Cryptography and Network Security

cuu duong than cong . com

Chapter 6

Electronic Mail Security

Lectured by
Nguyễn Đức Thái

CuuDuongThanCong.com https://fb.com/tailieudientucntt

Outline

- Pretty Good Privacy
- S/MIME

cuu duong than cong . com

cuu duong than cong . com

Electronic Mail Security

- In virtually all distributed environments, ***electronic mail*** is the ***most heavily used*** network-based application.
- Users expect to be able to, and do, send e-mail to others who are connected directly or indirectly to the Internet, regardless of host operating system or communications suite
- With the explosively growing reliance on e-mail, there grows a ***demand for authentication*** and confidentiality services
- Two schemes in use: ***Pretty Good Privacy*** (PGP) and ***S/MIME***

cuu duong than cong . com

Electronic Mail Security

- Currently message contents are not secure
  - may be inspected either ***in transit***
  - or by suitably privileged users on ***destination system***
- PGP provides a ***confidentiality*** and ***authentication*** service that can be used for electronic mail and file storage applications

cuu duong than cong . com

cuu duong than cong . com

Email Security Enhancements

- **Confidentiality**
  - protection from disclosure
- **Authentication**
  - of sender of message
- **Message integrity**
  - protection from modification
- **Non-repudiation of origin**
  - protection from denial by sender

cuu duong than cong . com

cuu duong than cong . com

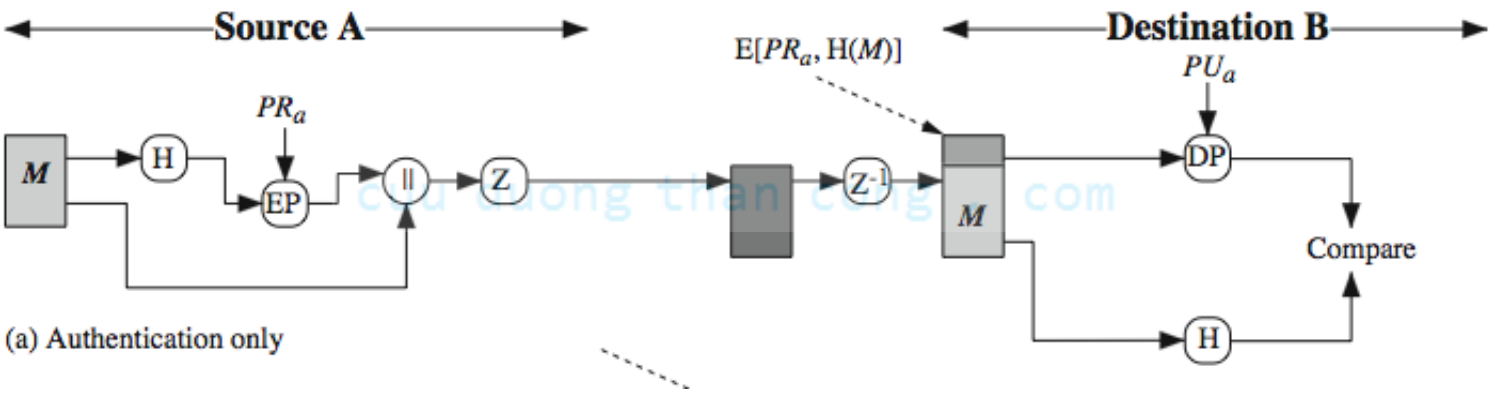
Pretty Good Privacy (PGP)

- widely used de facto secure email
- developed by Phil Zimmermann
- selected best available crypto algorithm to use
- integrated into a single program
- on Unix, PC, Macintosh and other systems
- originally free, now also have commercial versions available

cuu duong than cong . com

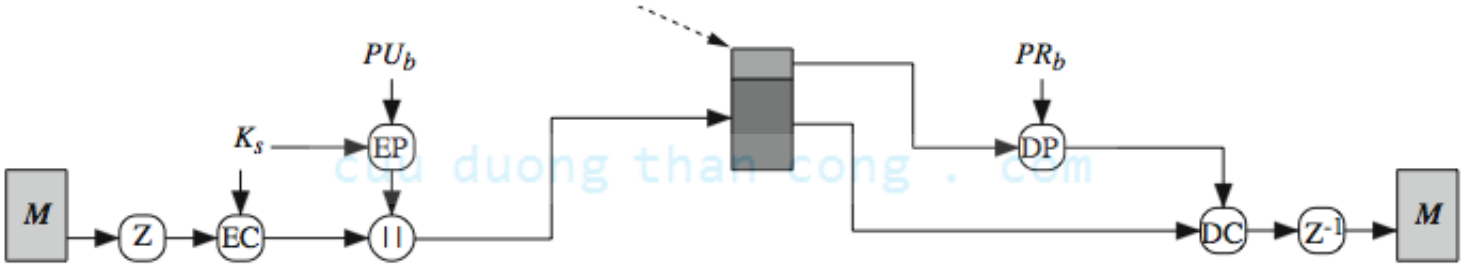
PGP Operation - Authentication

1. sender creates message
2. make SHA-1160-bit hash of message
3. attached RSA signed hash to message
4. receiver decrypts & recovers hash code
5. receiver verifies received message hash



PGP Operation - Confidentiality

1. sender forms 128-bit random session key
2. encrypts message with session key
3. attaches session key encrypted with RSA
4. receiver decrypts & recovers session key
5. session key is used to decrypt message



(b) Confidentiality only

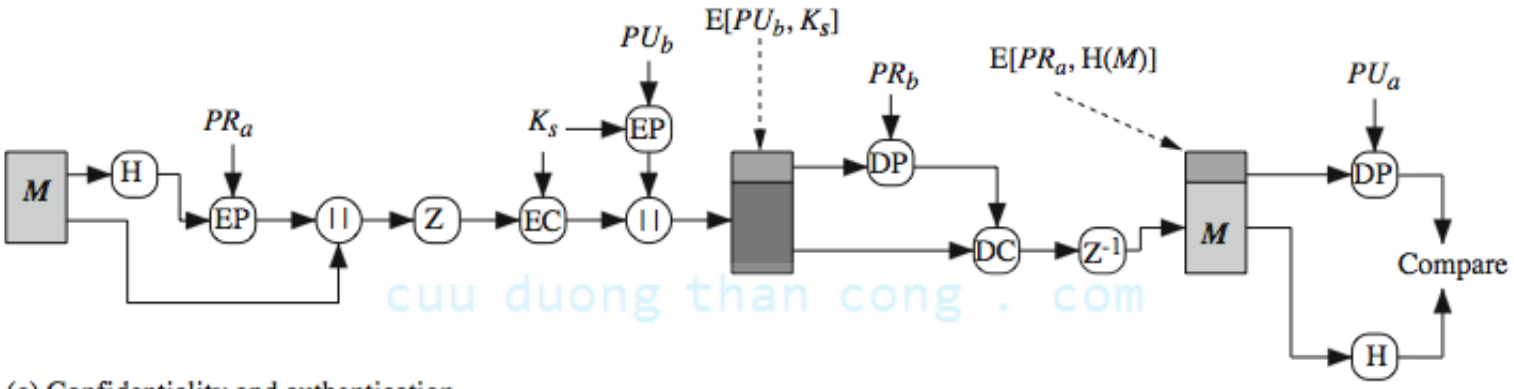
cuu duong than cong . com

PGP – Authentication & Confidentiality

Can use both services on same message

- create signature & attach to message
- encrypt both message & signature
- attach RSA/ElGamal encrypted session key

cuu duong than cong . com



(c) Confidentiality and authentication

cuu duong than cong . com

PGP Operation - Compression

- **by default PGP compresses message after signing but before encrypting**
  - so can store uncompressed message & signature for later verification
  - & because compression is non deterministic
- **uses ZIP compression algorithm**

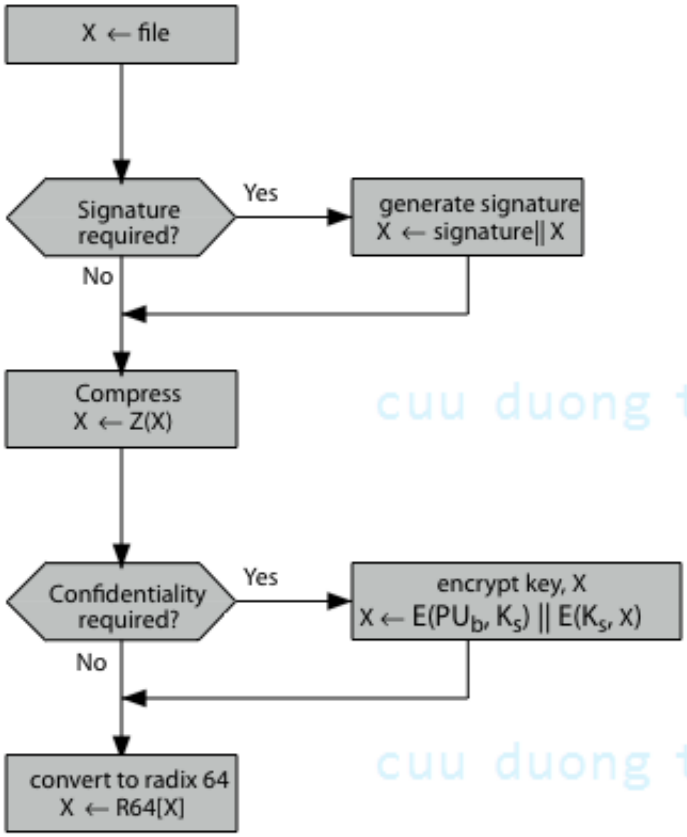
cuu duong than cong . com

PGP Operation – Email Compatibility

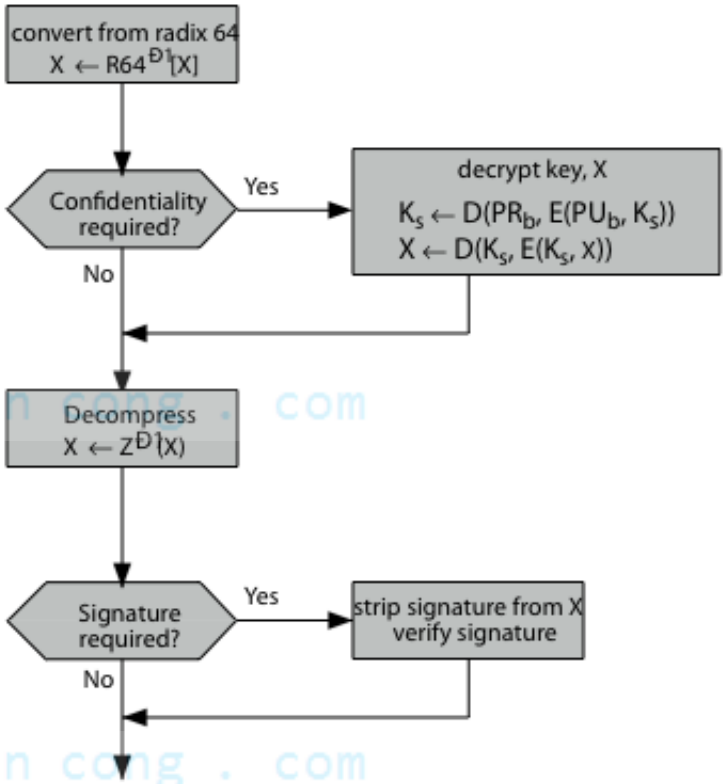
- When PGP is used, at least ***part of the block to be transmitted is encrypted***
- However email ***was designed only for text***
- Hence PGP must ***encode raw binary data*** into printable ASCII characters
- Uses radix-64 algorithm
  - maps 3 bytes to 4 printable chars
  - also appends a CRC
- PGP also ***segments messages*** if too big

cuu duong than cong . com

PGP Operation – Summary



(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

cuu duong than cong . com
cuu duong than cong . com

S/MIME

- **Secure/Multipurpose Internet Mail Extensions**
- **security enhancement to MIME email**
  - original Internet RFC822 email was text only
  - MIME provided support for varying content types and multi-part messages
  - with encoding of binary data to textual form
  - S/MIME added security enhancements
- **have S/MIME support in many mail agents**
  - eg MS Outlook, Mozilla, Mac Mail etc

cuu duong than cong . com

S/MIME Functions

- **enveloped data**
  - encrypted content and associated keys
- **signed data**
  - encoded message + signed digest
- **clear-signed data**
  - cleartext message + encoded signed digest
- **signed & enveloped data**
  - nesting of signed & encrypted entities

cuu duong than cong . com

S/MIME Cryptographic Algorithms

- Digital signatures: DSS & RSA
- Hash functions: SHA-1 & MD5
- Session key encryption: ElGamal & RSA
- Message encryption: AES, Triple-DES, RC2/40 and others
- MAC: HMAC with SHA-1
- Have process to decide which algorithms to use

cuu duong than cong . com

cuu duong than cong . com

S/MIME Messages

- **S/MIME secures a MIME entity with a signature, encryption, or both**
- **Forming a MIME wrapped PKCS object**
- **Have a range of content-types:**
  - enveloped data
  - signed data
  - clear-signed data
  - registration request
  - certificate only message

cuu duong than cong . com

S/MIME Certificate Processing

- S/MIME uses X.509 v3 certificates
- managed using a hybrid of a strict X.509 CA hierarchy & PGP's web of trust
- each client has a list of trusted CA's certificates
- and own public/private key pairs & certificates
- certificates must be signed by trusted CA's

cuu duong than cong . com

Certificate Authorities

- have several well-known CA's
- Verisign one of most widely used
- Verisign issues several types of Digital IDs
- increasing levels of checks & hence trust

Class	Identity Checks	Usage
1	name/email check	web browsing/email
2	+ enroll/addr check	email, subs, s/w validate
3	+ ID documents	e-banking/service access

cuu duong than cong . com

S/MIME Enhanced Security Services

- **3 proposed enhanced security services:**
  - signed receipts
  - security labels
  - secure mailing lists

cuu duong than cong . com

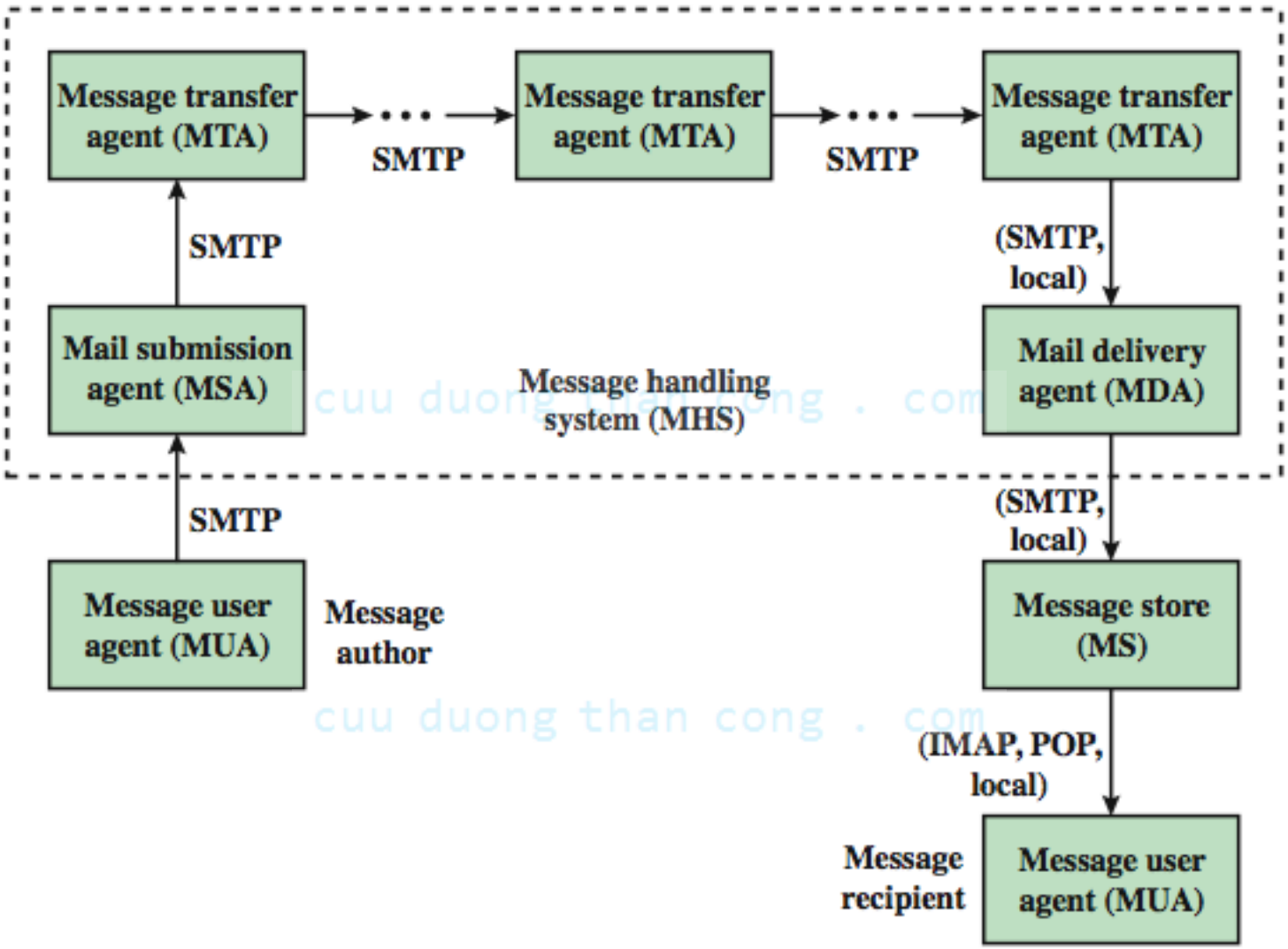
cuu duong than cong . com

Domain Keys Identified Mails

- a specification for cryptographically signing email messages
- so signing domain claims responsibility
- recipients / agents can verify signature
- proposed Internet Standard RFC 4871
- has been widely adopted

cuu duong than cong . com

Internet Mail Architecture



cuu duong than cong . com

Email Threats

- see RFC 4684- *Analysis of Threats Motivating DomainKeys Identified Mail*
- describes the problem space in terms of:
  - range: low end, spammers, fraudsters
  - capabilities in terms of where submitted, signed, volume, routing naming etc
  - outside located attackers

cuu duong than cong . com

Summary

We have discussed:

- Pretty Good Privacy
- S/MIME

cuu duong than cong . com

cuu duong than cong . com

References

1. Cryptography and Network Security, Principles and Practice, William Stallings, Prentice Hall, Fifth Edition, 2011

cuu duong than cong . com

cuu duong than cong . com