Bachelor of Computer Science

SCS2214 - Information System Security

Handout 6 - eMail and Document Security

Kasun de Zoysa
kasun@ucsc.cmb.ac.lk

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

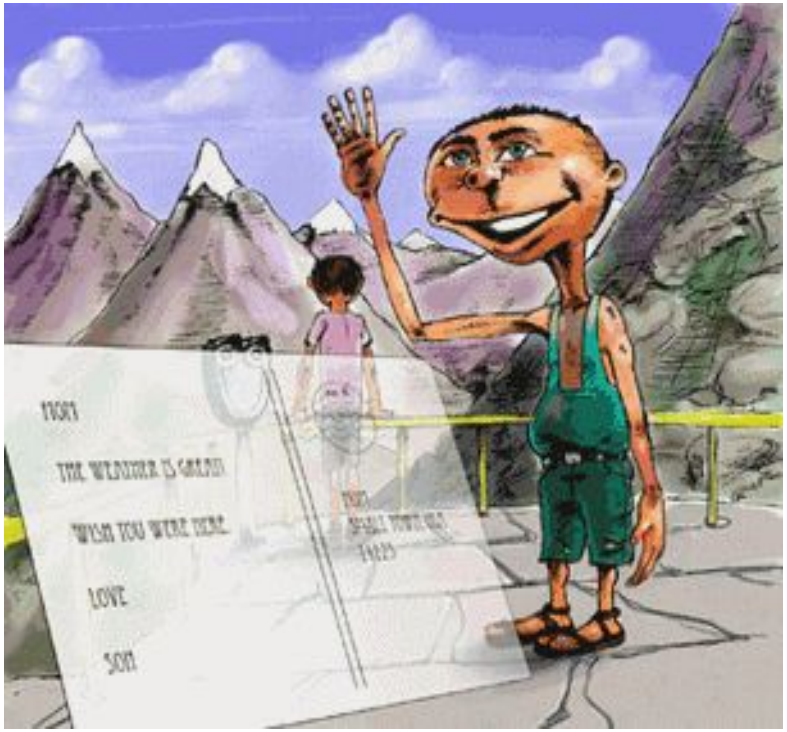
Security Wisdom

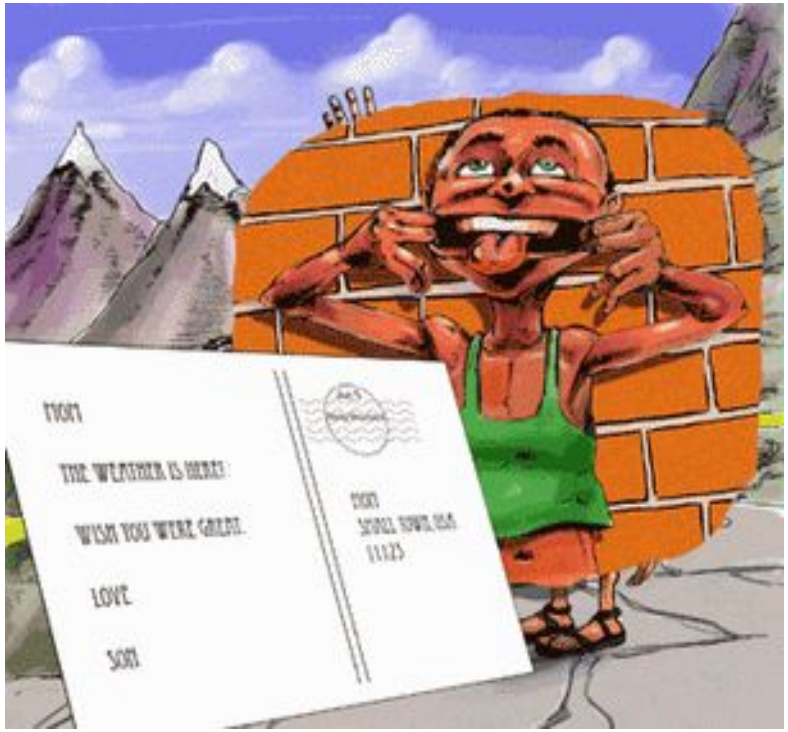
- **Popular Myth**:
  Information Security depends on...
  - firewalls
  - SSL
  - Virus Scanners or IDS

- **Unpopular Reality**:
  In a large, Information security is not achieved by above technologies.

Email is in the Clear

Email – A Postcard Written in Pencil





http://www.cert.org/homeusers/email_postcard.html

E-mail Security

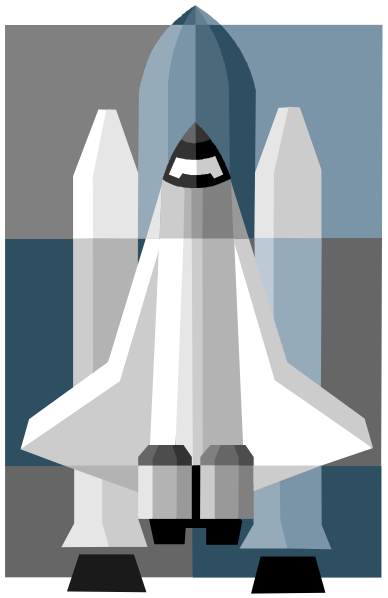
- Pretty Good Privacy (PGP) (www.pgp.com)
  - Philip R. Zimmerman is the creator of PGP.
  - PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.
- S/MIME
  - Secure/Multipurpose Internet Mail Extension
  - S/MIME will probably emerge as the industry standard.
  - PGP for personal e-mail security

Why Is PGP Popular?

- It is availiable free on a variety of platforms.
- Based on well known algorithms.
- Wide range of applicability
- Not developed or controlled by governmental or standards organizations

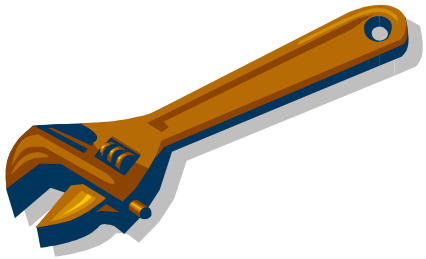
Operational Description

- Consist of five services:
  - Authentication
  - Confidentiality
  - Compression
  - E-mail compatibility
  - Segmentation

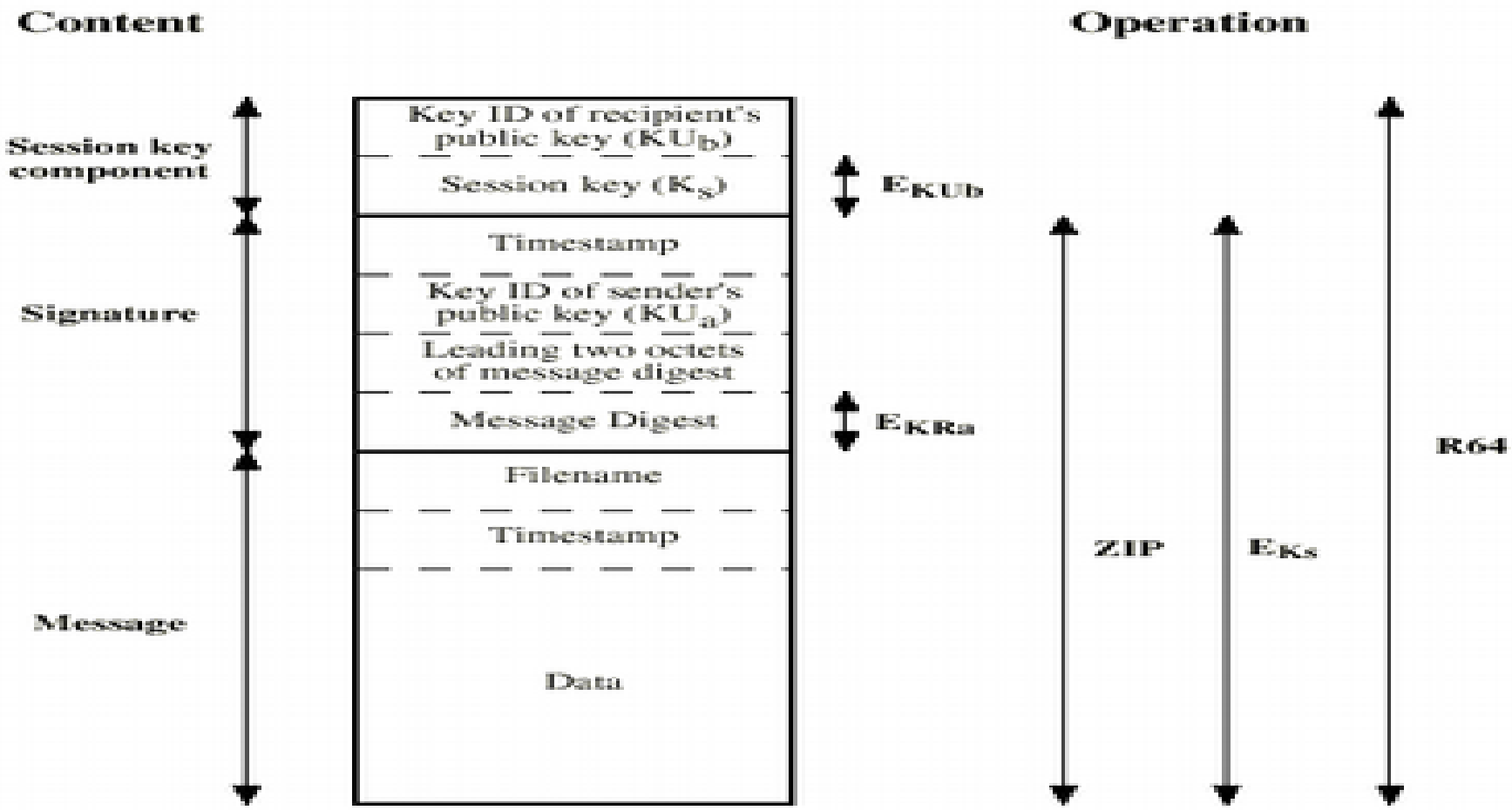


PGP Services

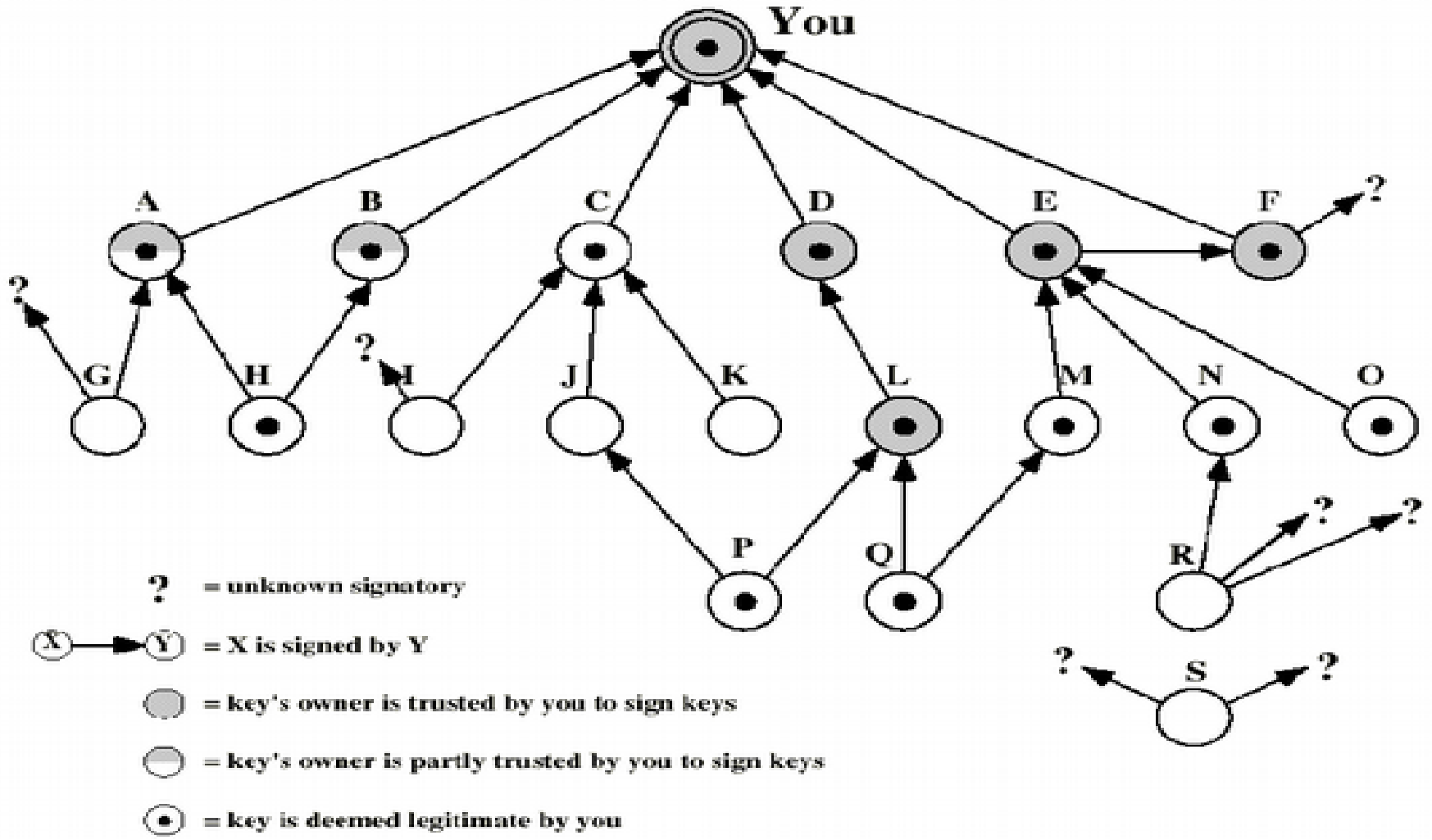
Function	Algorithm Used
Digital Signature	DSS/SHA or RSA/SHA
Message Encryption	CAST or IDEA or three-key triple DES with Diffie-Hellman or RSA
Compression	ZIP
E-mail Compatibility	Radix-64 conversion
Segmentation	-



Format of PGP



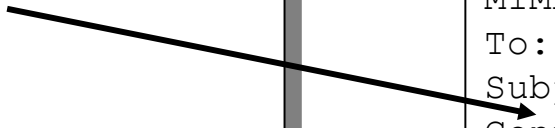
PGP Public Keys



MIME content (mixed)

MIME content headers

text/plain
text/richtext
multipart/mixed
multipart/parallel
multipart/alternative
multipart/digest
message/rfc822
message/partial
message/external-body
image/jpeg
image/gif
video/mpeg
audio/basic
application/postscript
application/octet-stream



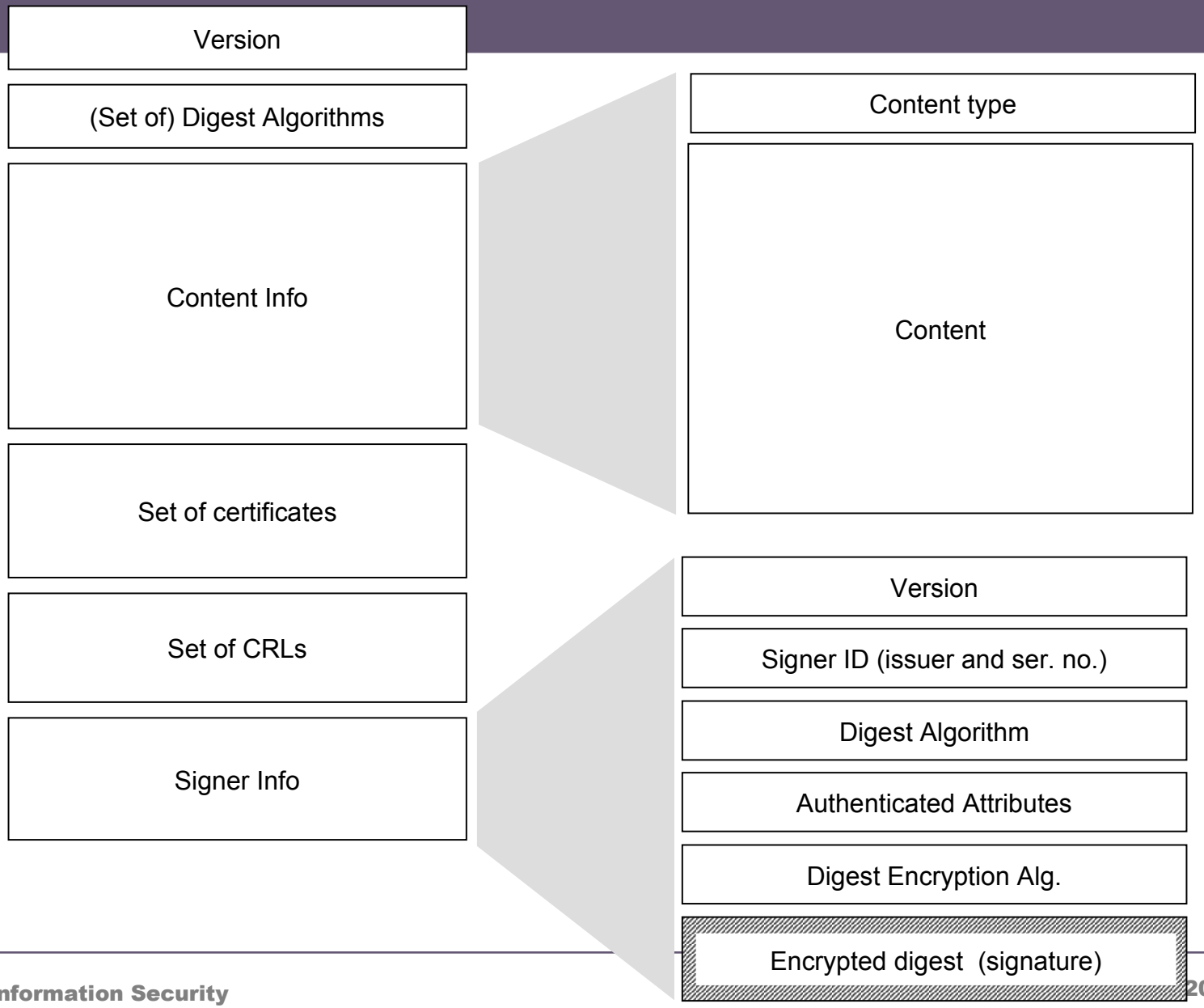
MIME content headers

```
From: Dr William Buchanan
<w.buchanan@napier.ac.uk>
MIME-Version: 1.0
To: w.buchanan@napier.ac.uk
Subject: Any subject
Content-Type: multipart/mixed;
boundary="boundary name"
This part of the message will be ignored.
-- boundary name
Content-Type: multipart/mixed;
boundary="boundary name"
This is the first mail message part.
-- boundary name
And this is the second mail message part.
-- boundary name --
```

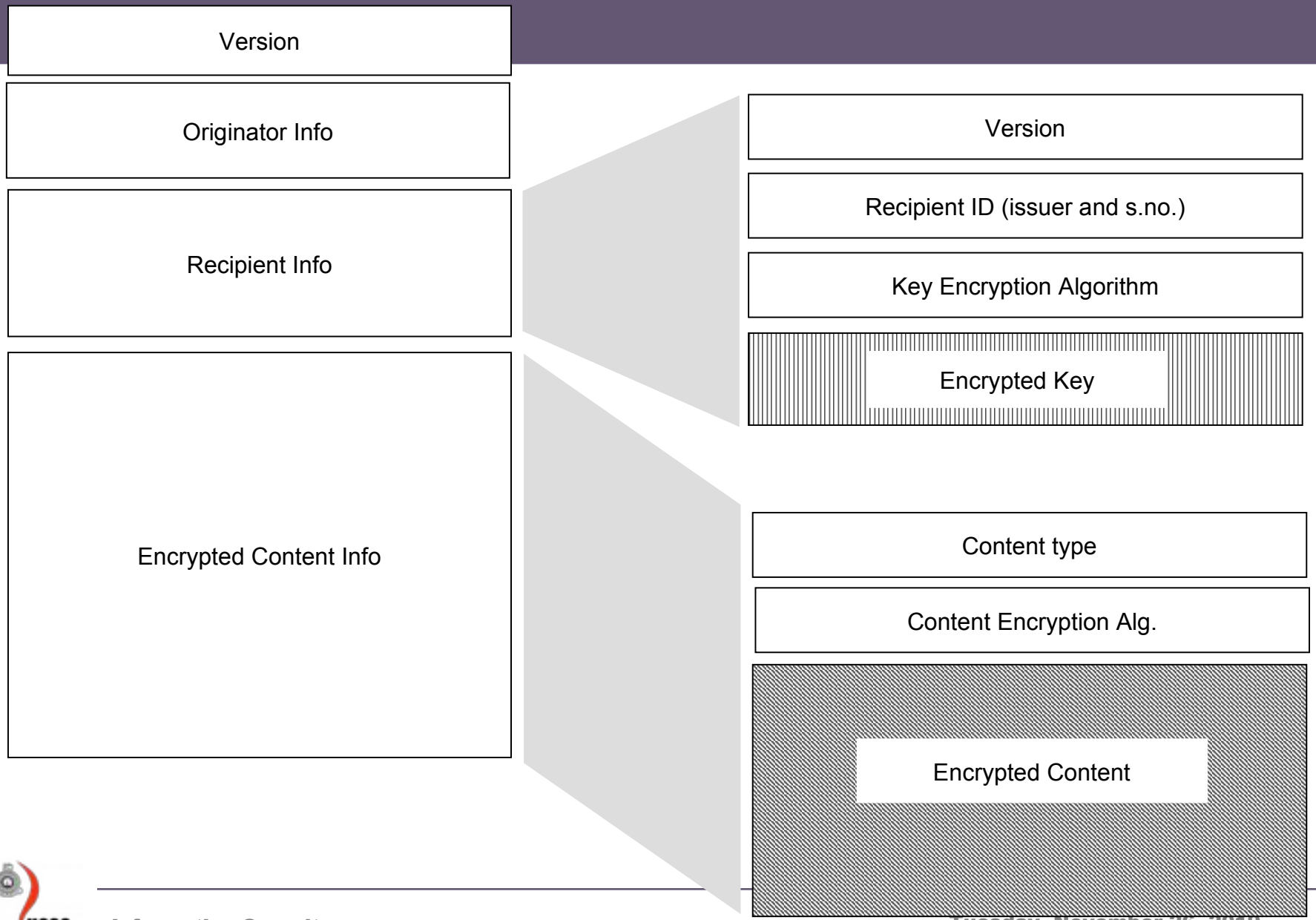
Securing a MIME entity

- MIME entity is prepared according to the normal rules for MIME message preparation
- prepared MIME entity is processed by S/MIME to produce a PKCS object
- the PKCS object is treated as message content and wrapped in MIME

PKCS7 “signed data”



PKCS7 “enveloped data”



Enveloped data – Example

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

rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GhIGfHfYT6
7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H
f8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
0GhIGfHfQbnj756YT64V

Clear-signed data – Example

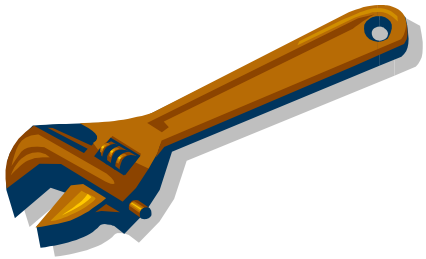
```
Content-Type: multipart/signed; protocol="application/pkcs7-signature";
  micalg=sha1; boundary=boundary42

--boundary42
Content-Type: text/plain

This is a clear-signed message.

--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756

--boundary42--
```

S/MIME Functions

- Enveloped Data: Encrypted content and encrypted session keys for recipients.
- Signed Data: Message Digest encrypted with private key of “signer.”
- Clear-Signed Data: Signed but not encrypted.
- Signed and Enveloped Data: Various orderings for encrypting and signing.

Algorithms Used

- Message Digesting: SHA-1 and MDS
- Digital Signatures: DSS
- Secret-Key Encryption: Triple-DES, RC2/40 (exportable)
- Public-Private Key Encryption: RSA with key sizes of 512 and 1024 bits, and Diffie-Hellman (for session keys).



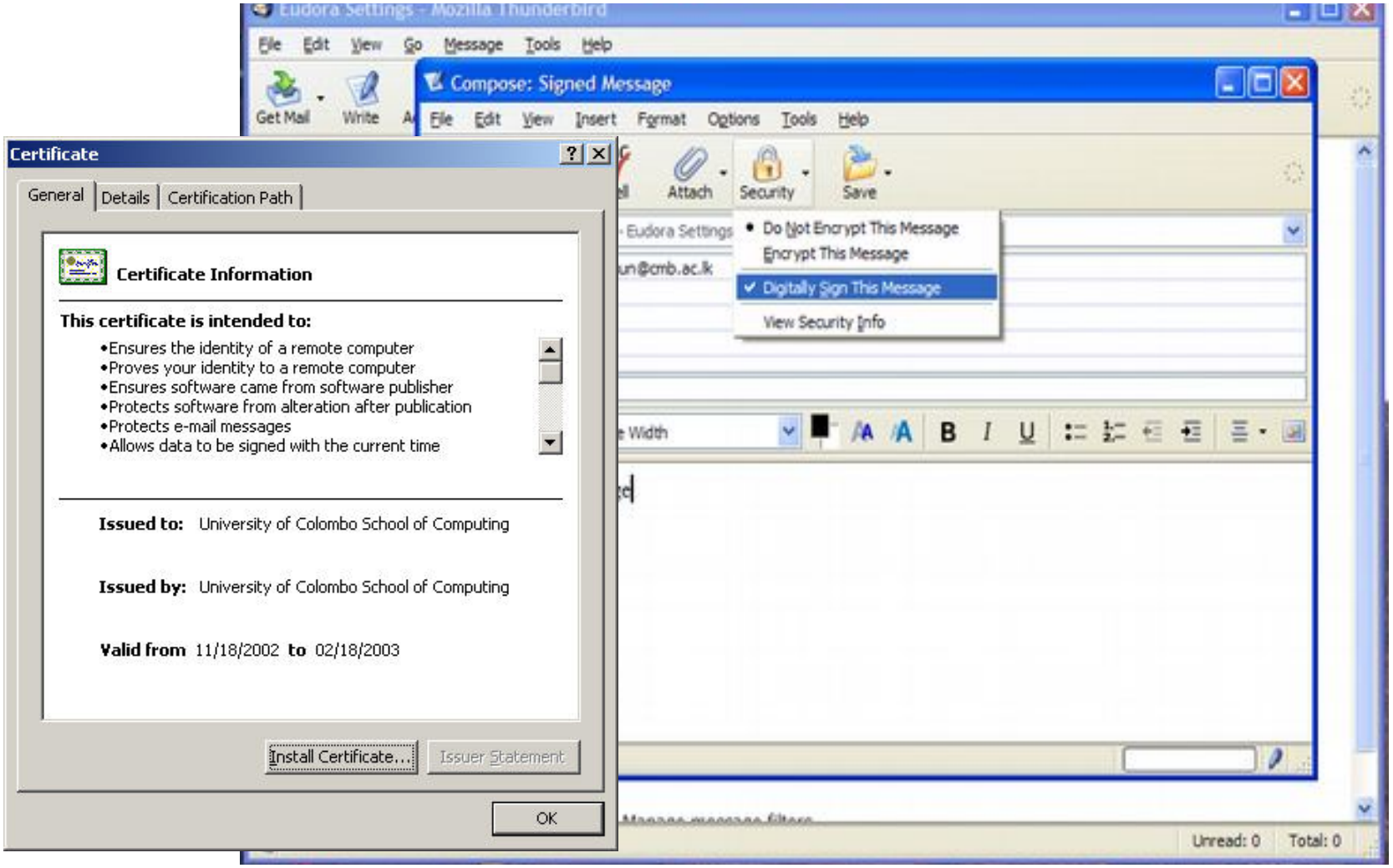
User Agent Role

- S/MIME uses Public-Key Certificates - X.509 version 3 signed by Certification Authority
- Functions:
  - Key Generation - Diffie-Hellman, DSS, and RSA key-pairs.
  - Registration - Public keys must be registered with X.509 CA.
  - Certificate Storage - Local (as in browser application) for different services.
  - Signed and Enveloped Data - Various orderings for encrypting and signing.

User Agent Role

- Example 1 : Verisign (www.verisign.com)
  - Class-1: Buyer's email address confirmed by emailing vital info.
  - Class-2: Postal address is confirmed as well, and data checked against directories.
  - Class-3: Buyer must appear in person, or send notarized documents.
- Example 2: UCSC CA (ca.cmb.ac.lk)

Sample Screens



Phishing

- Phishing is an illegal activity that uses social engineering techniques to trick people into giving out personal information.
- Typically you will receive an email that appears to be from a legitimate business or organization asking for verification of personal or financial information.

Phishing Email

- Information asked for in a phishing email may include:
  - Username, userid, email id, email identity
  - Password
  - ID number
  - Birthdate
- Or there may just be a link to click on that takes you to an official looking web site to enter information.

Phishing Technique

- Link manipulation
  - Technical deception designed to make a link in an email and the spoofed website it leads to, appear to belong to the spoofed organization.
- Spoofed website
  - Looks almost exactly like the real thing
- Website forgery
  - A spoofed website that uses JavaScript to alter the address bar to appear legitimate.
- Filter evasion
  - Misspelled words and images instead of text are used to evade anti-phishing filters.

Phishing Example

Foreign lottery scams are common

MEGAFORTUNE LOTTERY INTERNATIONAL
INTERNATIONAL PROMOTION/PRIZE AWARD DEPT.
REF: MLI/231-ILGI0431/04
BATCH: IPD/17/096/PTNL
RE: WINNING FINAL NOTIFICATION

Sir/Madam, We are pleased to inform you of the result of the Lottery Winners International programs held on the 17th of January 2005. Your e-mail address attached to ticket number 20511465897-6291 with serial number 472-971103 drew lucky numbers 8-66-97-22-71-64 which consequently won in the 3rd category, you have therefore been approved for a sum pay out of US$ 500,000 000. (five hundred Thousand United States Dollars). CONGRATULATIONS!!!

Due to mix up of some numbers and names, we ask that you keep your winning information very confidential till your claims has been processed and your prize/money Remitted toyou. This is part of our security protocol to avoid double claiming and unwarranted abuse of this program by some participants. All participants were selected through a computer ballot system drawn from over 200,000,000 company and 300,000,000 individual email addresses and names from all over the world. This promotional program takes place annually. We hope with part of your winning you will take part in our next year USD10 million international lottery. To file for your claim, please contact our/your fiducial agent MR.PHILIP GERE of the, MECURY TRUST AGENT TEL: +31-621-488-708 FAX: +31-645-236-856 Email: philipgere900@netscape.net Note that all winning must be claimed not later than 3rd of February 2005. After this date all unclaimed, funds will be included in the next stake.

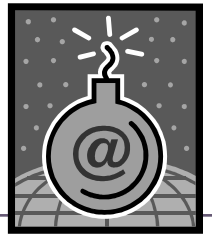
Please note in order to avoid unnecessary delays and complications please remember to quote your reference number and batch numbers in all correspondence. Furthermore, should there be any change of address do inform our agent as soon as possible. Congratulations once more from our members of staff and thank you for being part of our promotional program.

Note: Anybody under the age of 18 is automatically disqualified.

Sincerely yours,
Mrs Ellen Kloos,
Lottery Coordinator
. REPLY EMAIL TO philipgere900@netscape.net

Attachments

- Computer viruses and other malicious software are often spread through email attachments.
- If a file attached to an email contains a virus, it is often launched when you open (or double-click) the attachment.
- Don’t open email attachments unless you know whom it is from and you were expecting it.



Should you open attachments?

If it is suspicious, do not open it!

- What is suspicious?
  - Not work-related.
  - The email containing the attachment was not addressed to you, specifically, by name.
  - Incorrect or suspicious filename.
  - Unexpected attachments.
  - Attachments with suspicious or unknown file extensions (e.g., .exe, .vbs, .bin, .com, .pif, or .zzx)
  - Unusual topic lines: “Your car?”; “Oh!”; “Nice Pic!”; “Family Update!”; “Very Funny!”

Links in emails?

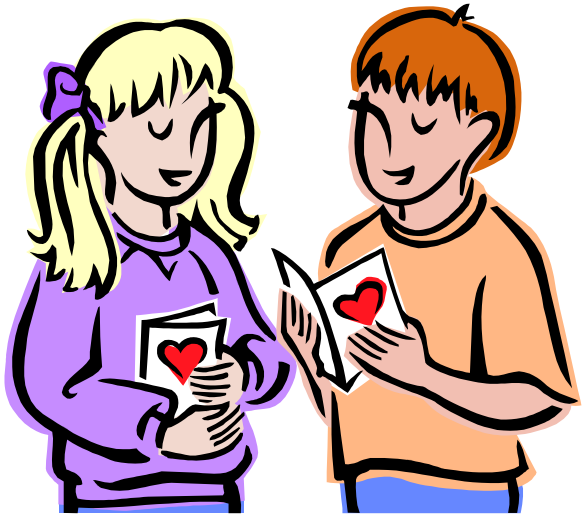
- Approach links in an email with caution.
- They might look genuine, but they could be forged.
- Copy and paste the link to your web browser.
- Type in the address yourself.
- Or even Google the company and go to their website from the search results.

Email best practices

- Use the BCC field when sending to large distribution lists.
  - Protects recipients email addresses
  - Prevents Reply to All issues
- Avoid use of large distribution lists unless legitimate business purpose.
  - E.g., All Faculty/Staff list
- Beware of Reply to All button
- Don’t forward chain email letters.

What is spam?

– Spam is difficult to define. In fact, there is no clear definition.
–Generally spam is like junk mail, you get it whether you want it or not.



Spam and viruses are ever-increasing security issue for anyone with an email account. Unsolicited junk mail steals system resources and leads to lost productivity, storage, and bandwidth. Spam can also be hostile and contain virus and Trojan horses.

What is spam?

- Spam is anonymous, unsolicited junk email sent indiscriminately to huge numbers of recipients.
- What for?
  - Advertising goods and services (often of a dubious nature)
  - Quasi-charity appeals
  - Financial scams
  - Chain letters
  - Phishing attempts
  - Spread malware and viruses

How do spammers harvest email addresses?

– **From posts to UseNet with your email address**

When you send email to UseNet, for example your address will be available to simple, automatic programs that are looking at the header which contain email address (From:, Reply-To:, etc). Spammers may easily build huge lists of potential targets.

– **From mailing lists.**

Spammer's regularly harvesting email addresses from poorly configured mailing lists.

How do spammers harvest email address?

– **From web pages**

Spammers have programs, which spider through web pages, check mail to: link, and collect the email address.

– **From various web forms**

Some site requests various details via web forms. E.g.; registration forms and guest books. Some of these sites collect the information and sell it to the spammers.

Existing anti-spamming techniques

Blacklist/Whitelist:
In blacklist technique, list of domains, mail serves, and email address are defined. Then e-mails come from above address will not be allowed. Whitelist technique is the opposite of blacklist technique.

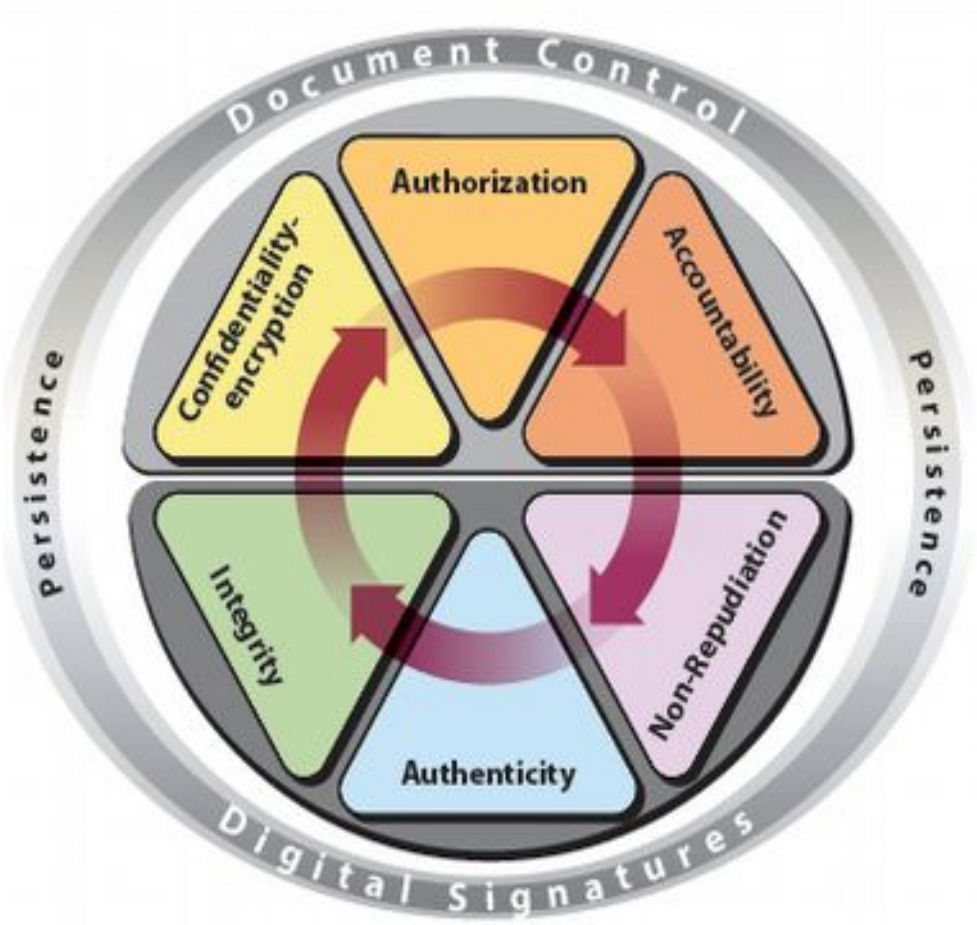
Integrity Check:
Mail can be check and filter if it has the characteristic of spam. However, identifying the characteristics of a spam is very difficult.

Existing anti-spamming techniques

Reverse DNS Lookup:
In this technique, when receiving a mail, the IP address of the sending sever is taken and DNS lookup is performed on that address to check whether the e-mail address is a real one or a bogus one.

Rules-based Filtering:
In rule-based filtering, mails are examined according to the specific rules. These rules are defined according to the patterns often used by spammers.

Document Security



Six key criteria for providing persistent document security

Document security Requirement

- **The following criteria define persistent document security:**
  - **Confidentiality**—Who should have access to the document?
  - **Authorization**—What permissions does the user have for working with the document?
  - **Accountability**—What has the recipient done with the document?
  - **Integrity**—How do you know if the document has been altered?
  - **Authenticity**—How do you know where the document came from?
  - **Non-repudiation**—Can the signatory deny signing the document?

Searching

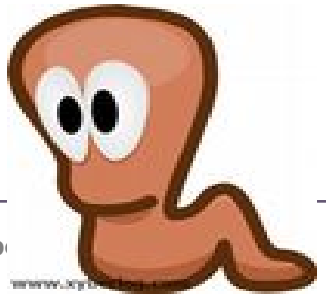
The use of modern search engines, such as Google, MSN, or Yahoo, makes it easy to find specific file types by searching for their extensions: .doc, .xls, and .ppt for Word, Excel, and PowerPoint, respectively. The use of specific terms, like clinical trial, religion, or credit card number, will target the search and may reveal hidden, potentially sensitive data.

Cloud

- Cloud computing is a new resource that is enables convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned.

- It has great scalability and cost-modulation advantages.

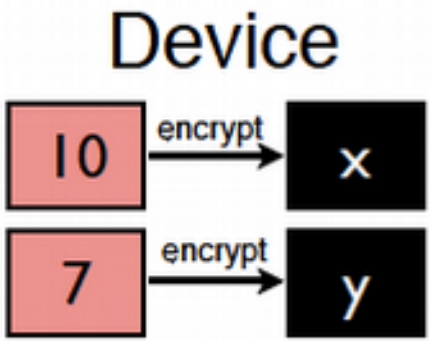
- **However it brings about new security concerns since documents are not physically controlled within the user enterprise.**



Homomorphic Encryption

(Gentry, 2009)

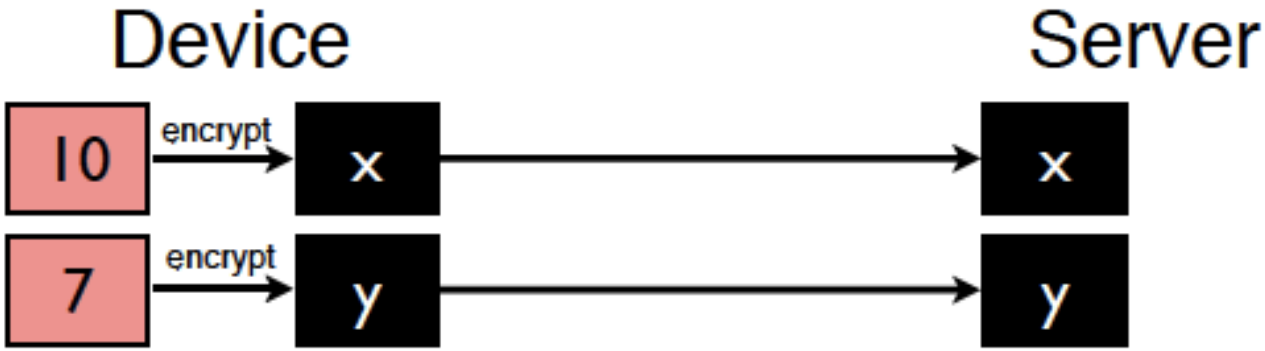
- Take a sensor value S, encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 2009)

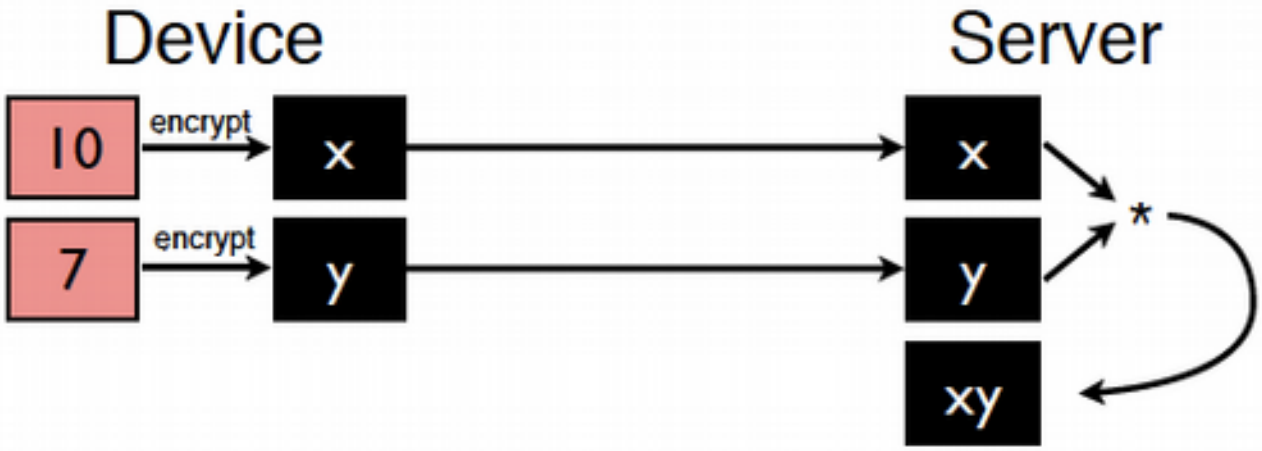
- Take a sensor value S, encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 2009)

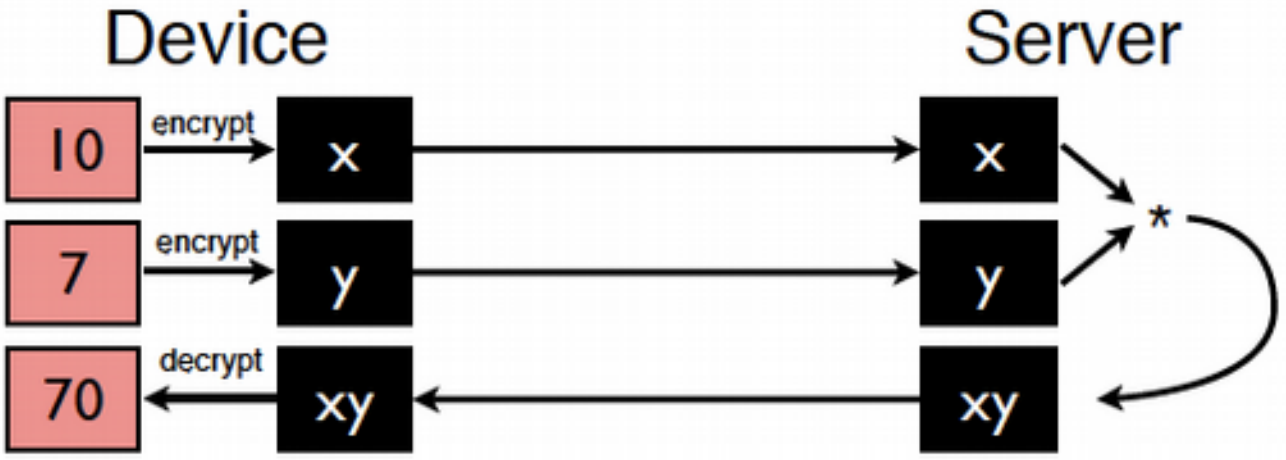
- Take a sensor value S, encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 2009)

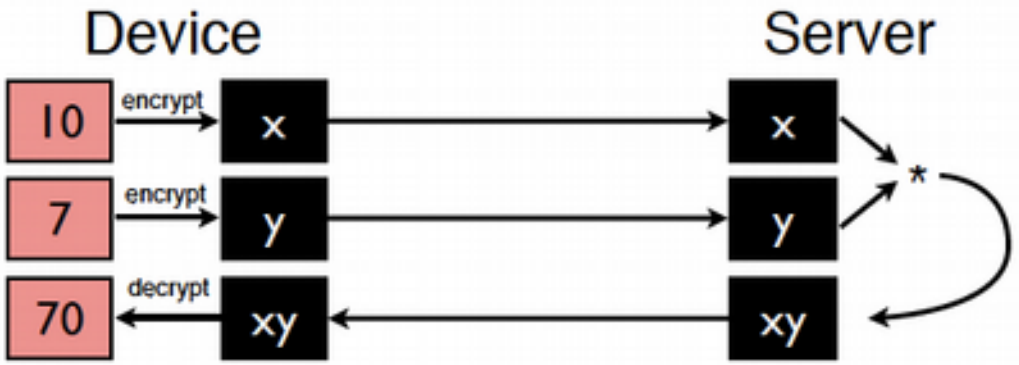
- Take a sensor value S, encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 2009)

- Take a sensor value *S*, encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



- So confidential analytics possible, but not yet practical
  - Computations on S_e are 1,000,000 slower than computations on *S*
- But can be fast for *specific* computations (e.g., *)

Cloud Security

"If you reveal your secrets to the wind you should not blame the wind for revealing them to the trees."

Kahil Gibran, *Artist & poet in United States (1883–1931)*

If you reveal your confidential data to the Internet/cloud you should not blame Internet/cloud for revealing them to Kasun

Discussion