Information Security

CS3002

Lecture 10

18th September 2024

Dr. Rana Asif Rehman

Email: r.asif@lhr.nu.edu.pk

DIGITAL SIGNATURE

Some Clarification

- Electronic Signatures vs. Digital Signatures:
  - An electronic signature is simply an image of your signature added to a document.
  - A digital signature is encrypted data that proves the document came from you.
    - For some purposes, a simple electronic signature will be fine, but for more important documents, a secure digital signature is highly recommended.

Digital Signature

- Operation is similar to that of the MAC.
- The hash value of a message is encrypted with a user's private key.
- Anyone who knows the user's public key can verify the integrity of the message.
- An attacker who wishes to alter the message would need to know the user's private key.
- Implications of digital signatures go beyond just message authentication.

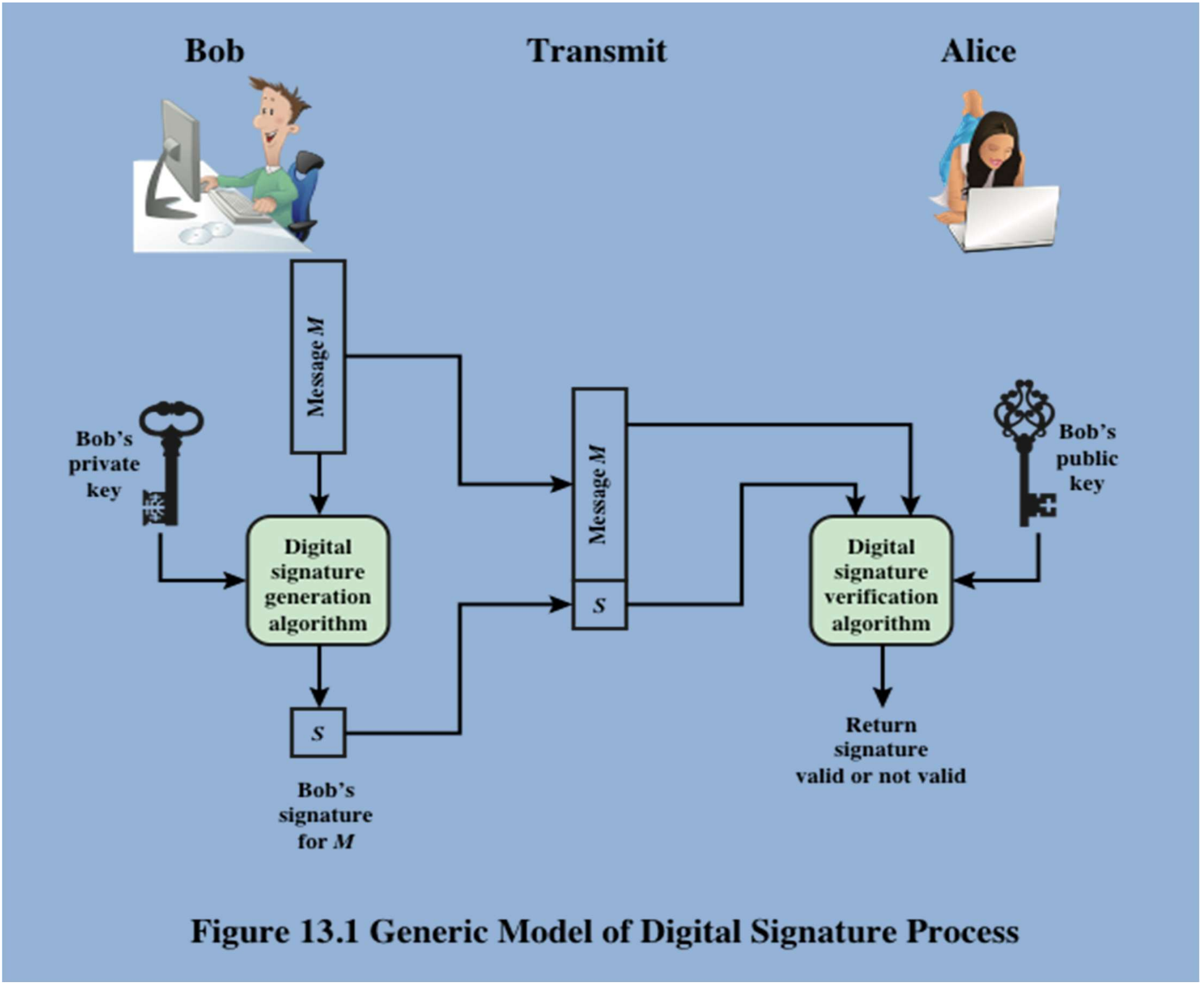


Figure 13.1 Generic Model of Digital Signature Process

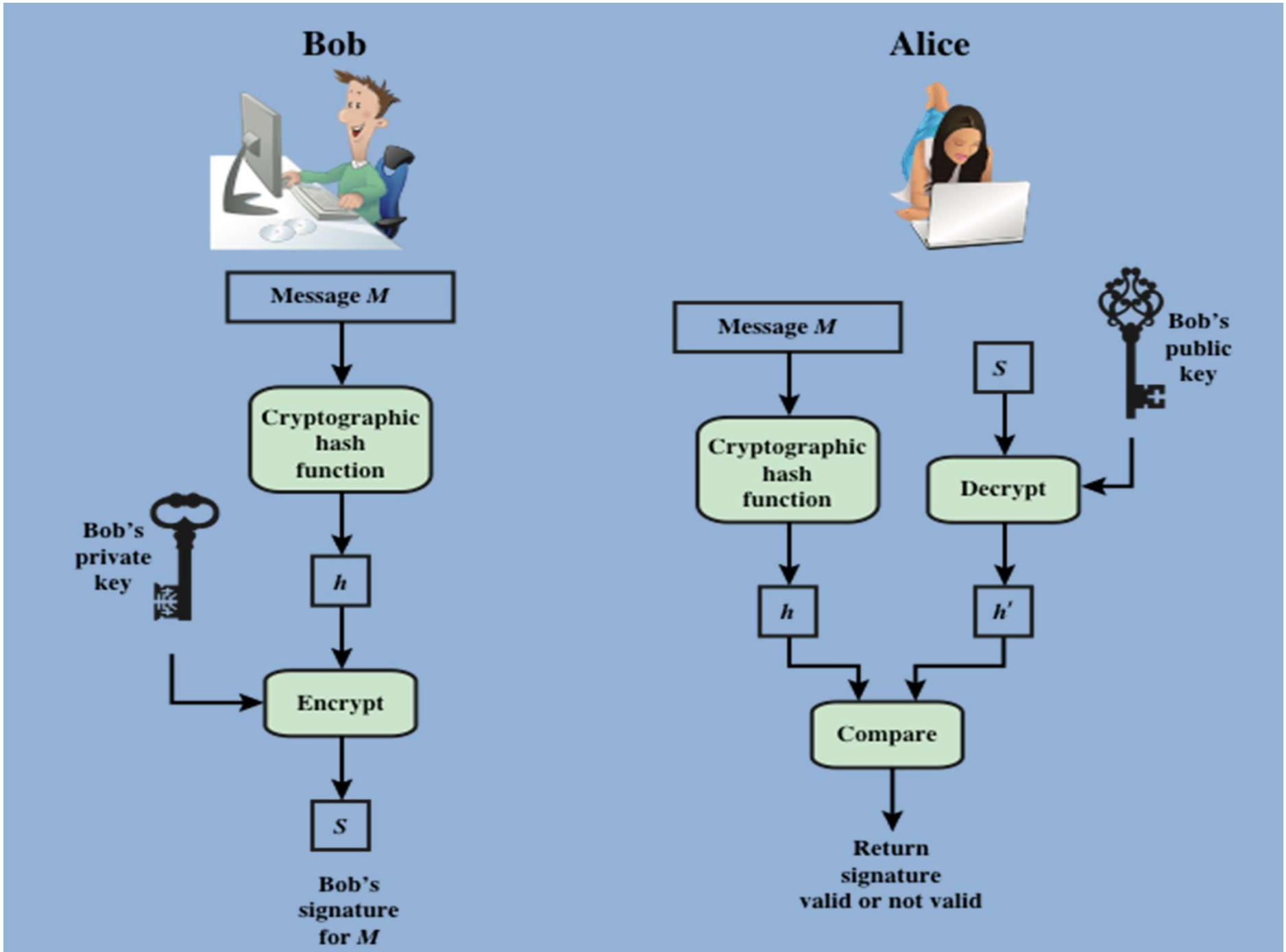
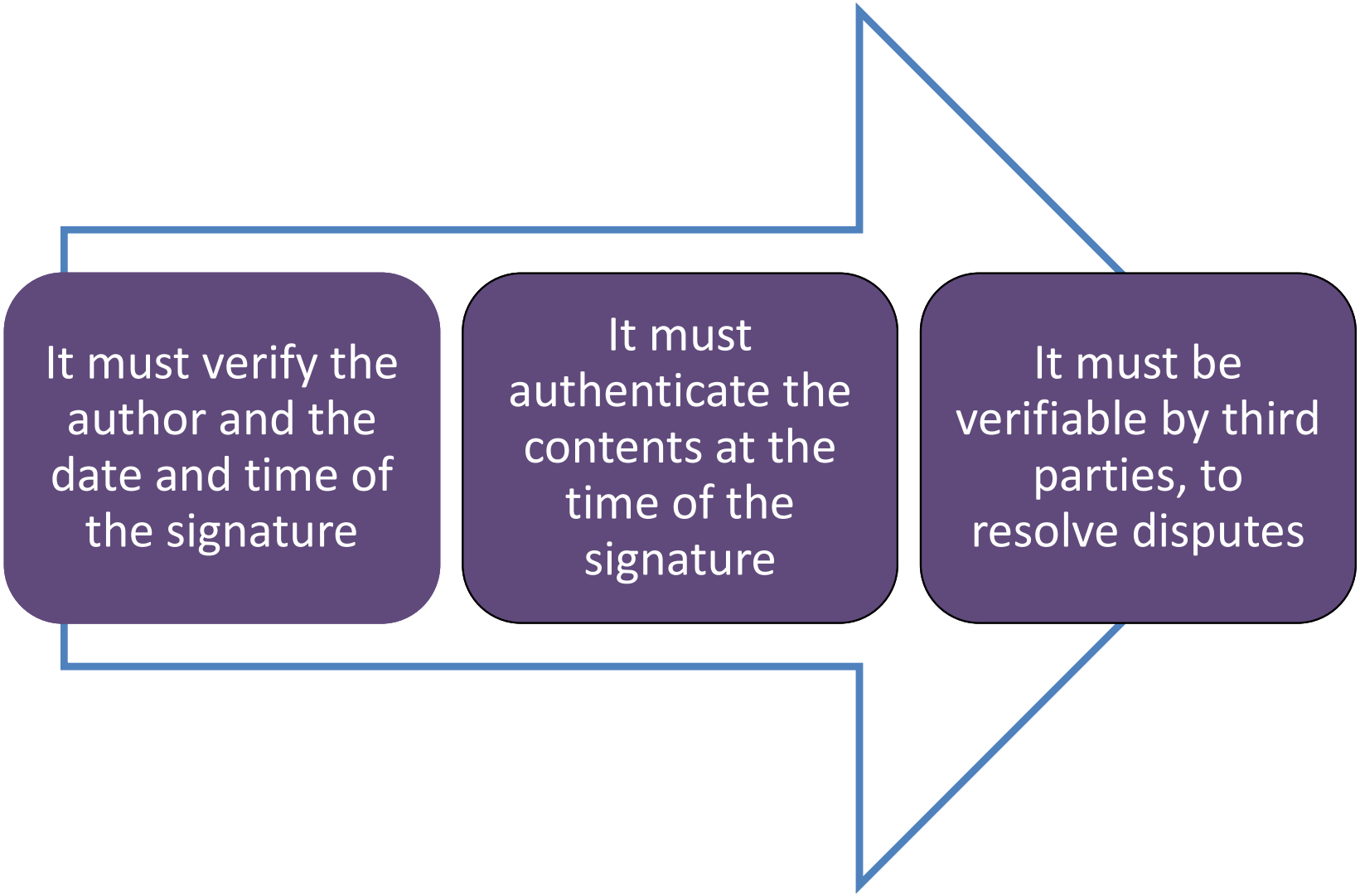
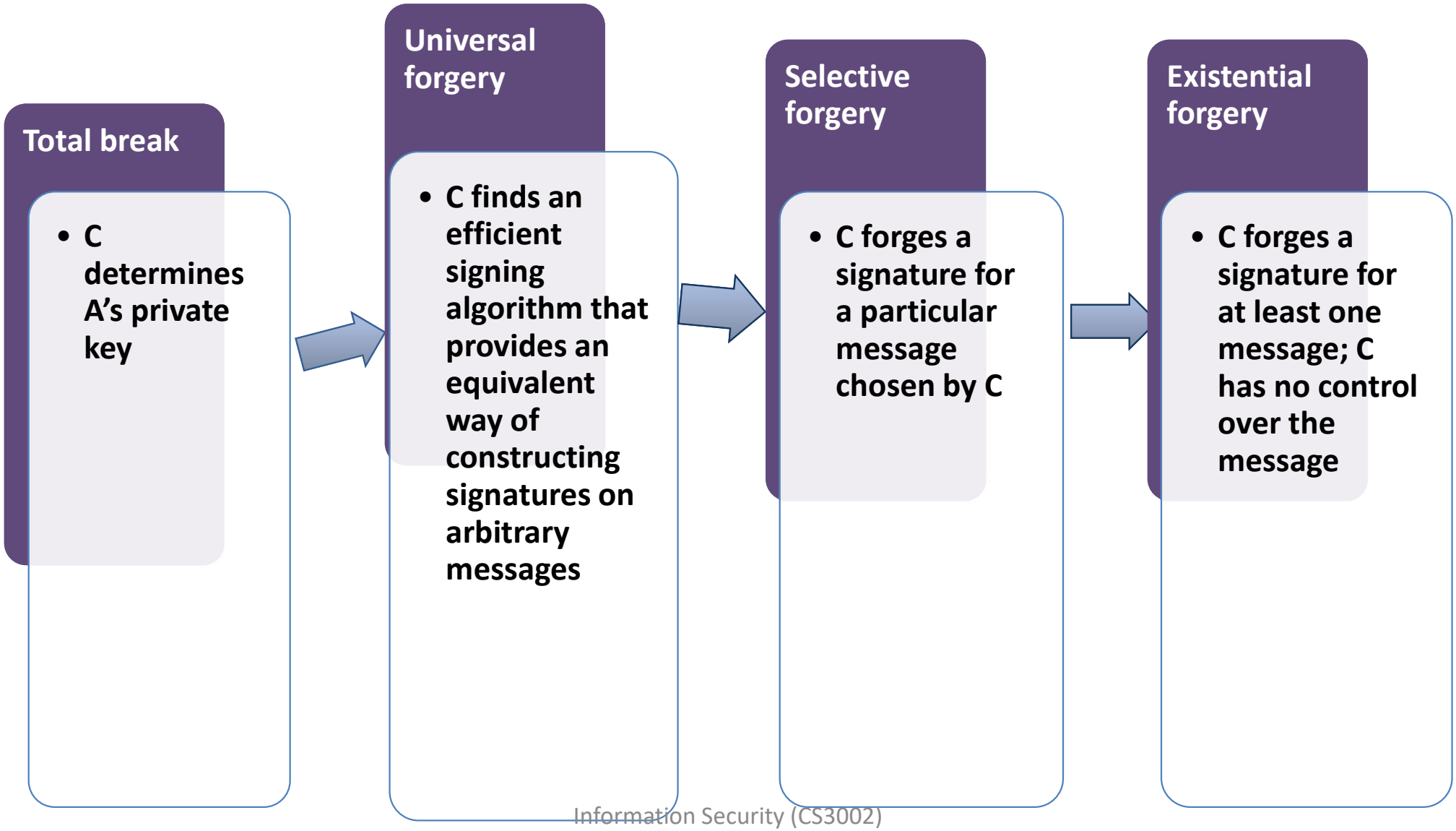


Figure 13.2 Simplified Depiction of Essential Elements of Digital Signature Process

Digital Signature Properties



Forgeries


Total break
• C determines A's private key
Universal forgery
• C finds an efficient signing algorithm that provides an equivalent way of constructing signatures on arbitrary messages
Selective forgery
• C forges a signature for a particular message chosen by C
Existential forgery
• C forges a signature for at least one message; C has no control over the message

Digital Signature Requirements

- The signature must be a bit pattern that depends on the message being signed.
- The signature must use some information unique to the sender to prevent both forgery and denial.
- It must be relatively easy to produce the digital signature.
- It must be relatively easy to recognize and verify the digital signature.
- It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.
- It must be practical to retain a copy of the digital signature in storage.

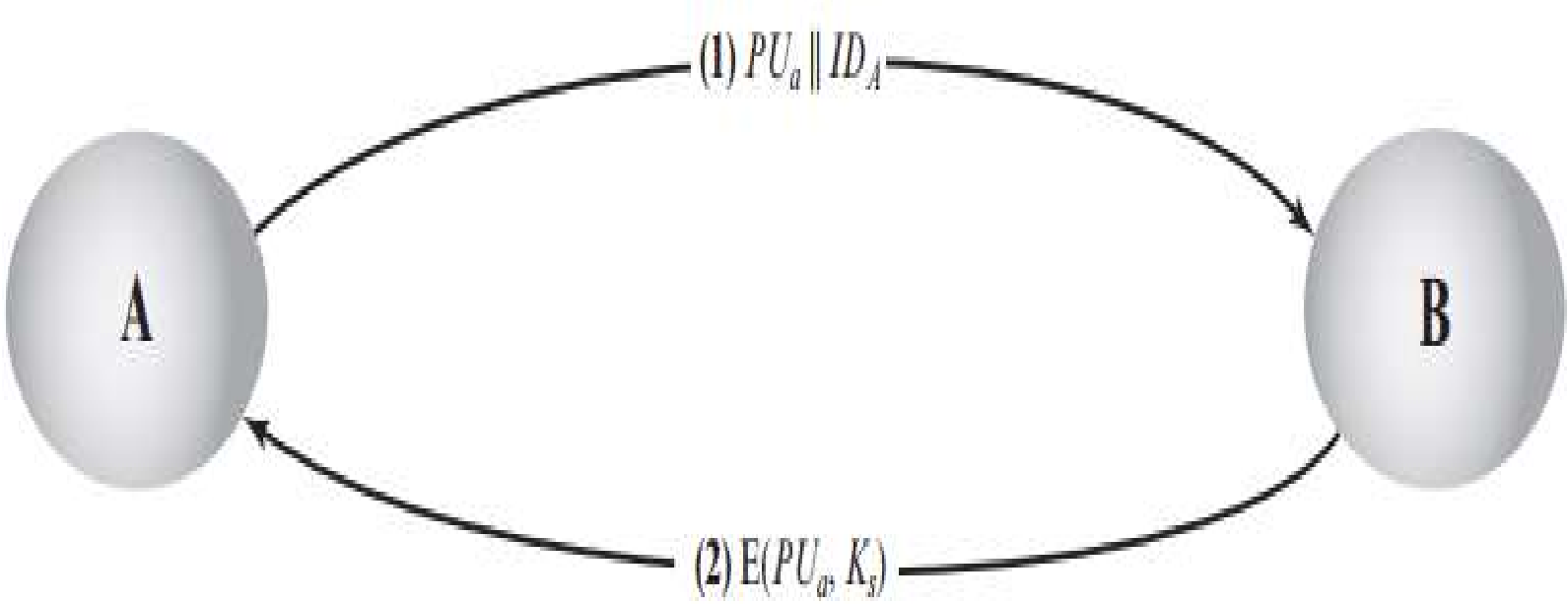
Direct Digital Signature Conflicts

- Refers to a digital signature scheme that involves only the communicating parties.
  - It is assumed that the destination knows the public key of the source.

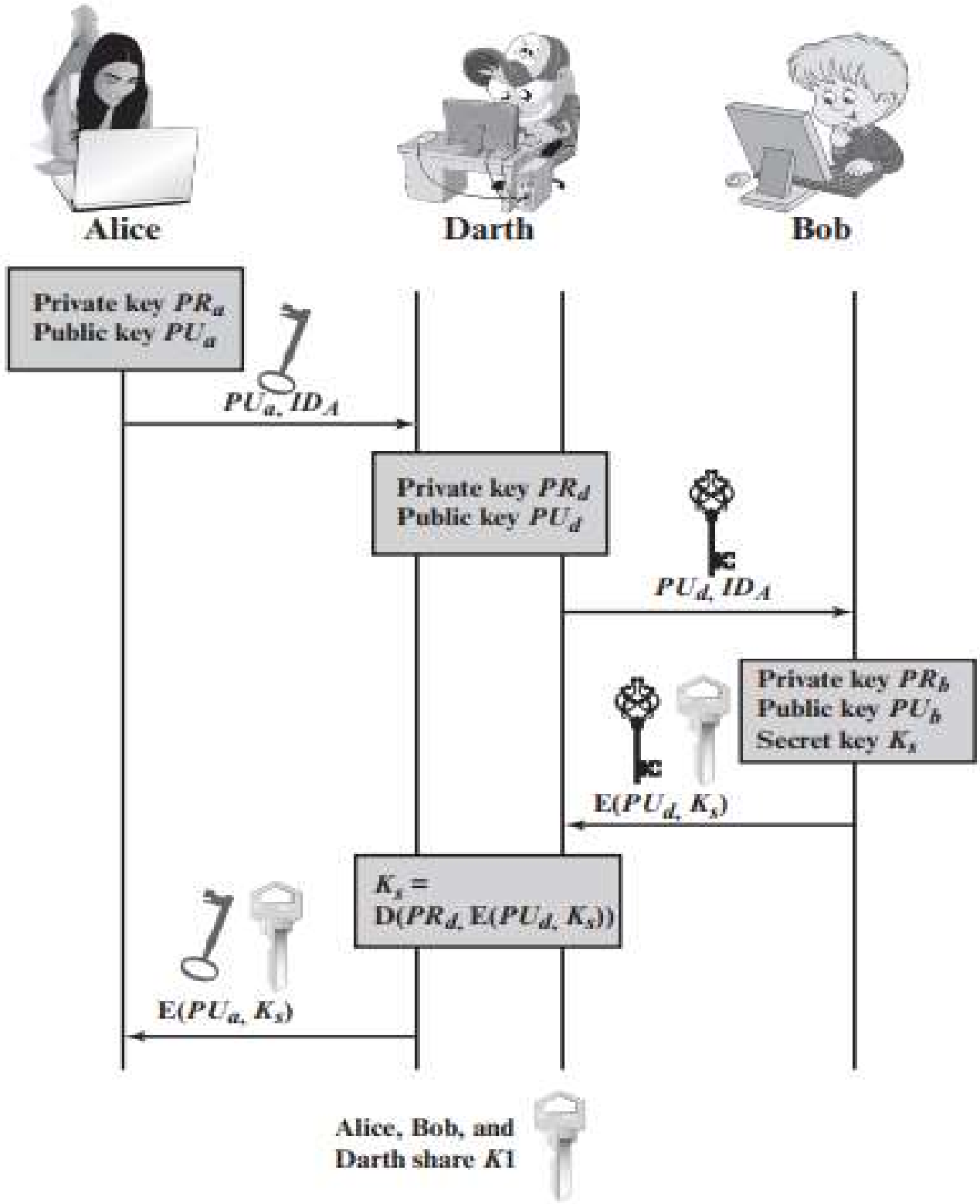
- Confidentiality can be provided by encrypting the entire message plus signature with a shared secret key.
  - It is important to perform the signature function first and then an outer confidentiality function.
  - In case of dispute some third party must view the message and its signature.

- The validity of the scheme depends on the security of the sender's private key
  - If a sender later wishes to deny sending a particular message, the sender can claim that the private key was lost or stolen and that someone else forged his or her signature.
  - One way to thwart or at least weaken this ploy is to require every signed message to include a timestamp and to require prompt reporting of compromised keys to a central authority.

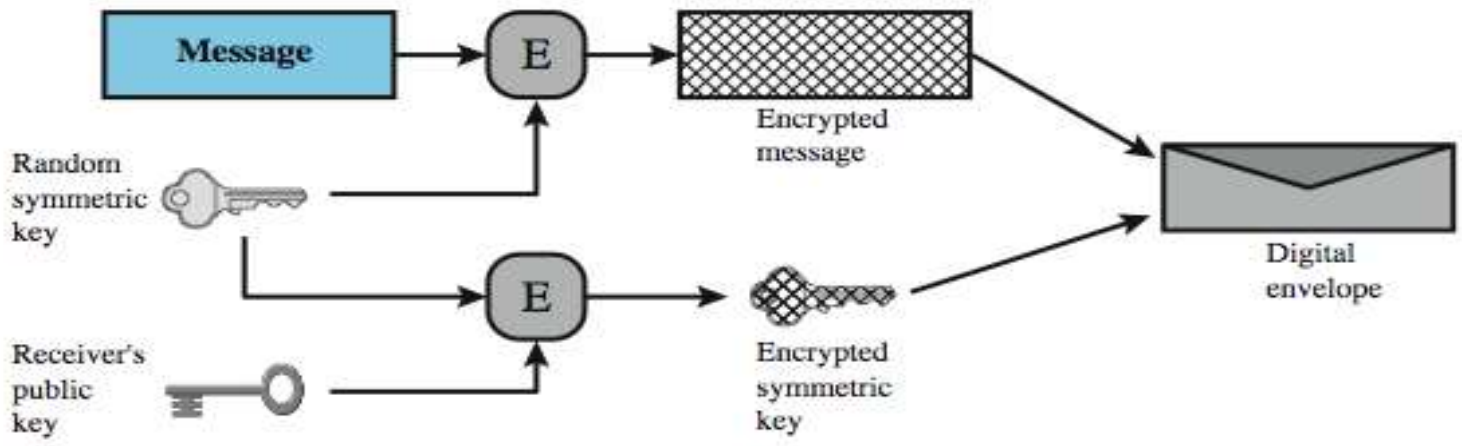
Simple Secret Key Distribution



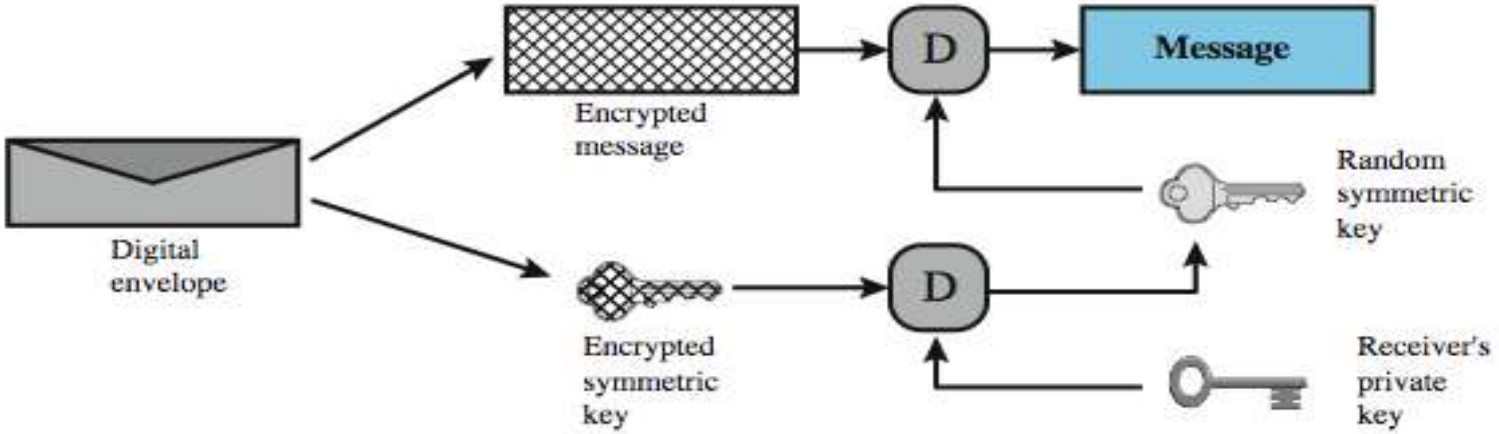
Man-in-the-Middle Attack



Digital Envelopes



(a) Creation of a digital envelope

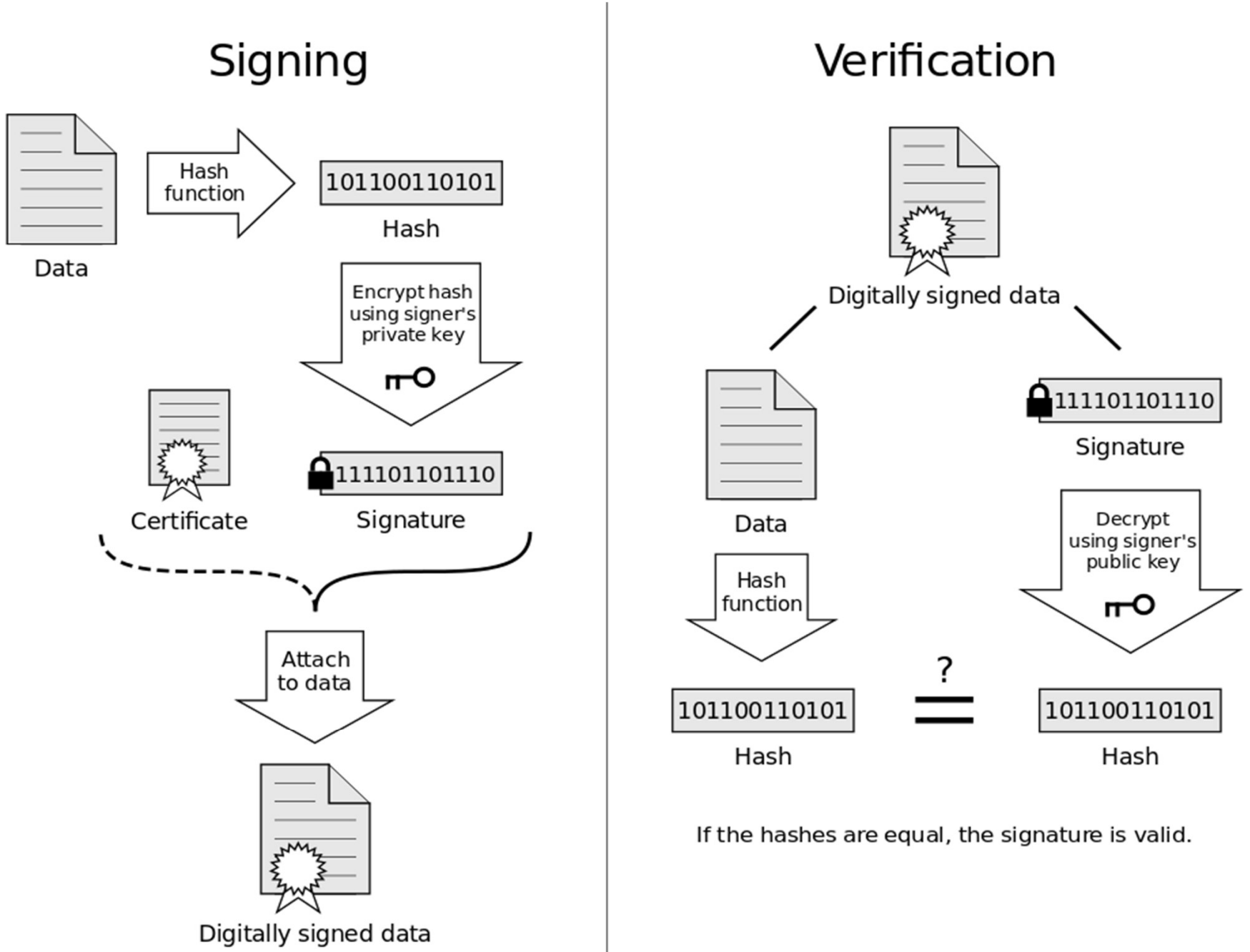


(b) Opening a digital envelope

How we can make sure,
the Public Key belongs to legitimate user?

DIGITAL CERTIFICATE

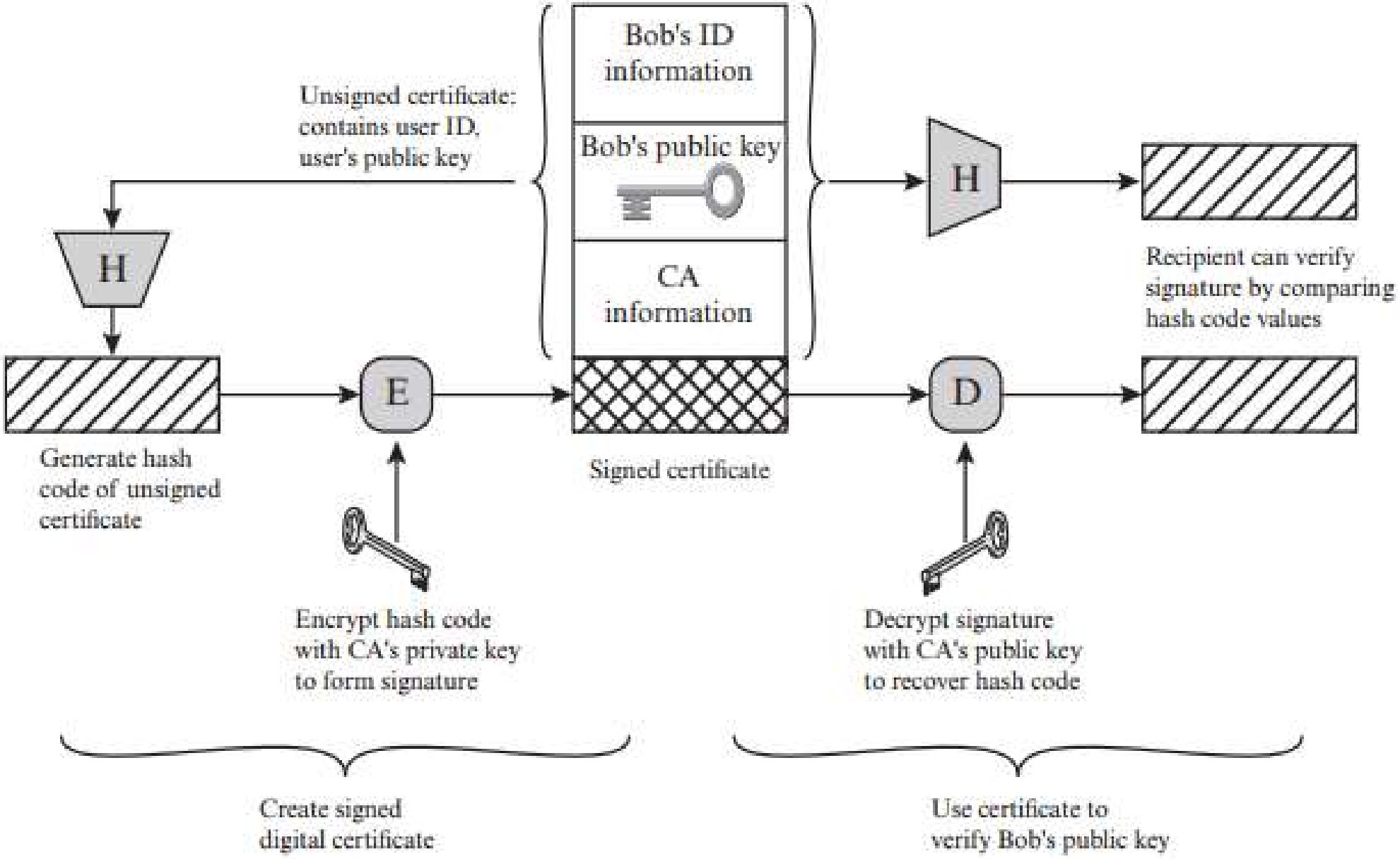
Digital Signature: Message Integrity & Sender Authenticity



Digital Certificate

- To decrypt the signature, the corresponding public key is required.
- A *digital certificate* is used to bind public keys to persons or other entities. If there were no certificates, the signature could easily be forged, as the recipient could not check if the public key belongs to the sender.
- The certificate itself is signed by a trusted third party, a *Certificate Authority* like VeriSign/ DigiCert Inc.

Digital Certificates



PUBLIC KEY INFRASTRUCTURE (PKI)

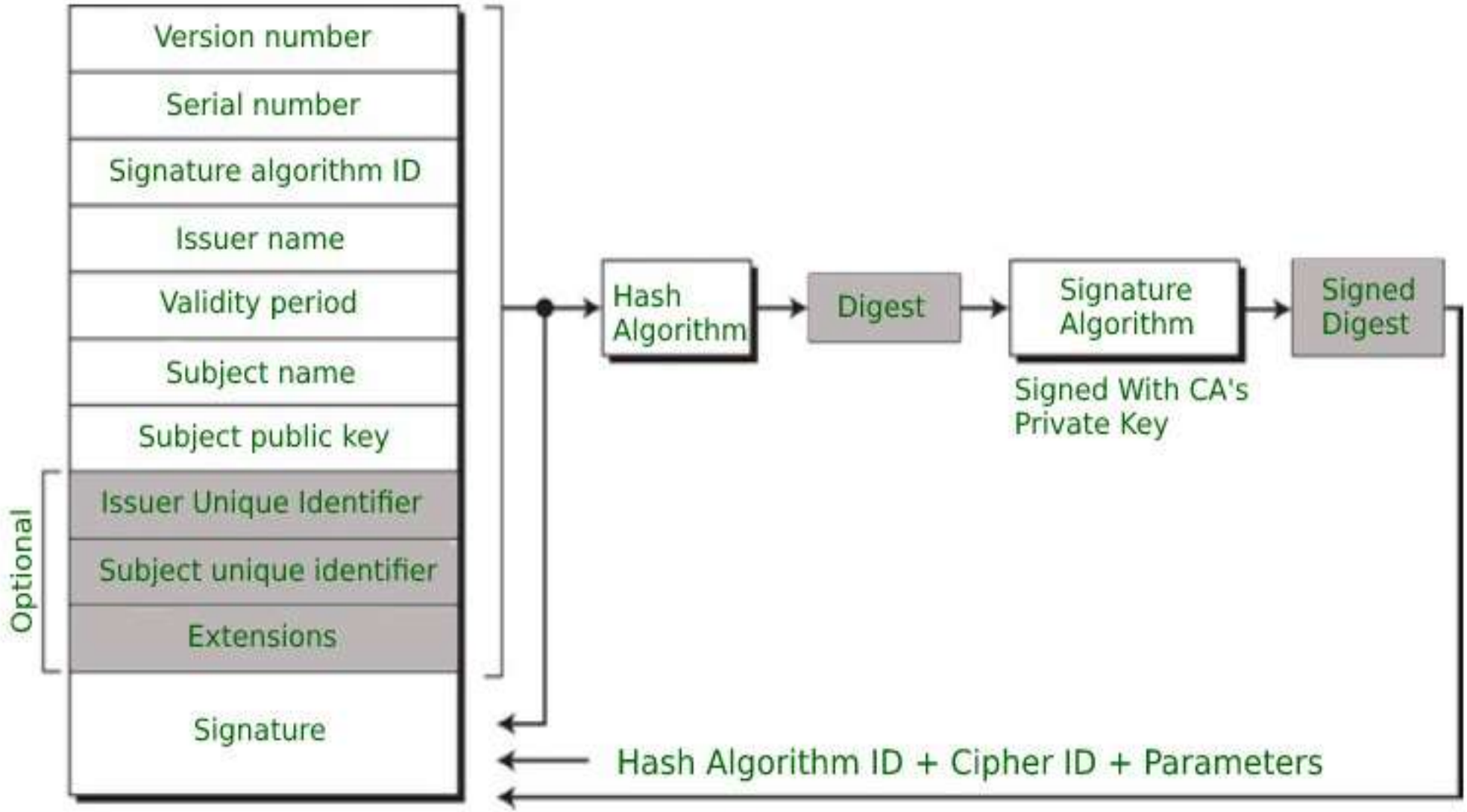
Elements of PKI

- Digital Certificate
  - X.509 standard
- Certificate Authorities (CA)
  - OpenSSL, Netscape, Verisign, Entrust, RSA Keon
- Registration Authority (RA)
- Public/Private Key Pairs - Key management
- Certificate Revocation Lists (CRL)

1. Digital Certificate

- Electronic file/data structure that contains the following information:
  - who issued the certificate: Comodo, Symantec etc
  - who the certificate is issued to
  - Public key of the owner
  - Validity period
  - Digital signature
- Issued by CA
- Helps in authentication
- Associate public key with an individual/company
- X.509 Standard

X.509 Standard



2. Certificate Authority

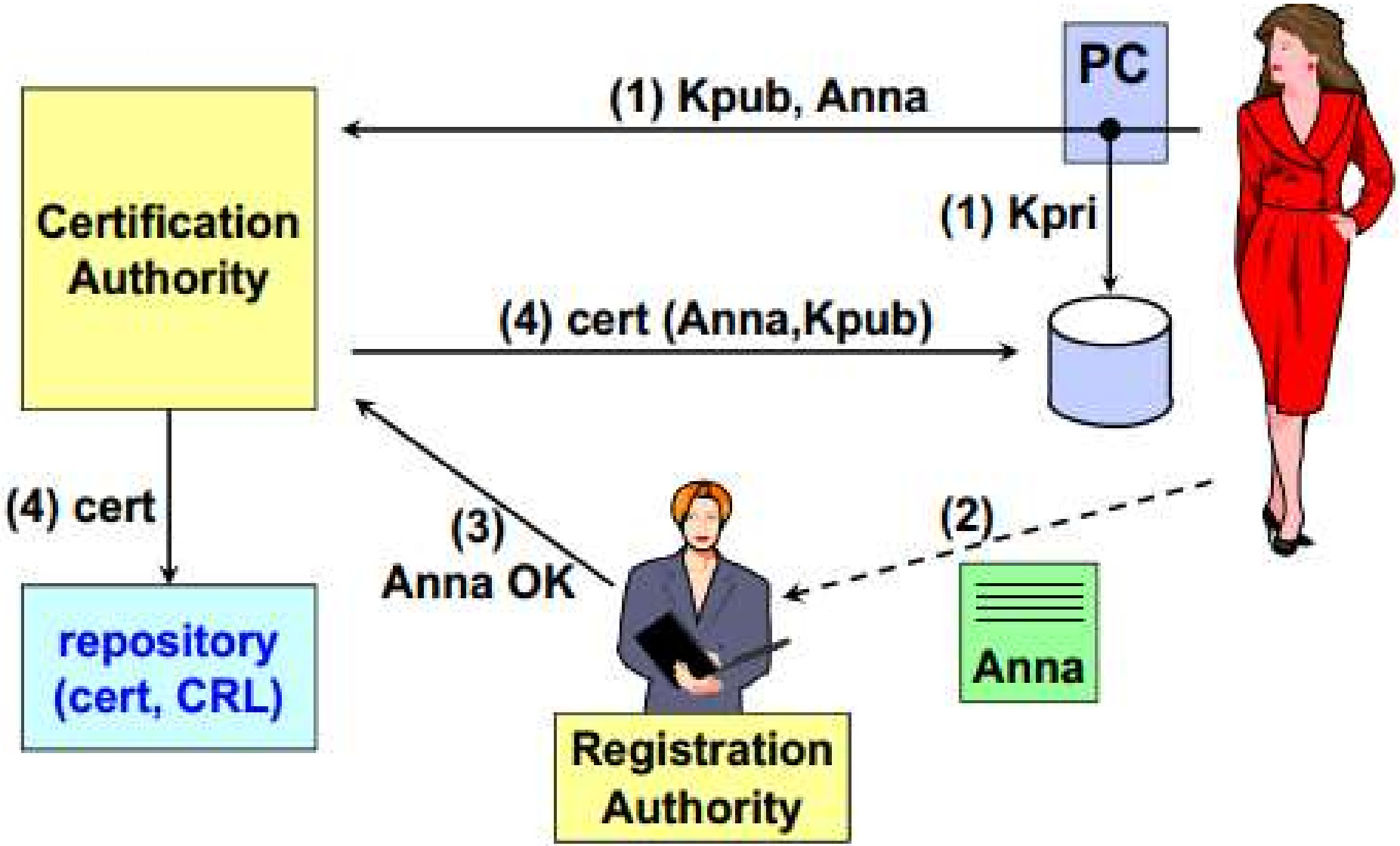
- A trusted third party - must be a secure server
- Signs and publishes X.509 Identity certificates
- Revokes certificates and publishes a Certification Revocation List (CRL)

- Many vendors
  - OpenSSL - open source, very simple
  - Netscape - free for limited number of certificates
  - Entrust - Can be run by enterprise or by Entrust
  - Verisign - Run by Verisign under contract to enterprise
  - RSA Security - Keon servers

3. Registration Authority

- An RA is responsible for accepting requests for digital certificates and authenticating the entity making the request.
- You provide RA with information and money
- Verifies the information before the CA issues the certificate
- Does not sign the certificate
- Key pair maybe created by RA or you

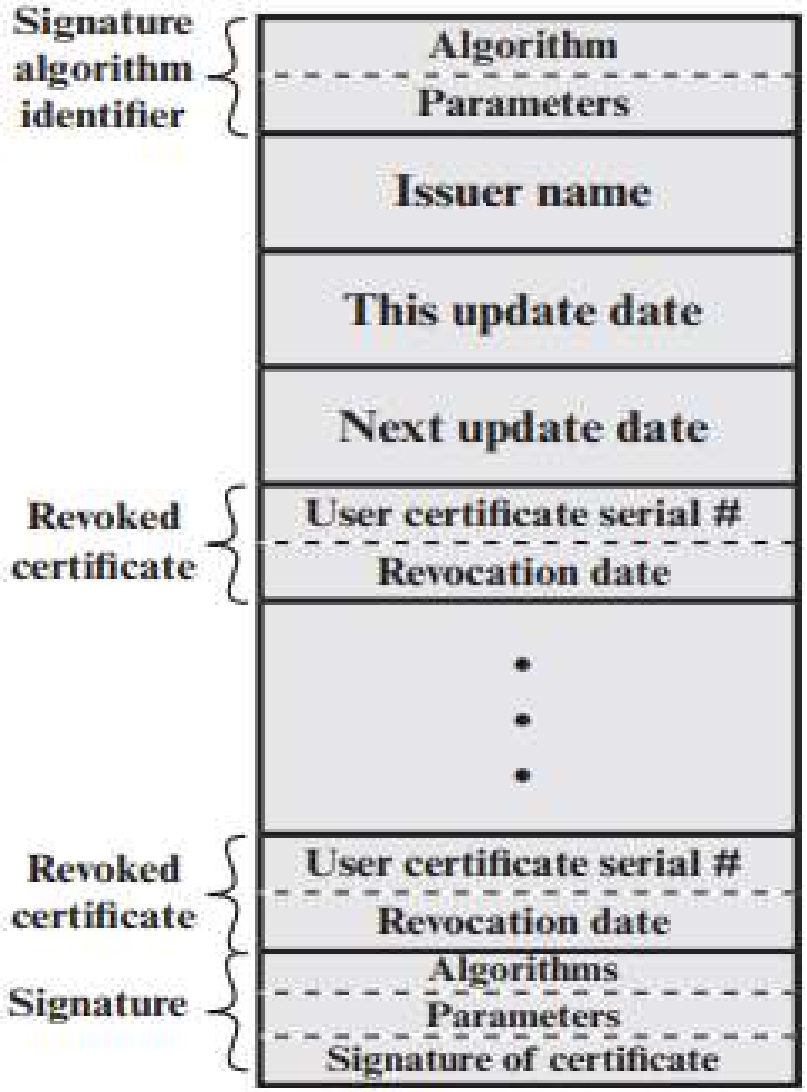
Certificate Issuance Process



4. Certificate Revocation List (CRL)

- List of revoked/cancelled certificates
- List published by CA frequently
- Reasons for revocation:
  - Certificate expiration
  - Certificate revocation (permanent)
    - Compromised private key
    - HR reasons
    - Company changed names, physical address, DNS
    - Any reason prior to expiration
  - Certificate suspended
    - “Certificate hold” as reason for revocation. E.g: resource on leave
- Owner can request the revocation of certificate

Certificate Revocation List



(b) Certificate revocation list

Certificate Revocation Lists

- Certificate revocation lists
  - Too much work on the client
  - Too much traffic on internet
    - Not used
- On-line Revocation Server (OLRS)
  - On-line certificate status protocol (OCSP)
  - Provides current information
  - Saves traffic on the internet
  - Allows chaining of OCSP responders

Certificate Revocation Timeline