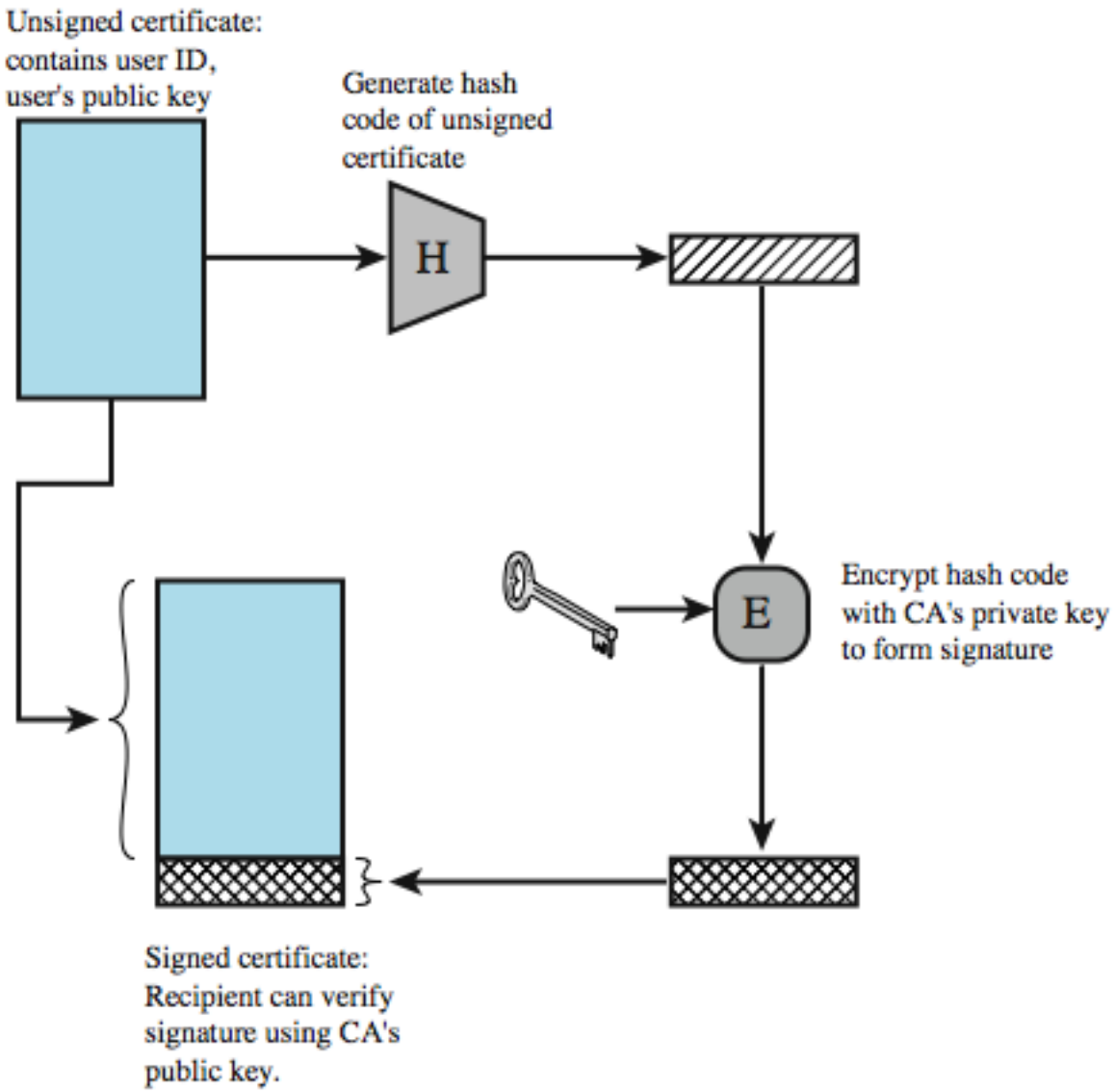
Information Security
CS 3002

Dr. Haroon Mahmood

Assistant Professor

NUCES Lahore

Digital Certificates



Digital Signatures

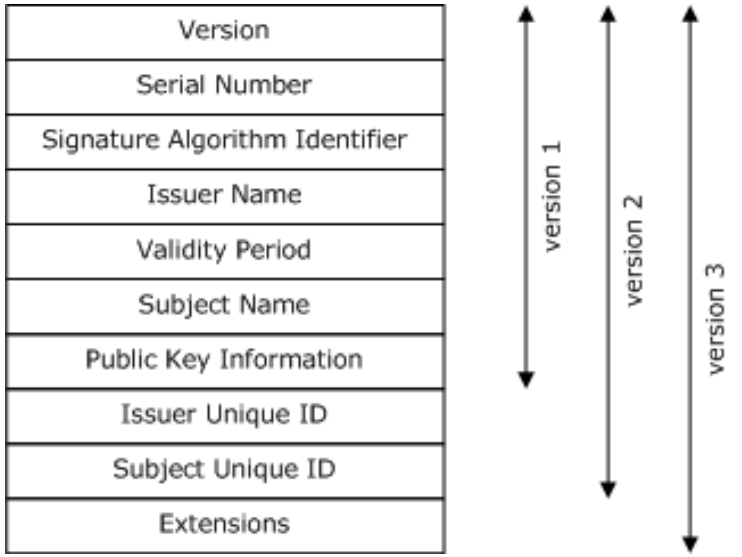
- Combines a hash with a digital signature algorithm
- To sign
  - hash the data
  - encrypt the hash with the sender's private key
  - send data signer’s name and signature
- To verify
  - hash the data
  - find the sender’s public key
  - decrypt the signature with the sender's public key
  - the result of which should match the hash

Elements of PKI

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

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 Identity Certificates

- Distinguished Name of user
  - C=US, O=Lawrence Berkely National Laboratory, OU=DSD, CN=Mary R. Thompson
- DN of Issuer
  - C=US, O=Lawrence Berkely National Laboratory, CN=LBNL-CA
- Validity dates:
  - Not before <date>, Not after <date>
- User's public key
- V3- extensions
- Signed by CA
- Defined in ANS1 notation - language independent

Certificate Authority

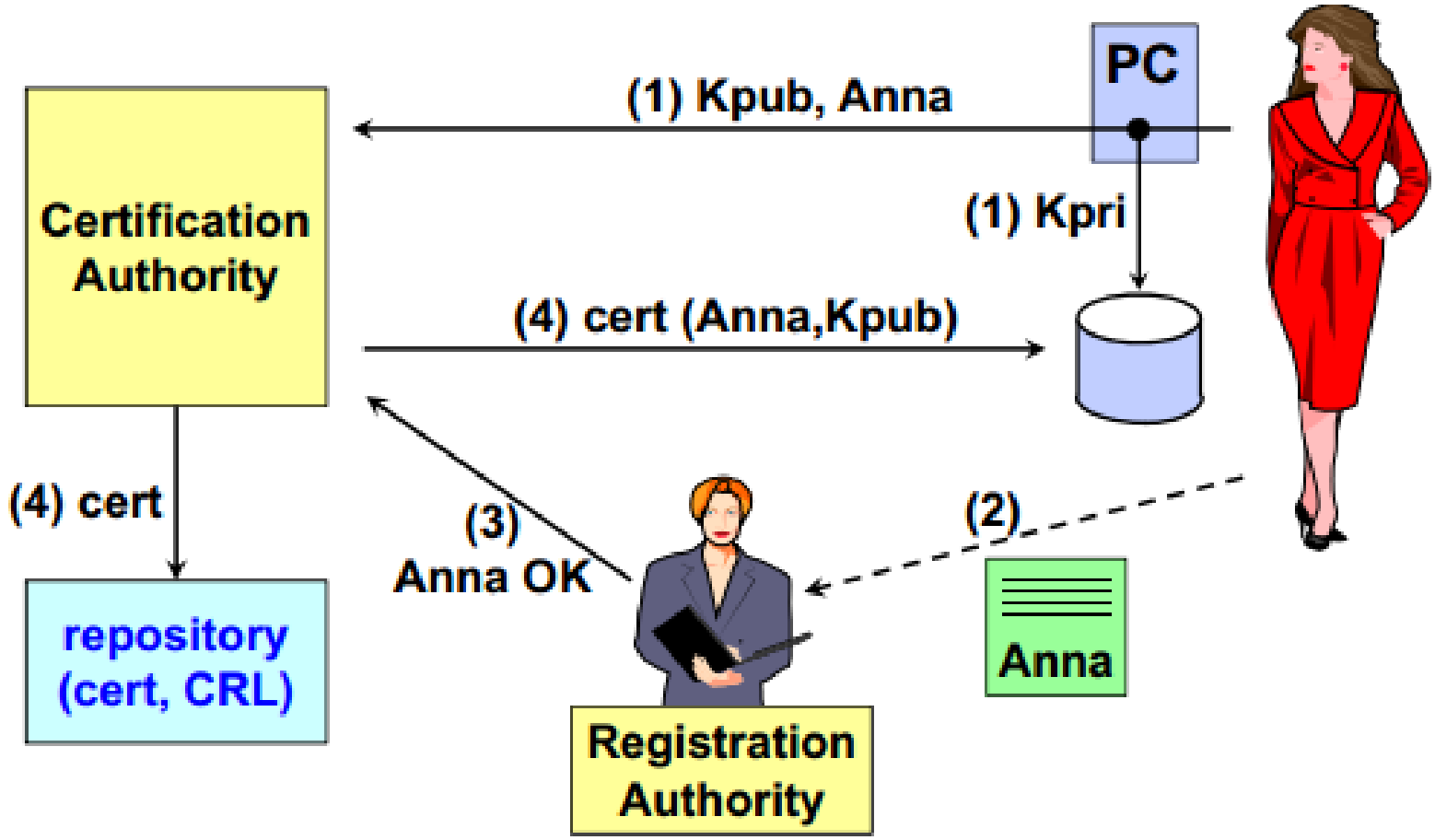
- A trusted third party - must be a secure server
- Signs and publishes X.509 Identity certificates
- Revokes certificates and publishes a Certification Revocation List (CRL)

- 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

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



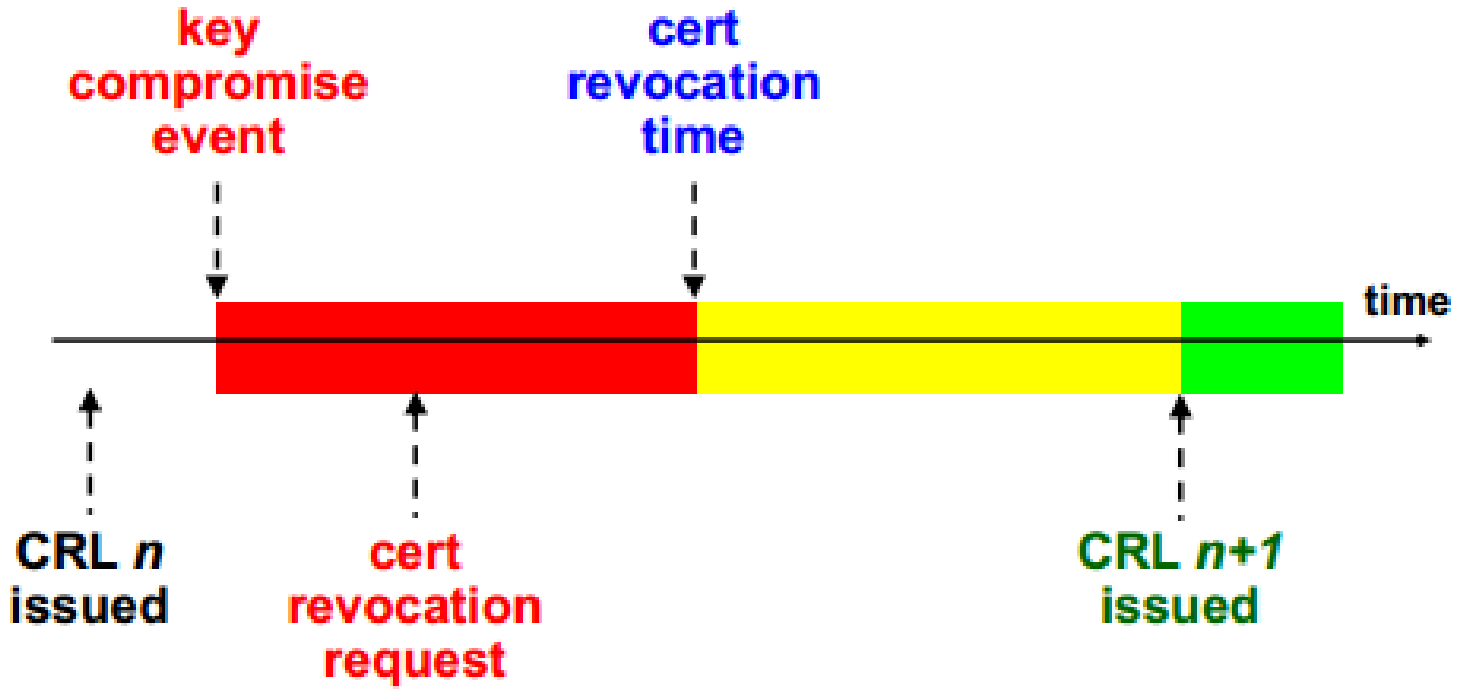
Certificate Revocation List (CRL)

- 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 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



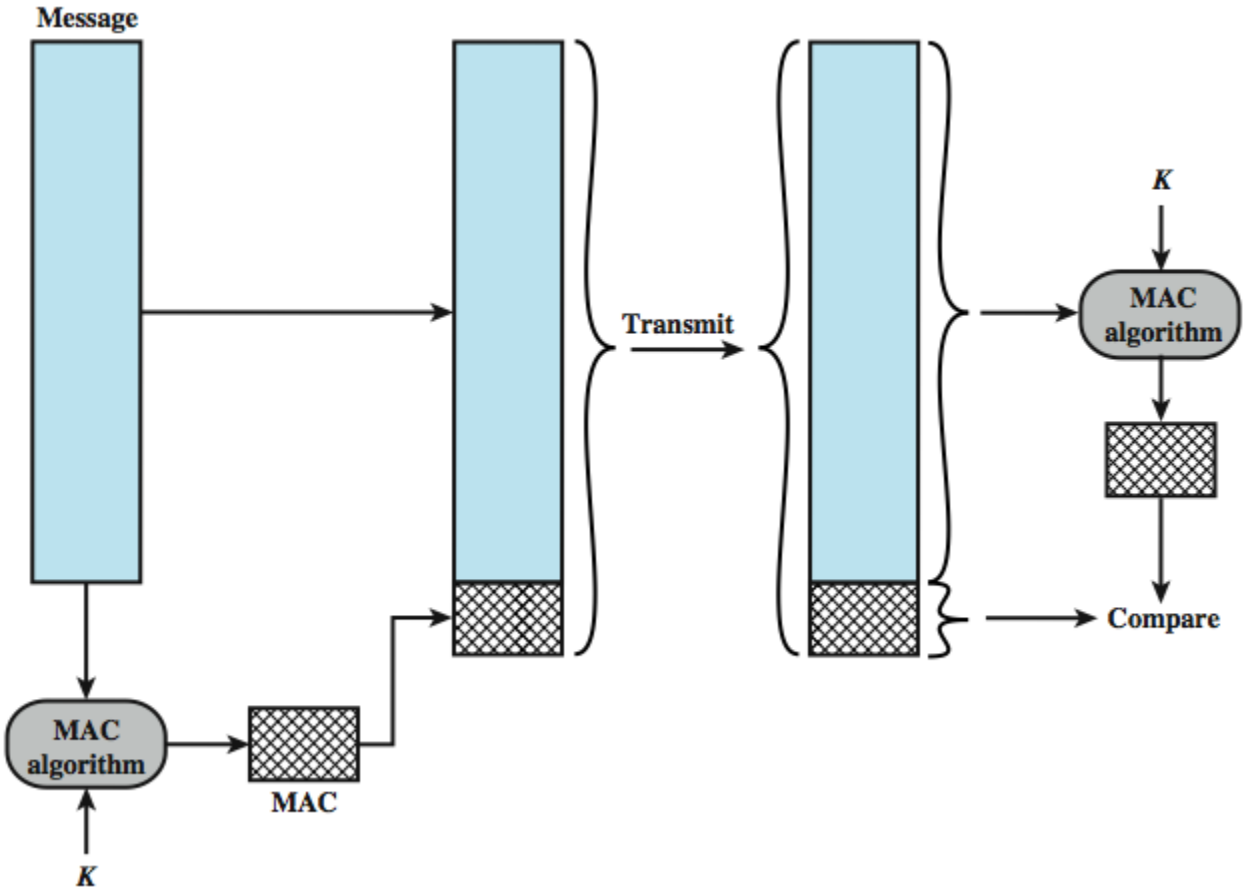
OCSP

- Online certificate status protocol
- IETF-PKIX standard to verify online if a certificate is valid:
  - Good/Verified
  - revoked
    - Revocation Time
    - revocation reason
  - unknown
- response signed by the server (not by the CA!)
- the OCSP server certificate cannot be verified with OCSP itself!

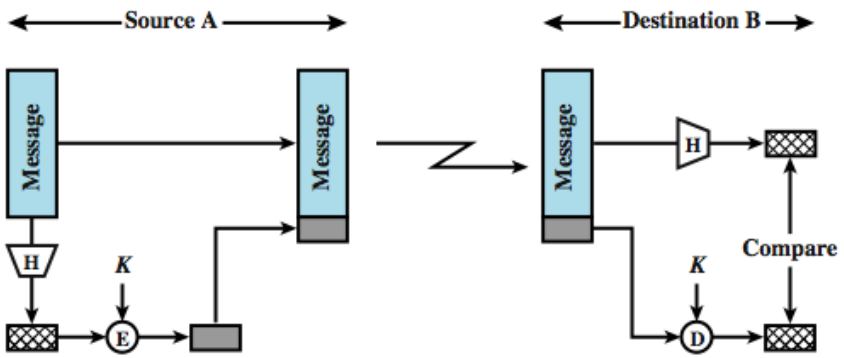
Message Authentication

- protects against active attacks
- verifies received message is authentic
  - contents unaltered
  - from authentic source
  - timely and in correct sequence
- can use conventional encryption
  - only sender & receiver have key needed
- Using public key cryptography
- or separate authentication mechanisms
  - append authentication tag to clear-text message

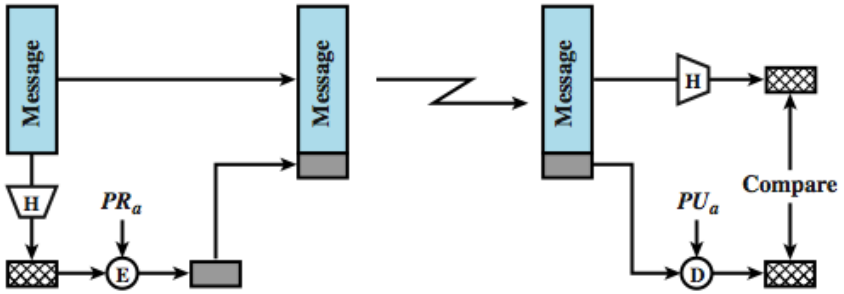
Message Authentication



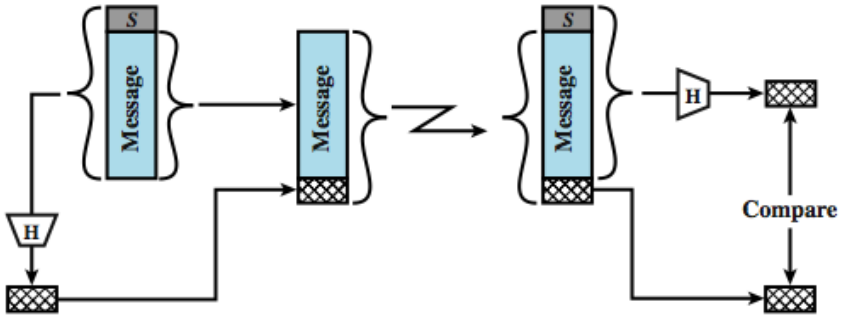
Types of message authentication



(a) Using conventional encryption



(b) Using public-key encryption



(c) Using secret value

Hash algorithms

- Also called message digests or one-way transformations
- Given a message m, the hash h is equal to → h = Hash(m)
- “h” is the output, “Hash” is the reference to hash function, “m” is the message

Review of hash function

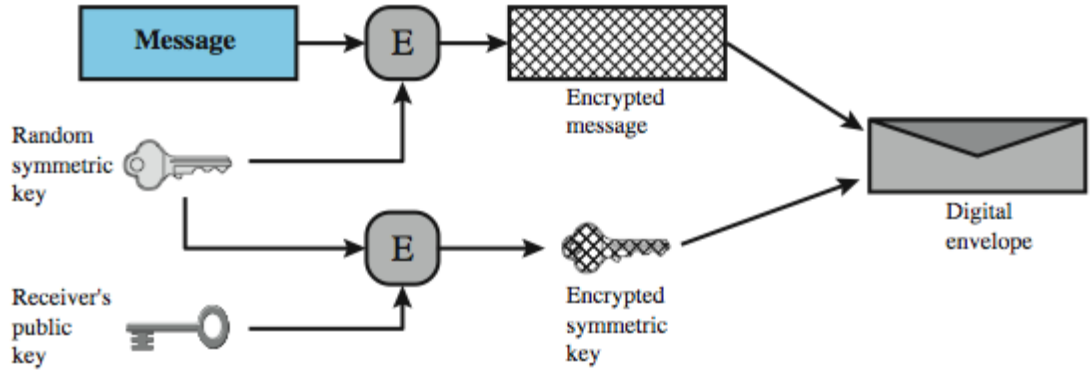
- Input(m) to hash functions can be variable size.
  - Any number of bits, Usually large
- Output of hashes(h) will be fixed.
  - Usually small number of bits
- Strong hash function
  - h is the combination of 1's and 0's distributed variably with a proportion of 50% each.
  - A single bit change in input must change the output by at least 50%
- Collisions in hash functions
  - Two messages having the same h is a collision

Hash functions

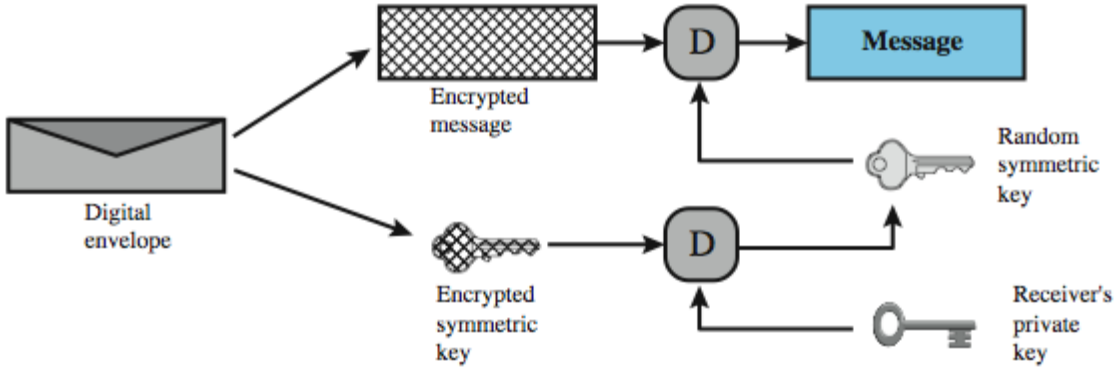
- two attack approaches
  - cryptanalysis
    - exploit logical weakness in algorithm
  - brute-force attack
    - trial many inputs
    - strength proportional to size of hash code ($2^{n/2}$)

- SHA most widely used hash algorithm
  - SHA-1 gives 160-bit hash
  - more recent SHA-256, SHA-384, SHA-512 provide improved size and security

Digital Envelopes



(a) Creation of a digital envelope



(b) Opening a digital envelope