Computer Security and Cryptography

CS381

来学嘉
计算机科学与工程系 电院3-423室
34205440 1356 4100825 laix@sjtu.edu.cn

2016-05

Organization

- Week 1 to week 16 (2016-02-24 to 2016-06-08)
- 东上院502
- Monday 3-4节; week 9-16
- Wednesday 3-4节; week 1-16
- lecture 10 + exercise 40 + random tests 40 + other 10
- Ask questions **in** class – counted as points
- Turn ON your mobile phone (after lecture)
- Slides and papers:
  - http://202.120.38.185/CS381
    - **computer-security**
  - http://202.120.38.185/references
- TA: '薛伟佳' xue_wei_jia@163.com, '黄格仕' <huang.ge.shi@foxmail.com>
- Send homework to: laix@sjtu.edu.cn and to TAs

Rule: do not disturb others!

2

Contents

- Introduction -- What is security?
- Cryptography
  - Classical ciphers
  - Today's ciphers
  - Public-key cryptography
  - Hash functions/MAC
  - Authentication protocols
- Applications
  - Digital certificates
  - Secure email
  - Internet security, e-banking

Network security
- SSL
- IPSEC
- Firewall
- VPN

Computer security
- Access control
- Malware
- DDos
- Intrusion

Examples
- Bitcoin
- Hardware
- Wireless

3

overview

IT-security
- Definition
- 5 services
- 1-way function

Classical Shannon

Security Un/condition

Integer factor Discrete log

Block cipher Stream cipher | **Hash MAC** | **PKC signature**

Key-manage →

Kerberos

Certificate PKI

Intrusion Malware

Firewall

IPSEC VPN

SSL TLS

PGP S/MIME

applications

4

Email Security

- email is one of the most widely used and regarded network services
- currently message contents are not secure
  - may be inspected either in transit
  - or by suitably privileged users on destination system

- PGP
- S/MIME

Pretty Good Privacy (PGP)

- widely used de facto secure email
- developed by Phil Zimmermann in 1989 (DES)
- published for free on the Internet in 1991 (IDEA)
- 1993-96: criminal investigation by US government
- PGP
  - selected best available crypto algorithms to use
  - integrated into a single program
  - available on Unix, PC, Mac and Amiga systems
  - Commercial: PGP Inc. -- Network Associates Inc. -- Symantec
  - Free: http://www.openpgp.org/

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

PGP Operation – Authentication

sender	receiver
1. creates a message 2. SHA-1 is used to generate 160-bit hash code of message 3. hash code is signed with RSA using the sender's private key, and result is attached to message	1. uses RSA with sender's public key to recover hash code 2. receiver generates new hash code for message and compares with recovered hash code, if match, message is accepted as authentic

PGP Operation – Confidentiality

sender

1. generates message and a random 128-bit number used as session key for this message only
2. message is compressed, then encrypted using CAST-128 / IDEA/3DES with session key
3. session key is encrypted using RSA with recipient's public key, then attached to message

receiver

1. uses RSA with private key to decrypt and recover session key
2. session key is used to decrypt message
3. Decompress the message

PGP Operations

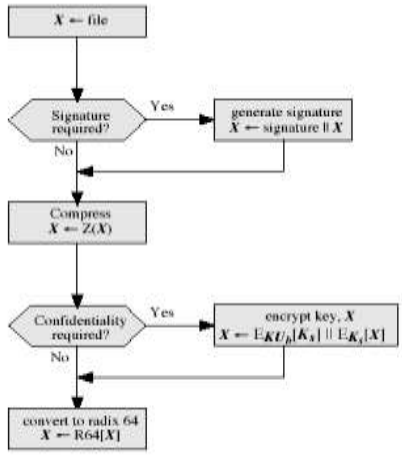
- Confidentiality & Authentication
  - uses both services on same message
  - create signature & attach to message
  - encrypt both message & signature
  - attach RSA encrypted session key
- Compression
  - by default PGP compresses message after signing but before encrypting
  - One can store uncompressed message & signature for later verification, because compression is non deterministic
  - uses ZIP compression algorithm

PGP Operation – Email Compatibility

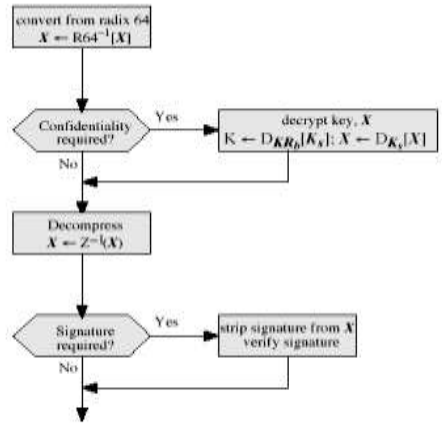
- PGP sends binary data (encrypted message etc)
- Email was designed only for text
- must encode raw binary data into printable ASCII characters
- PGP uses radix-64 algorithm (base-64, .b64)
  - maps 3 bytes to 4 printable chars
  - also appends a CRC
- PGP also segments messages if too big

- PGP message can be sent use any email client

PGP Operation – Summary

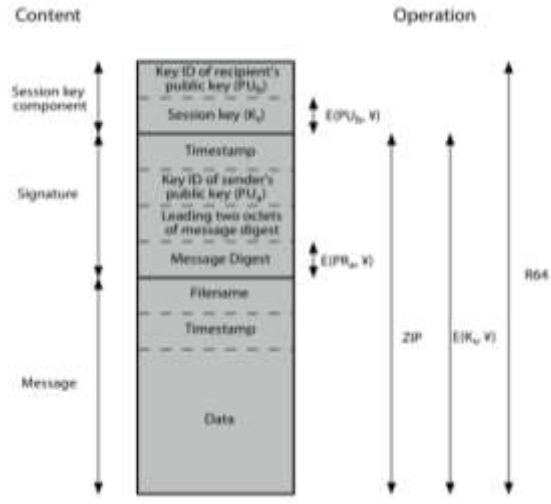


(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

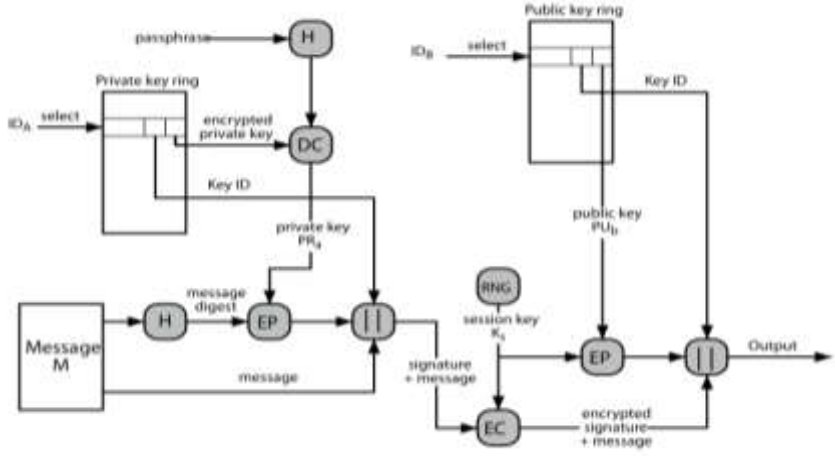
PGP Message , keys



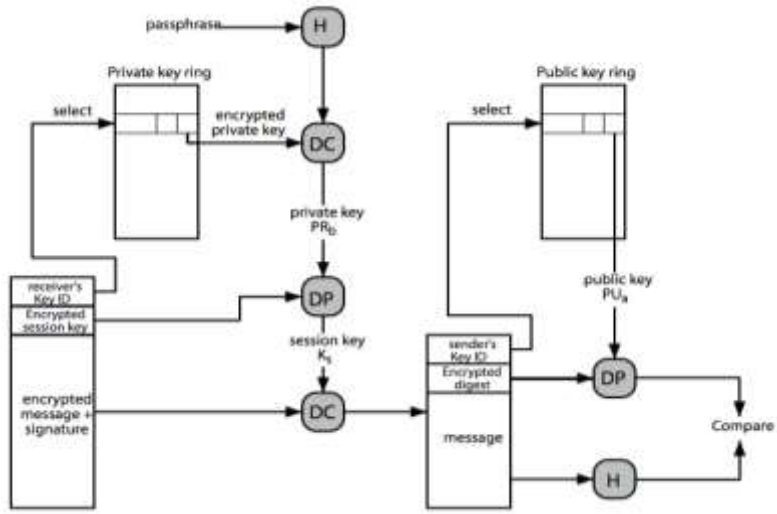
Session key
- 56-bit DES, 128-bit CAST or IDEA, 168-bit 3-DES
- generated using ANSI X12.17 mode
- uses random inputs taken from previous uses and from keystroke timing of user

PGP user keyrings
- public-key ring contains the public-keys of all other users, indexed by key ID
- private-key ring contains the public/private key pair(s) for this user, indexed by key ID & encrypted keyed from a hashed passphrase

PGP Message Generation



PGP Message Reception



PGP Key Management

- rather than relying on certificate authorities
- in PGP every user is own CA
  - can sign keys for users they know directly
- forms a "web of trust"
  - trust keys have signed
  - can trust keys others have signed if have a chain of signatures to them
- key ring includes trust indicators
- users can also revoke their keys

Email Security

- email is one of the most widely used and regarded network services
- currently message contents are not secure
  - may be inspected either in transit
  - or by suitably privileged users on destination system

- PGP
- S/MIME

What is S/MIME?

- When email (SMTP) was first developed, people could only send plain text messages
- MIME (Multipurpose Internet Mail Extension)
  - developed in early 90s to
  - allow to send pictures, sound, programs and general attachments
  - has no security features, can be read or forged (easily)
- S/MIME is a secure version of MIME

Simple Mail Transfer Protocol (SMTP)

- Documented in RFC 821.
- Internet's standard host-to-host mail transport protocol and operates over TCP, port 25.
- RFC 822 SMTP mail has headers like "To:" and "From:" and "Subject"
- SMTP is limited to text with hard line breaks.

```
From: Hodapp, Phil
To: McFadden, Mark
Subject: Examples of MIME Messages
Content-Type: text/plain

Would you kindly make an effort to insure
that your explanations are in English and not
in that other language you occasionally drift
into?  Many Thanks.

-Phil
```

Message Header

Message Body (ASCII)

19

MIME

- Multipurpose Internet Mail Extensions (MIME) is an official Internet standard that specifies how messages must be formatted so that they can be exchanged between different email systems.
- MIME is a very flexible format, permitting one to include virtually any type of file or document in an email message.
- MIME uses these RFC 822 headers
  - Content-Type
  - Content-Transfer-Encoding
- Allows to send
  - formatted text
  - non-English character sets
  - images, sounds, video and HTML

20

Typical MIME Content Types

- text
  - text/plain
  - text/richtext
- message
  - message/rfc822
- image
  - image/jpeg
  - image/gif
- Audio
  - sound
- video
  - video/mpeg
- application
  - application/postscript
  - application/octet-stream
- multipart
  - multipart/mixed
  - multipart/alternative

- RFC 2045. "MIME Part 1: Format of Internet Message Bodies",
- RFC 2046. "MIME Part 2: Media Types",
- RFC 2047. "MIME Part 3: Message Header Extensions for Non-ASCII Text",
- RFC 2048. "MIME Part 4: Registration Procedures",
- RFC 2049. "MIME Part 5: Conformance Criteria and Examples",

21

MIME example

MIME – Multipurpose Internet Mail Extension

```
From: trinity@matrix.org
To: neo@matrix.org
MIME- Version: 1.0
Content- Type: multipart/mixed;
   boundary=boundary1

-- boundary1
Content- Type: text/plain; charset=us -ascii

    Dear Neo, please study the attached Word document.

-- boundary1
Content- Type: application/msword; name="Matrix.doc"
Content- Transfer- Encoding: base64

     ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfH
    4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbTrfv=

-- boundary1 --
```

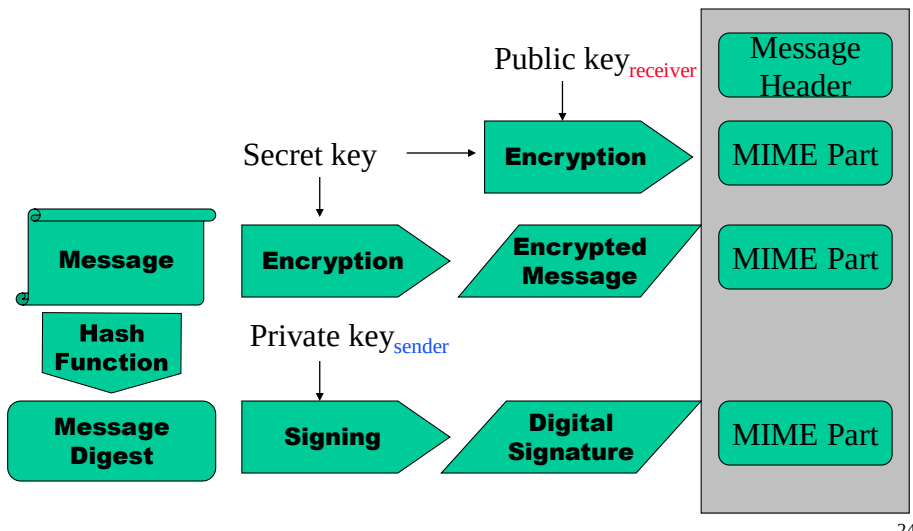
22

Security in S/MIME

- Secure MIME
  - *Secrecy* – Only intended recipient can read the message. (A thick envelope and trustworthy couriers.)
  - *Authenticity* – Recipient knows the message came from the apparent sender. (signature)
  - *Integrity* – Recipient knows the message was not changed en route.
  - *Non-repudiation* – signed document can be used as an evidence.

23

S/MIME operations



24

S/MIME Versions

- Version 2
  - RFC 2311: S/MIME Version 2 Message Specification
  - widely implemented but limited
    - 40-bit keys (RC2,4)
    - RSA-patented asymmetric algorithms
- Version 3
  - RFC 2633 - S/MIME Version 3 Message Specification
    - uses Diffie-Hellman and RSA.
    - support for strong encryption

25

Creating S/MIME Messages

- S/MIME messages are a combination of MIME bodies and CMS (RFC 3369: Cryptographic Message Syntax) objects.
  - The data to be secured is always a canonical MIME entity.
  - The MIME entity and other data, such as certificates and algorithm identifiers, are given to CMS processing facilities which produces a CMS object.
  - The CMS object is then finally wrapped in MIME
- S/MIME formats:
  - one format for enveloped-only data,
  - 2 formats for signed-only data,
  - several formats for signed and enveloped data.

26

MIME File Extension

MIME Type	File Extension
Application/pkcs7-mime (signedData, envelopedData)	.p7m
Application/pkcs7-mime (degenerate signedData "certs-only" message)	.p7c
Application/pkcs7-signature	.p7s
application/x-pkcs7-certificates	.p7b

27

S/MIME Message Format

Certificates-only Message (p7c)

Enveloped-only Message (.p7m)

Signed-only Message
SignedData (p7m), multipart/signed (p7s, clear-signing, preferred).

- Signing and Encrypting
  - sign a message first, then encryption
  - envelope message first (can verify signatures without decryption, but no relation between signature and plaintext)

28

S/MIME – Encrypted Message Format (.p7m)

```
Content-Type: application/pkcs7-mime;
  smime-type=enveloped-data;
  name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfH
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbTrfv=
```

- ASN.1 structure for the EnvelopedData content type

```
version
recipientInfos
encryptedContentInfo
```

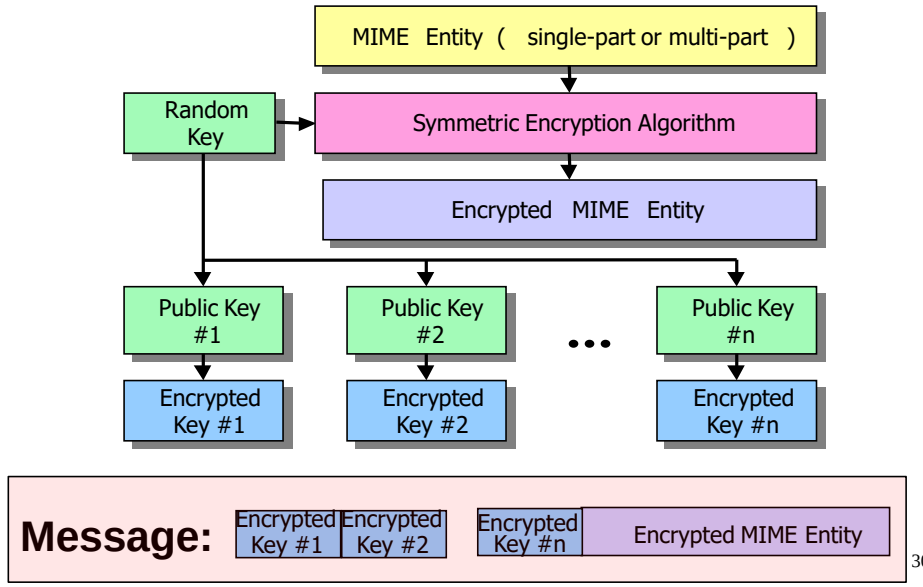
several recipients possible
(encrypted symmetric key)

```
contentType
contentEncryptionAlgorithm
encryptedContent
```

encrypted MIME entity
(single-part or multi-part)

29

Encrypted Message with Multiple Recipients



30

S/MIME -- Signed Message Format I (multipart/signed, .p7s)

```
Content-Type: multipart/signed;
protocol= "   application/pkcs7-signature ";
  micalg=sha1; boundary=boundary1

--boundary1
Content-Type: text/plain

This is a clear-signed message.

--boundary1
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfH
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbTrfv=

--boundary1--
```

MIME entity to be signed

- receivers without S/MIME software can view the message
- changes in transfer can cause signature fail

31

S/MIME – Signed Message Format II (signedData, .p7m)

```
Content-Type: application/pkcs7-mime;
  smime-type=signed-data;
  name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfH
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbTrfv=
```

- MIME content carried within PKCS#7 Signed Data Object
  - This alternative format is used e.g. by Outlook
  - 👍: MIME content is not prone to changes of the transfer encoding enforced by intermediate mail transfer agents.
  - 👎: In order to read the emedded MIME message, the receiver‘s mail client must support S/MIME.

32

S/MIME – Signed and Encrypted Messages

Signing before Encryption

- Signature not visible before decryption (Anonymity)
- Good crypto practise

Encryption before Signing

- Signature(s) can be checked before decryption (Trust)
- **?**

33

S/MIME Key Management

- S/MIME uses X.509 public-key certificates , requires a PKI
- need a directory, key server or CA to get the public key of a recipient
- Recipients use the same mechanisms
- Interoperability – PGP, X.509 certificates
- S/MIME is widely supported (Outlook, Outlook Express, Navigator, Eudora)

34

In Summary

- S/MIME is secure messaging using MIME formats
- Uses both public key and symmetric encryption
- Interoperability is still a problem
- Dependent upon certificate management
- S/MIME Internet task force: www.imc.org/ietf-smime/index.html
- Relationship between S/MIME and PGP/MIME: www.imc.org/smime-pgpmime.html

35

Summary

- PGP
- S/MIME

- Next:
  - SSL, web-security HTTPS
  - IPSEC

Exercise 13

1. **Install certificate, send encrypted and signed email to laix@sjtu.edu.cn**
   - Get free certificate from
     - www.startssl.com
     - www.thawte.com
     - www.comodo.com
     - www.verisign.com (1 month)
   - or anywhere you can
   - my certificate is on file server

2. Describe the similarities and differences between PGP and S/MIME.

- Deadline: one week