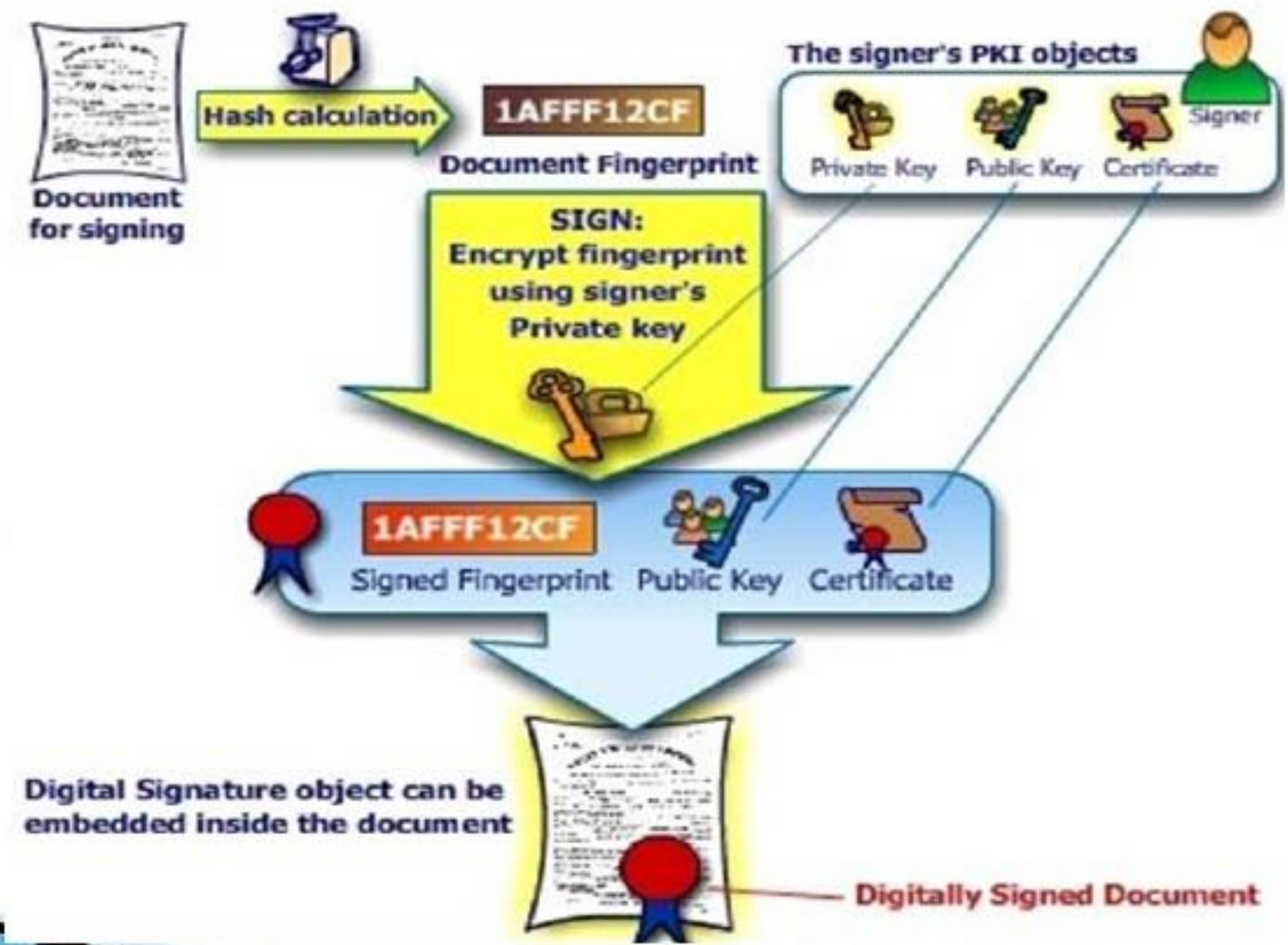
SYMMETRIC KEY CRYPTOGRAPHY



ASYMMETRIC KEY CRYPTOGRAPHY



DIGITAL SIGNATURE



Digital Signatures

Each individual generates his own key pair

[Public key known to everyone
&
Private key only to the owner]

Private Key – Used for making Digital Signature

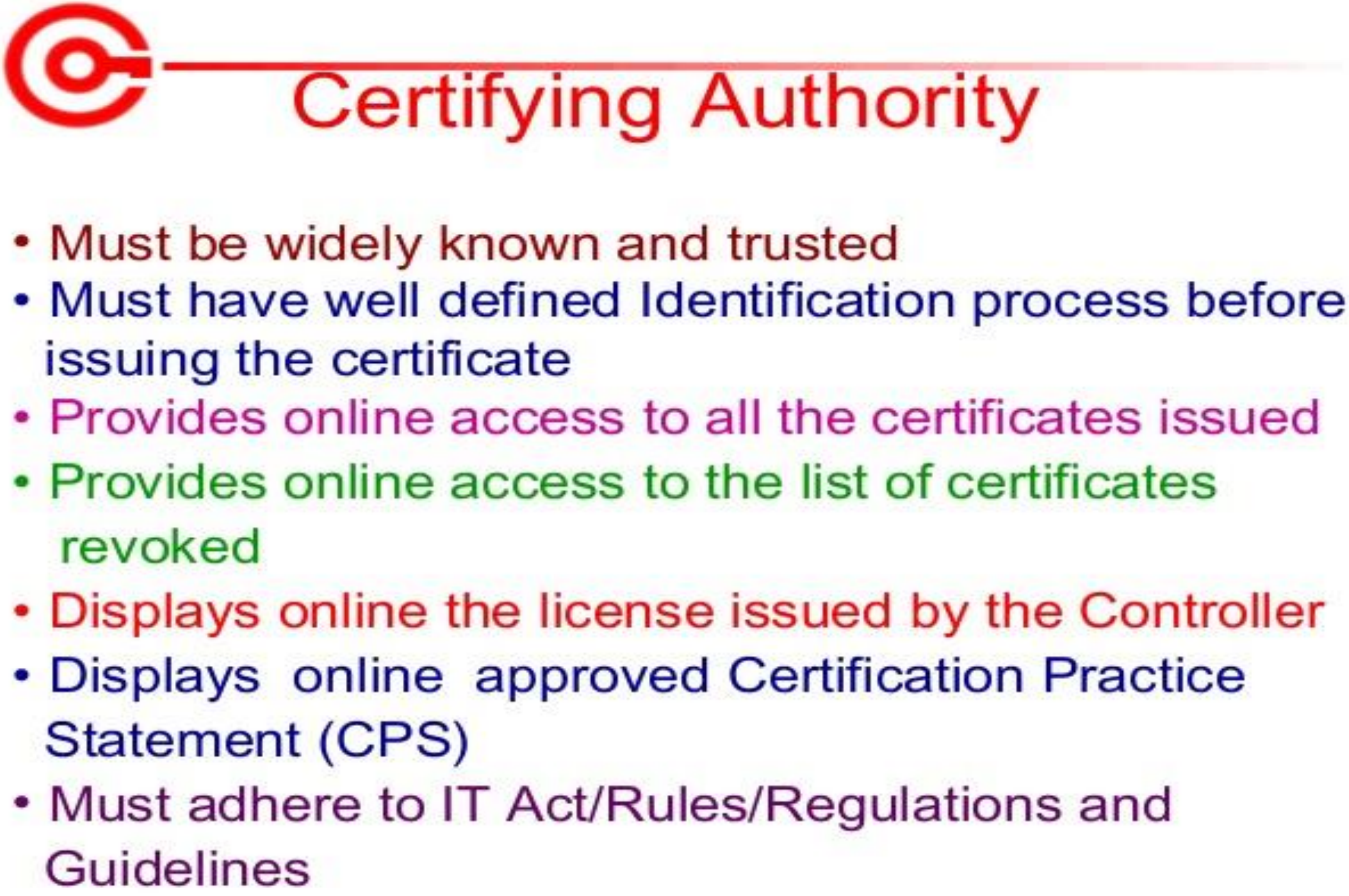
Public Key – Used to verify the Digital Signature

DIGITAL CERTIFICATE

- Digital Identity that establishes your credentials when doing business or other transactions on the Web
- Issued by a Certifying Authority (CA)
- Contains your name, serial number, expiration dates, public key, signature of CA

CERTIFYING AUTHORITY

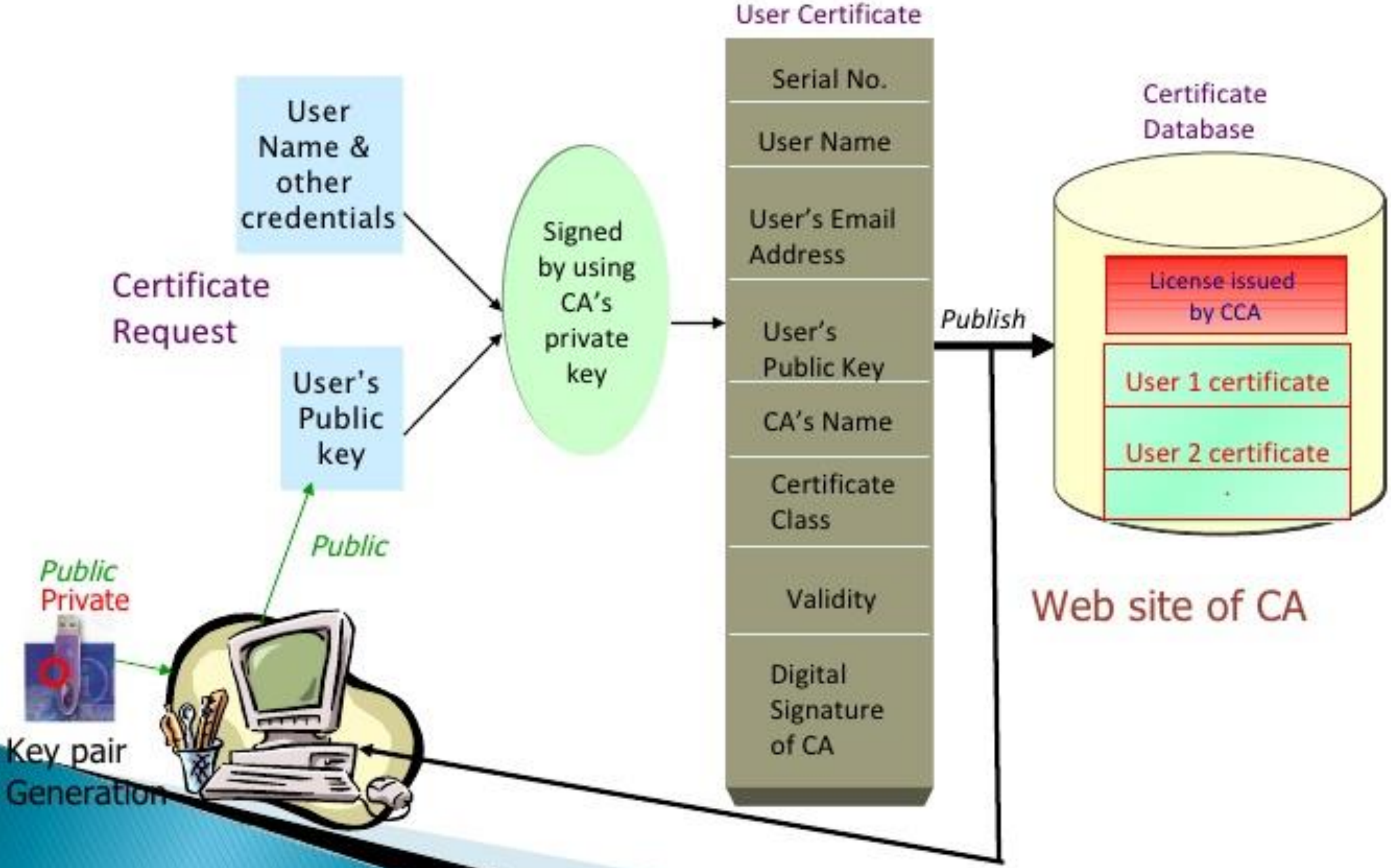
- Trusted Third Party
- An organization which issues public key certificates
- Assures the identity of the parties to whom it issues certificates
- Maintains online access to the public key certificates issued



Certifying Authority

- Must be widely known and trusted
- Must have well defined Identification process before issuing the certificate
- Provides online access to all the certificates issued
- Provides online access to the list of certificates revoked
- Displays online the license issued by the Controller
- Displays online approved Certification Practice Statement (CPS)
- Must adhere to IT Act/Rules/Regulations and Guidelines

PUBLIC KEY CERTIFICATION



Certificate Request

User Name & other credentials

User's Public key

Public

Public
Private

Key pair Generation

Signed by using CA's private key

User Certificate

Serial No.

User Name

User's Email Address

User's Public Key

CA's Name

Certificate Class

Validity

Digital Signature of CA

Publish

Certificate Database

License issued by CCA

User 1 certificate

User 2 certificate

.

Web site of CA

Private key of CA or CCA require highest level of security

Hardware Security Module (HSM) is used for storing the Private Key

More than one person are required for signing

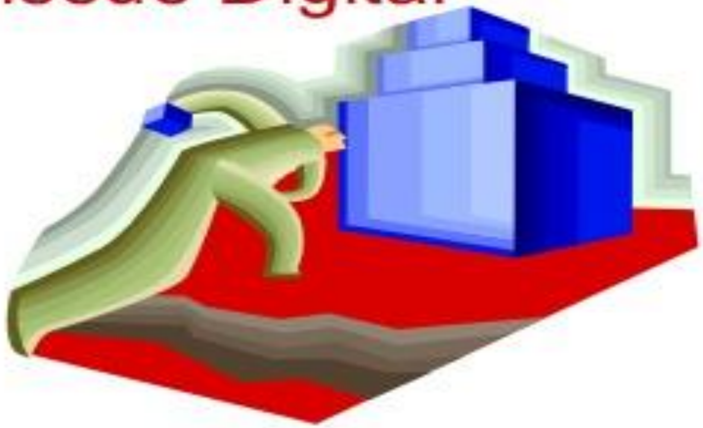
HSM is housed in a strong room with video surveillance on 24x7 basis.

Trust Path

- Controller is the Root certifying authority responsible for regulating Certifying Authorities (CAs)
- Controller certifies the association of CA with his public key
- Certifying Authority (CA) is the trusted authority responsible for creating or certifying identities.
- CA certifies the association of an individual with his public key

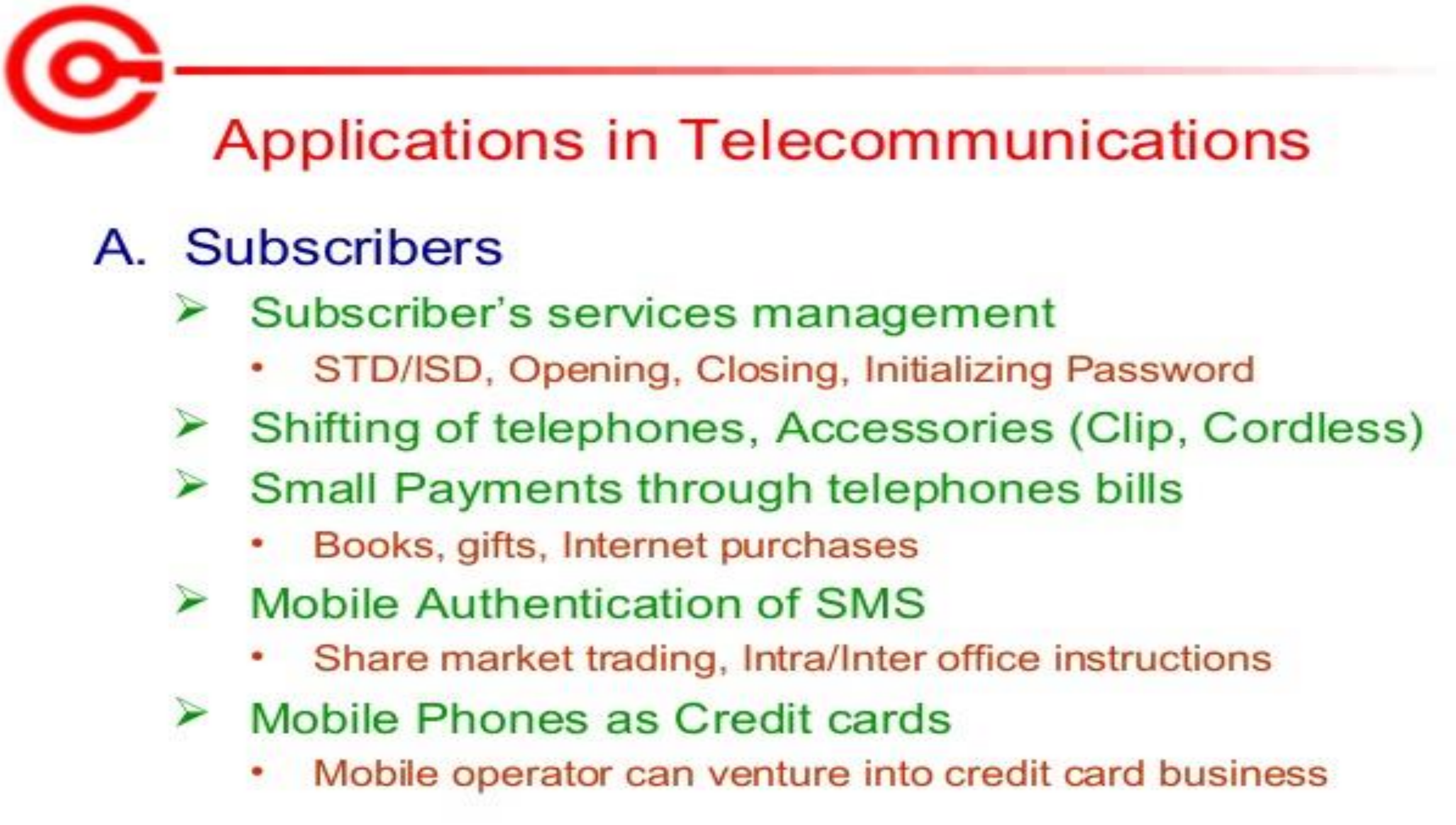
Role of controller

Controller of Certifying Authorities as the “Root” Authority certifies the technologies,infrastructure and practices of all the Certifying Authorities licensed to issue Digital Signature Certificates



Summary

- Each individual has a pair of keys
- Public key of each individual is certified by a CA (Certifying Authority)
- Public keys of CAs are certified by the Controller
- Public key of the Controller is self certified
- Public keys of everyone are known to all concerned and are also available on the web
- Certification Practice Statement is displayed on the web site



Applications in Telecommunications

A. Subscribers

- ➢ Subscriber’s services management
  - STD/ISD, Opening, Closing, Initializing Password
- ➢ Shifting of telephones, Accessories (Clip, Cordless)
- ➢ Small Payments through telephones bills
  - Books, gifts, Internet purchases
- ➢ Mobile Authentication of SMS
  - Share market trading, Intra/Inter office instructions
- ➢ Mobile Phones as Credit cards
  - Mobile operator can venture into credit card business

Applications in Telecommunications

(contd.)

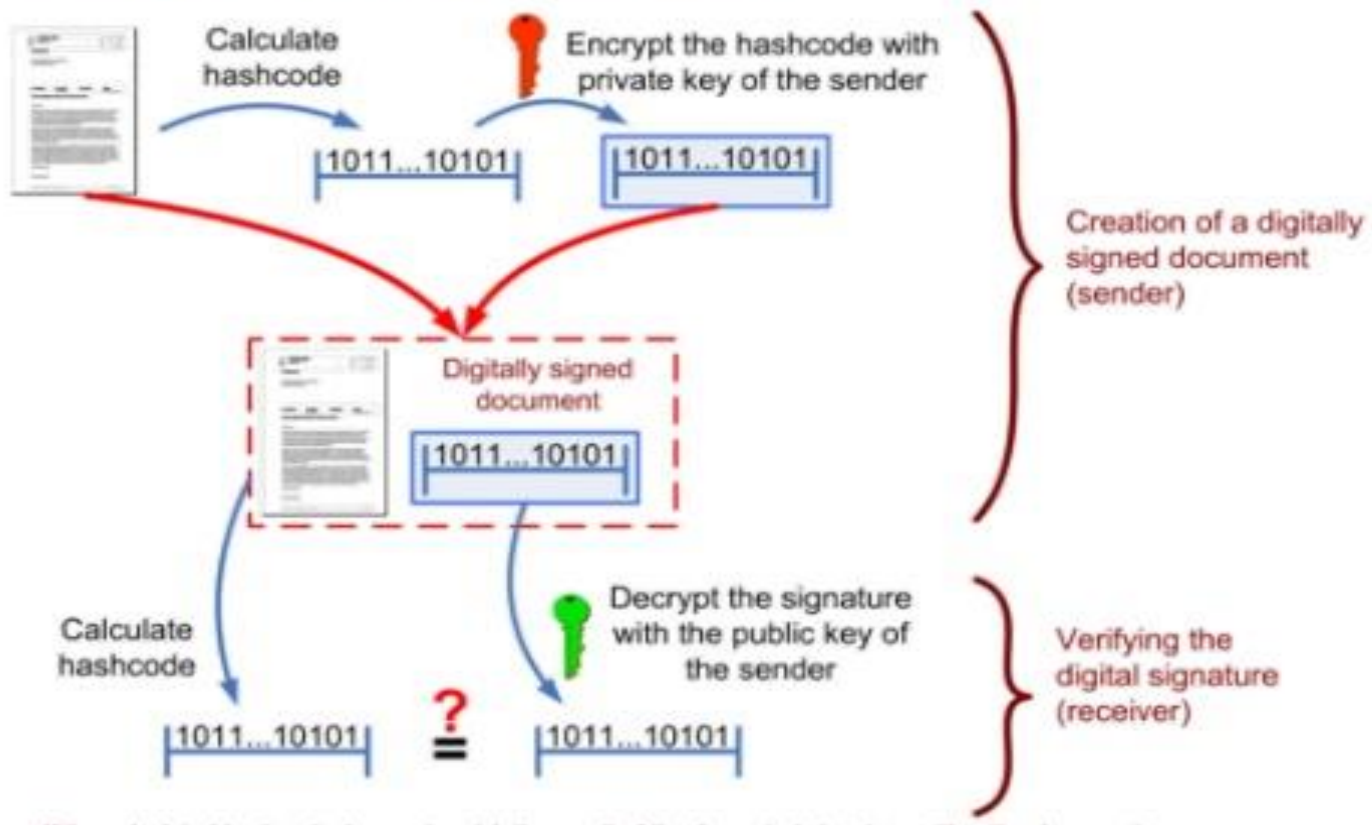
B. Internal

- ➢ Intra/Inter offices authentic communications
  - OBs, approvals, Instructions, requests
- ➢ Procurement of material
  - Calling/Receiving bids, Purchase orders, Payment instructions
- ➢ Network Management functions
  - Change of configuration, Blocking/unblocking routes

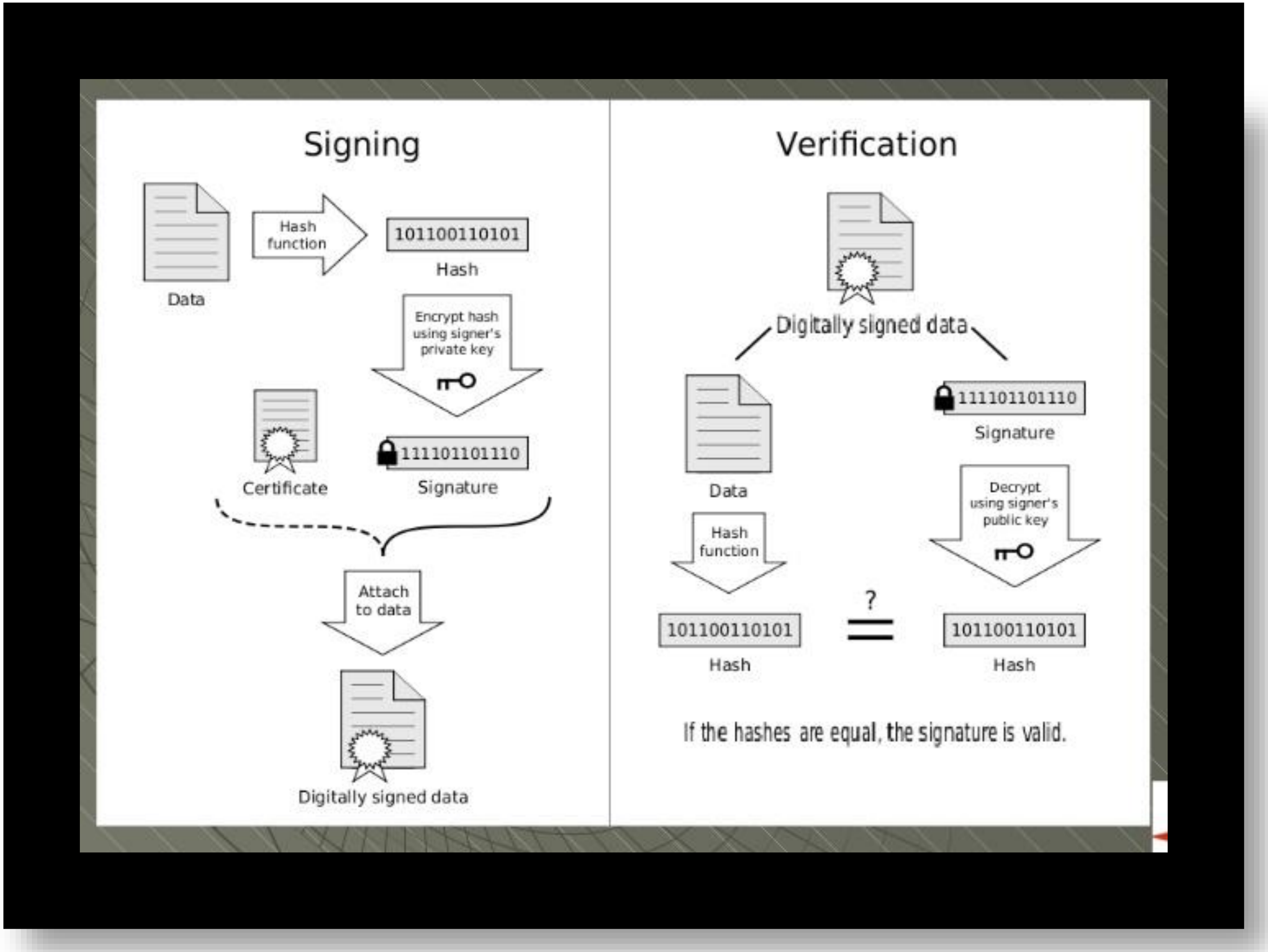
DIGITAL SIGNATURE STANDARDS

- Uses secure hash algorithm
- Condenses message to 160 bit
- Key size 512-1024 bits
- Proposed by NIST in 1991
- Adopted

Creating and verifying a digital signature


Calculate hashcode
1011...10101
Encrypt the hashcode with private key of the sender
1011...10101
Creation of a digitally signed document (sender)
Digitally signed document
1011...10101
Calculate hashcode
Decrypt the signature with the public key of the sender
1011...10101
?
=
1011...10101
Verifying the digital signature (receiver)

If the calculated hashcode does not match the result of the decrypted signature, either the document was changed after signing, or the signature was not generated with the private key of the alleged sender.



If the hashes are equal, the signature is valid.

PRIVATE KEY PROTECTION

Soft Token

Smart card

Hardware tokens

Hardware Tokens

- **They are similar to smart cards in functionality as**
  - **Key is generated inside the token.**
  - **Key is highly secured as it doesn't leave the token.**
  - **Highly portable.**
  - **Machine Independent.**

- **iKEY is one of the most commonly used token as it doesn't need a special reader and can be connected to the system using USB port.**

Smart Cards

- The Private key is generated in the crypto module residing in the smart card.
- The key is kept in the memory of the smart card.
- The key is highly secured as it doesn't leave the card, the message digest is sent inside the card for signing, and the signatures leave the card.
- The card gives mobility to the key and signing can be done on any system. (Having smart card reader)

Hardware Tokens

iKey

Smart Card

Biometrics – adds another level of security to these tokens

Public Key Infrastructure (PKI)

- Some Trusted Agency is required which certifies the association of an individual with the key pair.

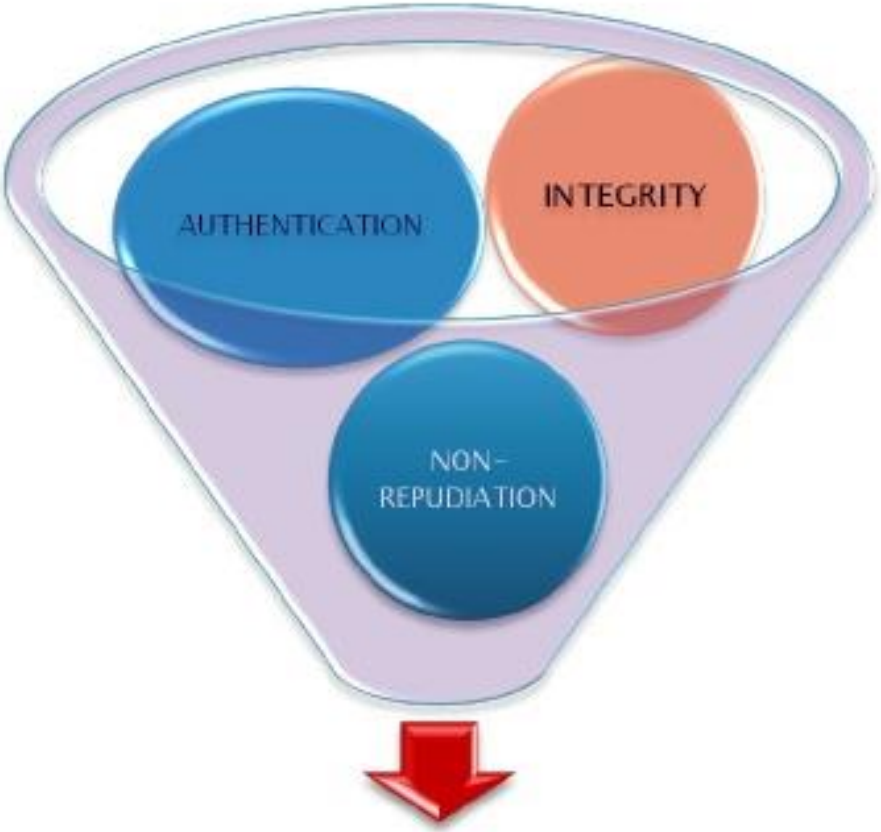
    Certifying Authority (CA)

- This association is done by issuing a certificate to the user by the CA

    Public key certificate (PKC)

- All public key certificates are digitally signed by the CA

WHY DIGITAL SIGNATURE



DIGITAL SIGNATURE

Why Digital Signatures?

- To provide Authenticity, Integrity and Non -repudiation to electronic documents

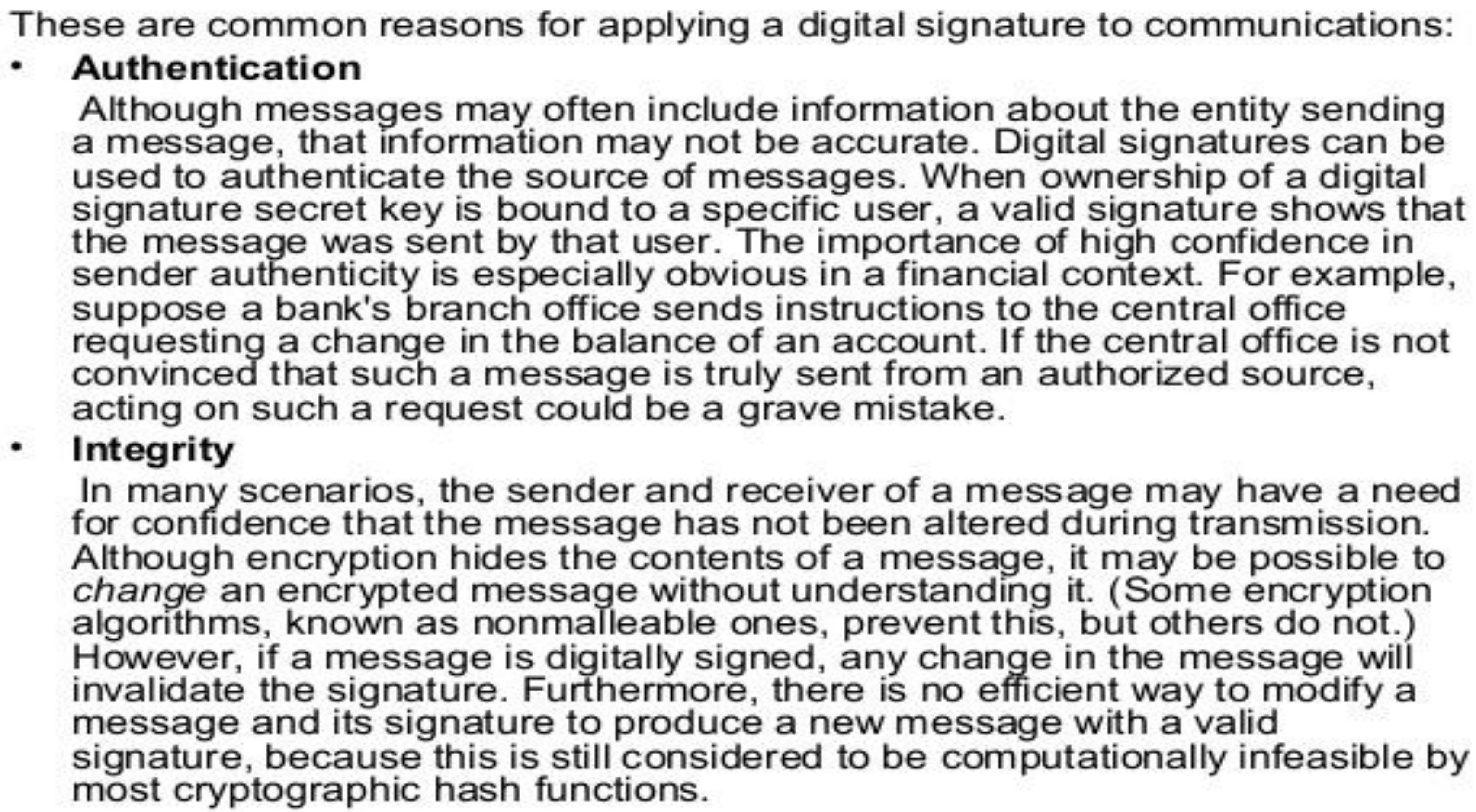
- To use the Internet as the safe and secure medium for e-Governance and e-Commerce

Paper signatures v/s Digital Signatures

V/s

Parameter	Paper	Electronic
Authenticity	May be forged	Can not be copied
Integrity	Signature independent of the document	Signature depends on the contents of the document
Non-repudiation	a. Handwriting expert needed b. Error prone	a. Any computer user b. Error free

Benefits of digital signatures



These are common reasons for applying a digital signature to communications:

- **Authentication**

  Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

- **Integrity**

  In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to *change* an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message will invalidate the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions.

Drawbacks of digital signatures

Despite their usefulness, digital signatures do not alone solve all the problems we might wish them to.

Non-repudiation

In a cryptographic context, the word *repudiation* refers to the act of disclaiming responsibility for a message. A message's recipient may insist the sender attach a signature in order to make later repudiation more difficult, since the recipient can show the signed message to a third party (eg, a court) to reinforce a claim as to its signatories and integrity. However, loss of control over a user's private key will mean that all digital signatures using that key, and so ostensibly 'from' that user, are suspect. Nonetheless, a user cannot repudiate a signed message without repudiating their signature key.

THANKYOU