EMAIL SECURITY

Budi Rahardjo

2025

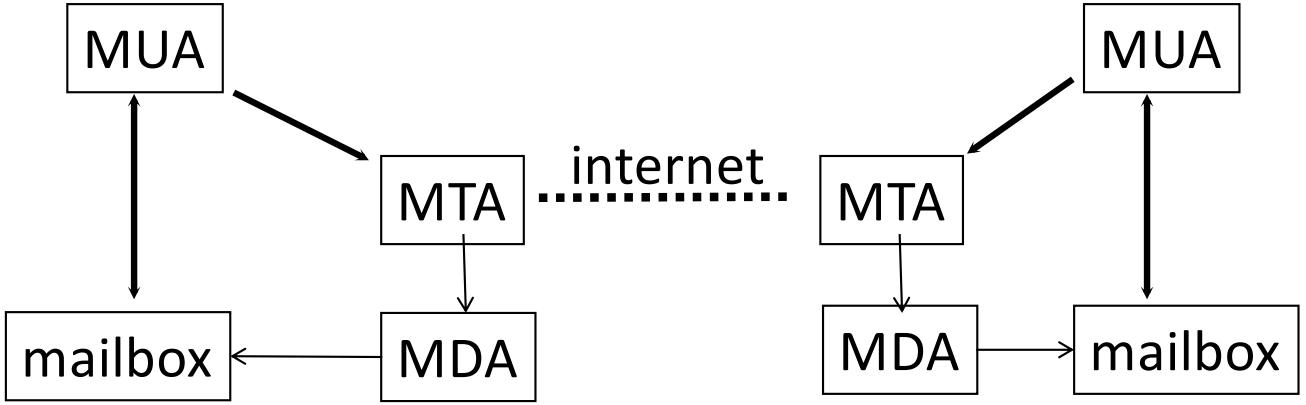
Email

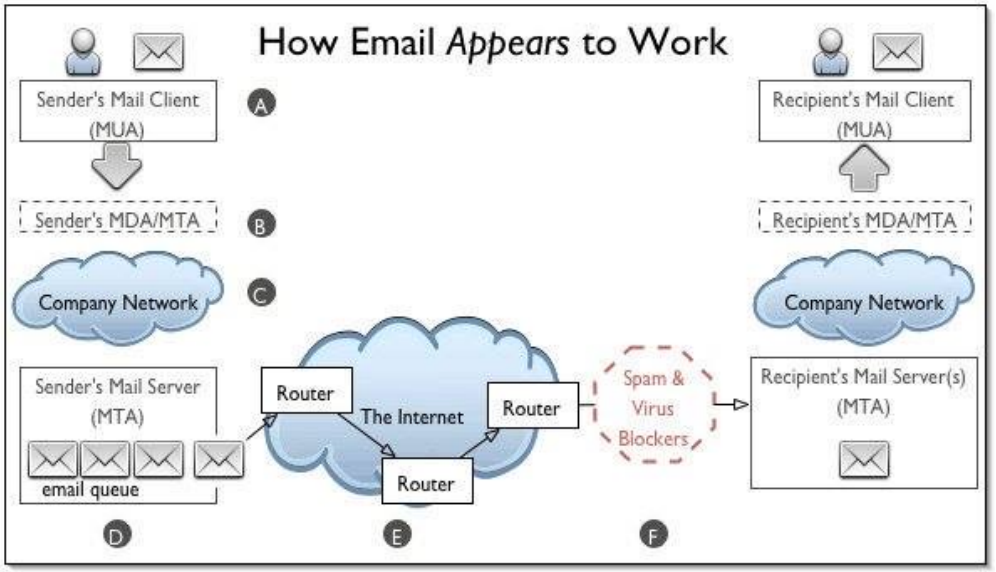
- (masih) merupakan aplikasi utama di internet
- Digunakan sebagai basis identitas
- untuk menerima OTP
- (by default) email tidak aman

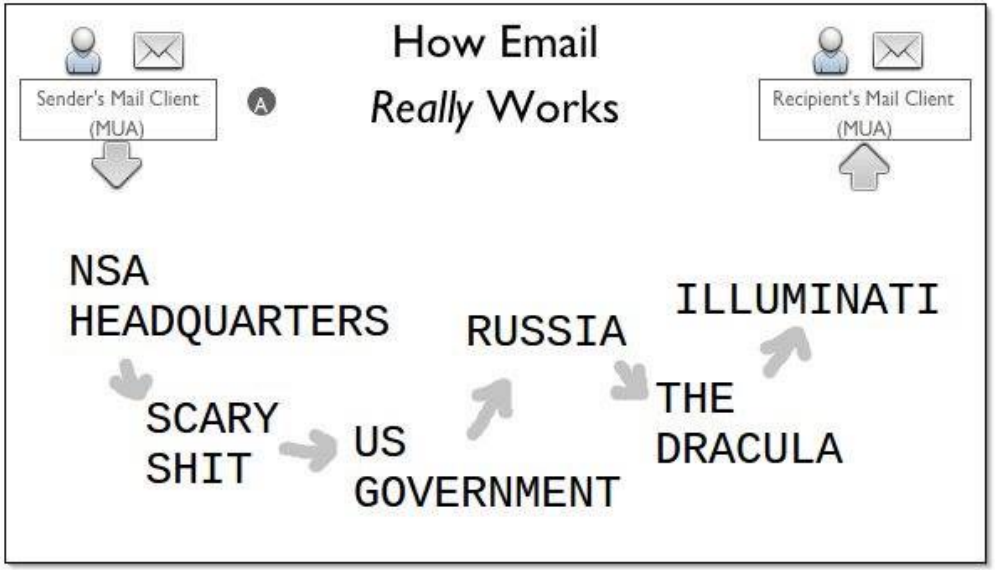
Struktur Sistem Email

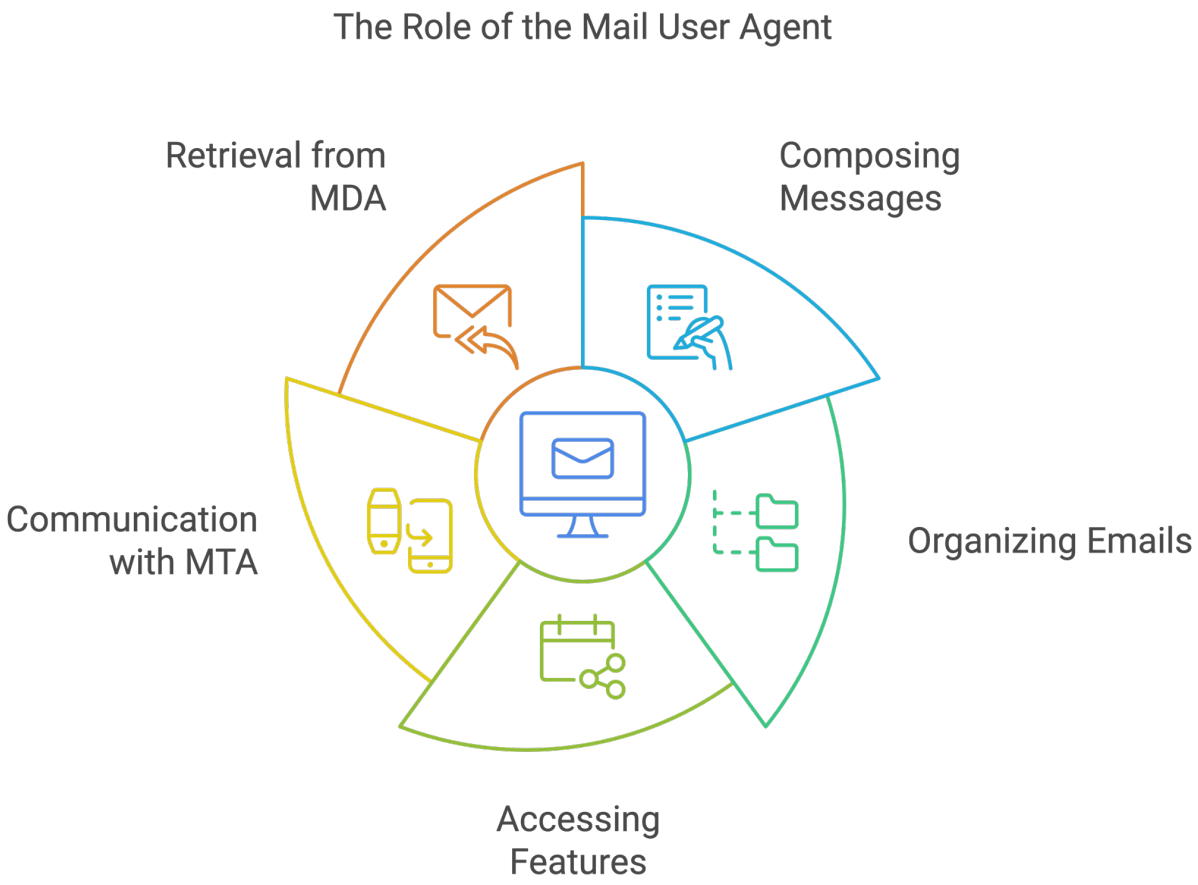
- **Mail User Agent (MUA)**
  Berhubungan dengan pengguna.
  Contoh: Outook, Thunderbird, mutt, ...
- **Mail Transfer Agent (MTA)**
  Yang melakukan pengiriman email.
  Contoh: sendmail, qmail, postfix, exchange
- Mail Delivery Agent (MDA)
  Yang menyimpan email ke mailbox penerima

topologi email



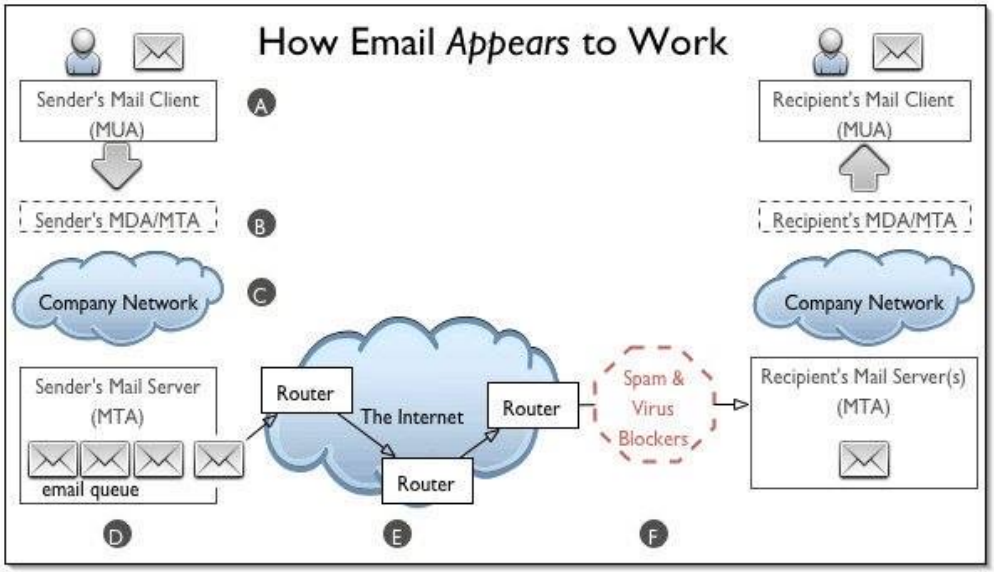

How Email *Appears* to Work
Sender's Mail Client (MUA)
A
Recipient's Mail Client (MUA)
Sender's MDA/MTA
B
Recipient's MDA/MTA
Company Network
C
Company Network
Sender's Mail Server (MTA)
email queue
Router
The Internet
Router
Router
Spam & Virus Blockers
Recipient's Mail Server(s) (MTA)
D
E
F

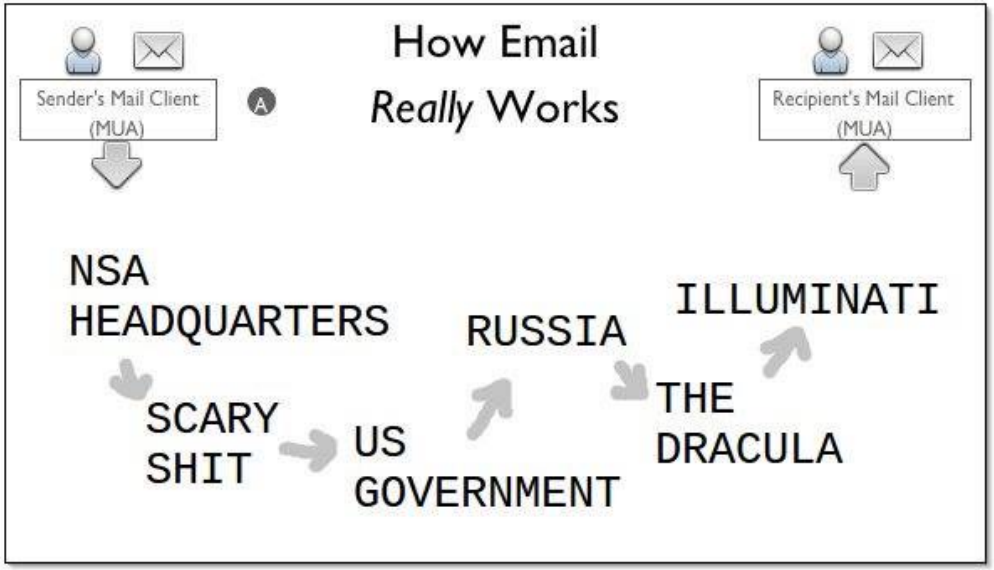

How Email
Really Works
Sender's Mail Client (MUA)
A
Recipient's Mail Client (MUA)
NSA HEADQUARTERS
SCARY SHIT
US GOVERNMENT
RUSSIA
THE DRACULA
ILLUMINATI


The Role of the Mail User Agent
Retrieval from MDA
Composing Messages
Communication with MTA
Organizing Emails
Accessing Features

Serangan Terhadap Email

- Dapat disadap
  - Dapat disadap (tcpdump, mailsnarf)
- Diubah, dipalsukan
  - Contoh email palsu
- Mailbomb
  - Skrip mailbom
- Lain-lain
  - Disisipi virus/malware / ransomware
  - Spamming
  - Server digunakan sebagai mail relay


How Email *Appears* to Work
Sender's Mail Client (MUA)
Recipient's Mail Client (MUA)
Sender's MDA/MTA
Recipient's MDA/MTA
Company Network
Company Network
Sender's Mail Server (MTA)
email queue
Router
The Internet
Router
Router
Spam & Virus Blockers
Recipient's Mail Server(s) (MTA)
A
B
C
D
E
F


How Email
Really Works
Sender's Mail Client (MUA)
Recipient's Mail Client (MUA)
A
NSA HEADQUARTERS
RUSSIA
ILLUMINATI
SCARY SHIT
US GOVERNMENT
THE DRACULA

Format Email

- Didefinisikan oleh RFC 822
  ("Standard for the format of Arpa Internet Text Messages"), kemudian digantikan oleh RFC 2822 "Internet Message Format"
  - **header**
    Seperti amplop, berisi informasi tentang alamat pengirim dan yang dituju.
  - **body**
    Isi dari surat. Dipisahkan dari header dengan sebuah baris kosong.

header – body

```
From: Budi Rahardjo <budi@cert.or.id>
To: kelasBR@itb.ac.id
Subject: Kuliah hari ini dibatalkan

Kelas hari ini dibatalkan dan akan
digantikan pada hari lain.

-- budi
--
```

```
Received: from nic.cafax.se (nic.cafax.se [192.71.228.17])
   by alliance.globalnetlink.com (8.9.1/8.9.1) with ESMTP id QAA31830
   for <budi@alliance.globalnetlink.com>; Mon, 26 Mar 2001 16:18:01 -
   0600
Received: from localhost (localhost [[UNIX: localhost]])
   by nic.cafax.se (8.12.0.Beta6/8.12.0.Beta5) id f2QLSJVM018917
   for ietf-provreg-outgoing; Mon, 26 Mar 2001 23:28:19 +0200 (MEST)
Received: from is1-55.antd.nist.gov (is1-50.antd.nist.gov
   [129.6.50.251])
   by nic.cafax.se (8.12.0.Beta5/8.12.0.Beta5) with ESMTP id
   f2QLSGiM018912
   for <ietf-provreg@cafax.se>; Mon, 26 Mar 2001 23:28:17 +0200 (MEST)
Received: from barnacle (barnacle.antd.nist.gov [129.6.55.185])
   by is1-55.antd.nist.gov (8.9.3/8.9.3) with SMTP id QAA07174
   for <ietf-provreg@cafax.se>; Mon, 26 Mar 2001 16:28:14 -0500 (EST)
Message-ID: <04f901c0b63b$16570020$b9370681@antd.nist.gov>
From: "Scott Rose" <scottr@antd.nist.gov>
To: <ietf-provreg@cafax.se>
Subject: confidentiality and transfers
Date: Mon, 26 Mar 2001 16:24:05 -0500
MIME-Version: 1.0
X-Mailer: Microsoft Outlook Express 5.50.4133.2400
Sender: owner-ietf-provreg@cafax.se
Precedence: bulk
```

Bagaimana Dengan Berkas Biner

- Dikonversikan ke bentuk ASCII
  - UUEncode & UUDecode
  - Base64
  - Standar MIME Multimedia Extension (RFC) untuk menyisipkan ke dalam email

Penyadapan Email

- Masalah Confidentiality
- Email seperti kartu pos, bukan seperti surat tertutup
- Email ”meloncat” (hopping) dari satu MTA ke MTA lainnya
- Pada awalnya menggunakan protokol yang mudah disadap (SMTP)
- Penyadapan dapat dilakukan pada jaringan & MTA
- Proteksi: PGP (Pretty Good Privacy)

Email Palsu

- Mudah membuat email palsu dengan membuat header sesuka kita
- Email palsu ini kemudian dikirimkan via MTA atau langsung via SMTP
- Tapi, aktivitas tercatat di server dalam berkas log

Email Palsu

Isi berkas "email-palsu.txt"

```
To: siapasaja@dimanasaja.com
From: saya@hotmail.com
Subject: email palsu

Saya akan coba kirim email palsu. Perhatikan
header dari email ini.
```

```
unix$ /usr/sbin/sendmail user01@training < email-palsu.txt
```

Email via SMTP

```
Unix% telnet mailserver 25
HELO localhost
MAIL FROM: <saya@hotmail.com>
RCPT TO: <user01@mailserver.domain>
DATA
354 Enter mail, end with "." on a line by itself
To: haha@hotmail.com
From: hoho@hotmail.com
Subject: palsu

nih palsu
.

250 HAA20290 Message accepted for delivery
QUIT
```

Disisipi Malware

- Email sering dijadikan media yang paling efektif untuk menyebarkan malware (melalui attachment)
- Isi email pada mulanya tidak diperiksa oleh firewall (karena firewall konvensional bukan pada layer aplikasi)
- Email langsung menuju pengguna yang seringkali teledor. (The weakest link)
- Email client langsung mengeksekusi program berdasarkan jenis berkas yang diterima untuk kenyamanan pengguna. Kepercayaan ini diabuse oleh virus
- Solusi:
  - Menggunakan anti virus dengan data terbaru
  - Tidak memperkenankan email client langsung menjalankan aplikasi
  - Melakukan pemeriksaan virus pada mail server

Spamming

- Mengirim satu email ke banyak orang
- [Slide SPAM]

Mailbomb

- Mengirimkan banyak email ke satu orang
  - Menghabiskan bandwidth dan mailbox
- Proteksi:
  - membatasi ukuran email,
  - quota disk (di direktori *spool*),
  - menggunakan filter khusus yang mendeteksi duplikasi isi (content) email

Contoh Skrip Mailbomb

```
#! /usr/bin/perl
#
for ($i=0; $i < 10 ; $i++) {
    system("/usr/sbin/sendmail target@somedomain.com < junkmail.txt");
}
```

Mail Relay

- Menggunakan server orang lain untuk mengirimkan email
- Akibat:
  - Bandwidth orang lain (pemilik server yang dapat di-relay) terpakai untuk mengirim email tersebut (yang biasanya jumlahnya sangat banyak)
  - Mengelabui penerima email dengan alamat palsu
  - Kena sanksi (dan terfilter) karena server kita digunakan untuk melakukan spamming

Proteksi Mail Relay

- Mail Abuse Prevention System
  http://mail-abuse.org/
- ORBZ – Open Relay Blackhole Zone
  http://www.orbz.org/
- ORDB – Open Relay Database
  http://www.ordb.org/
- RBL-type services
  http://www.ling.helsinki.fi/users/reriksso/rbl/rbl.html
- SPF

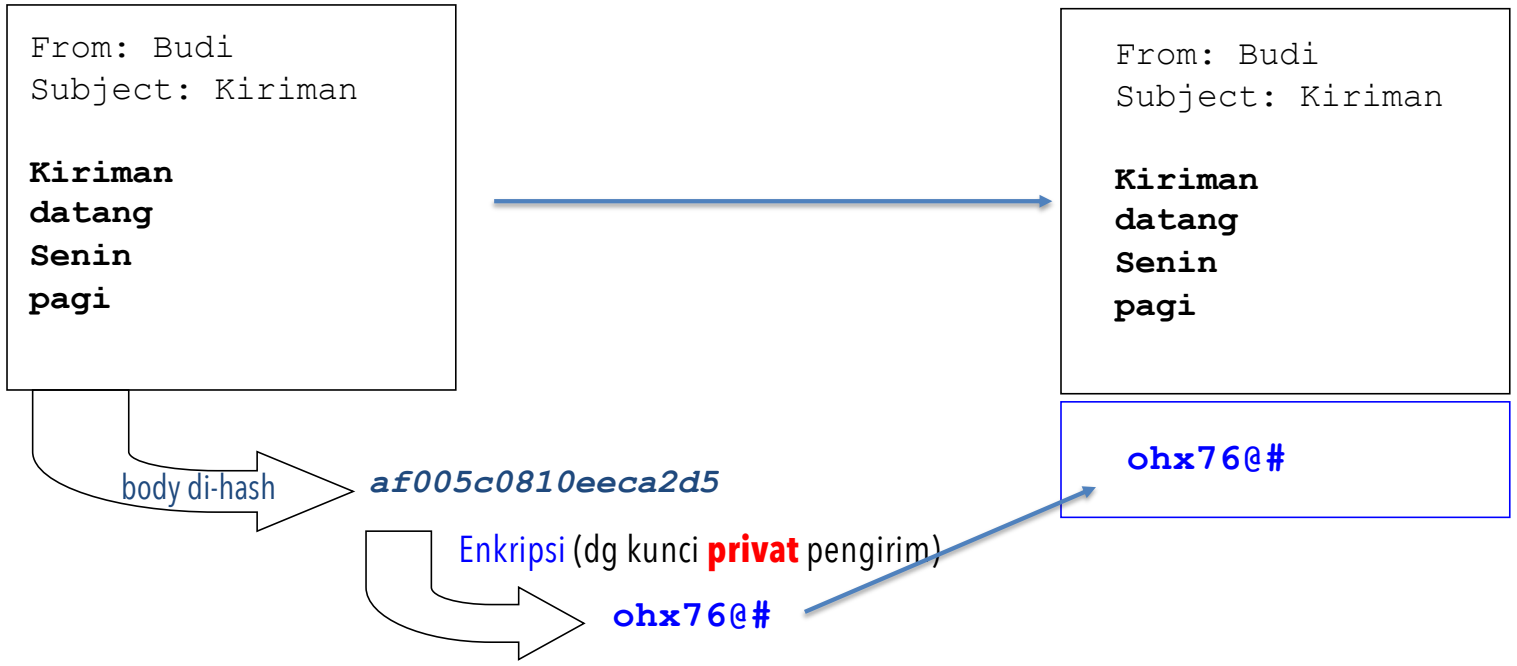
Konsep Public Key Infrastructure

- [slide terpisah]
- Adanya kriptografi kunci public (public key cryptosystem)

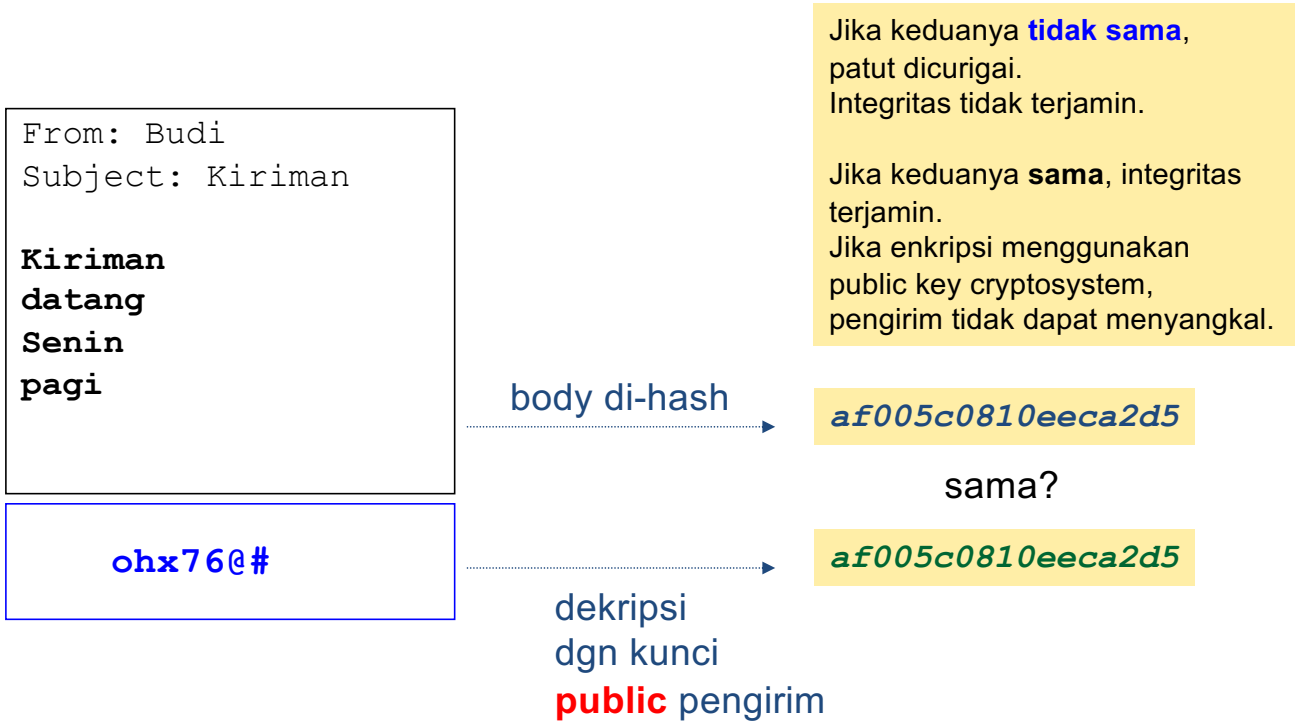
Signed Email

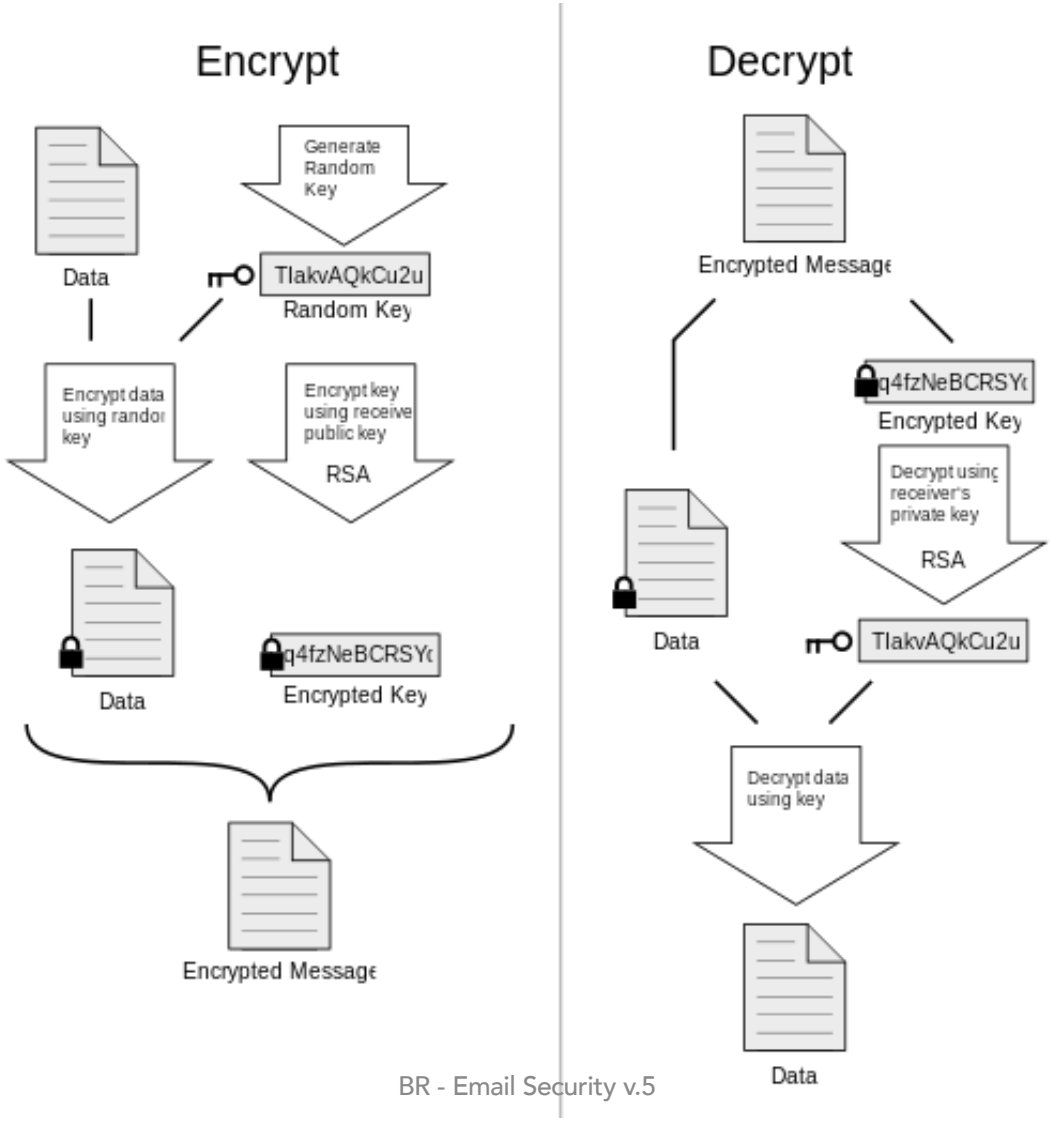
Isi email tidak dirahasiakan. Diinginkan terjaganya integritas dan non-repudiation

Keduanya disatukan dan dikirimkan



Pada Penerima



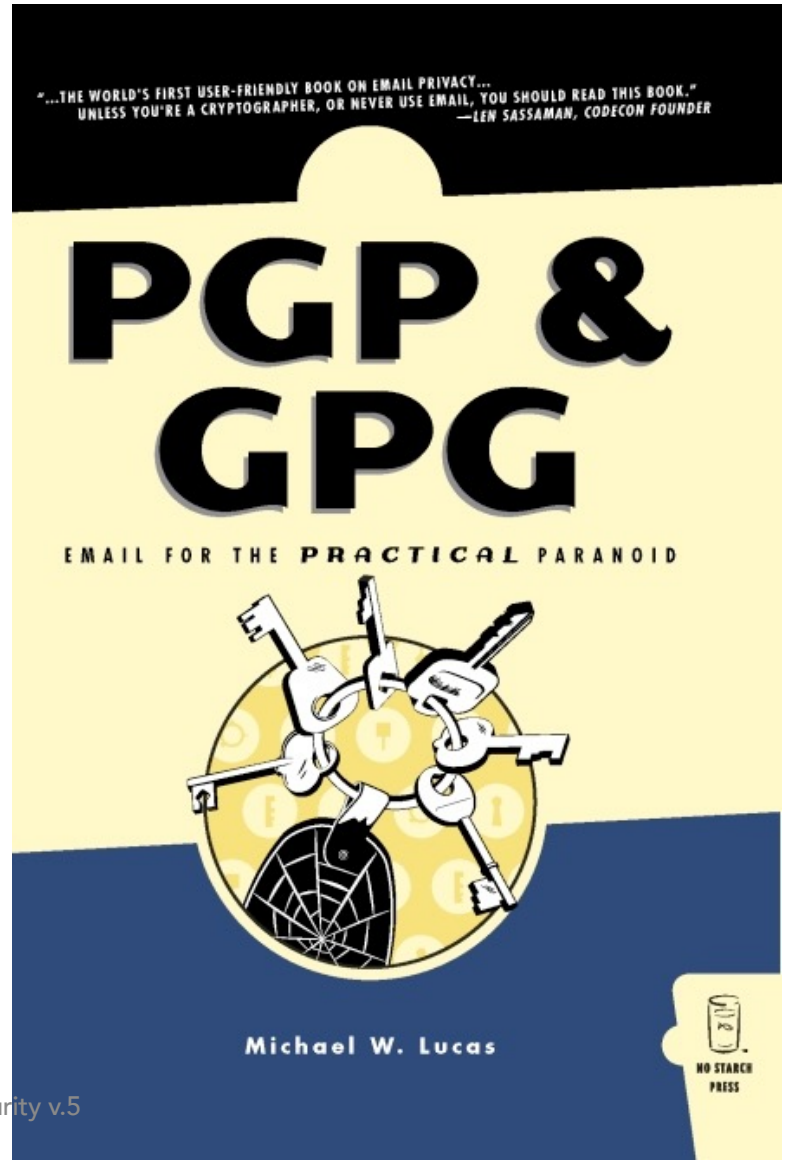

Encrypt
Data
Generate Random Key
TlakvAQkCu2u
Random Key
Encrypt data using rando key
Encrypt key using receive public key
RSA
Data
q4fzNeBCRSY
Encrypted Key
Encrypted Message
Decrypt
Encrypted Message
q4fzNeBCRSY
Encrypted Key
Decrypt using receiver's private key
RSA
Data
TlakvAQkCu2u
Decrypt data using key
Data

(Public) Key Management

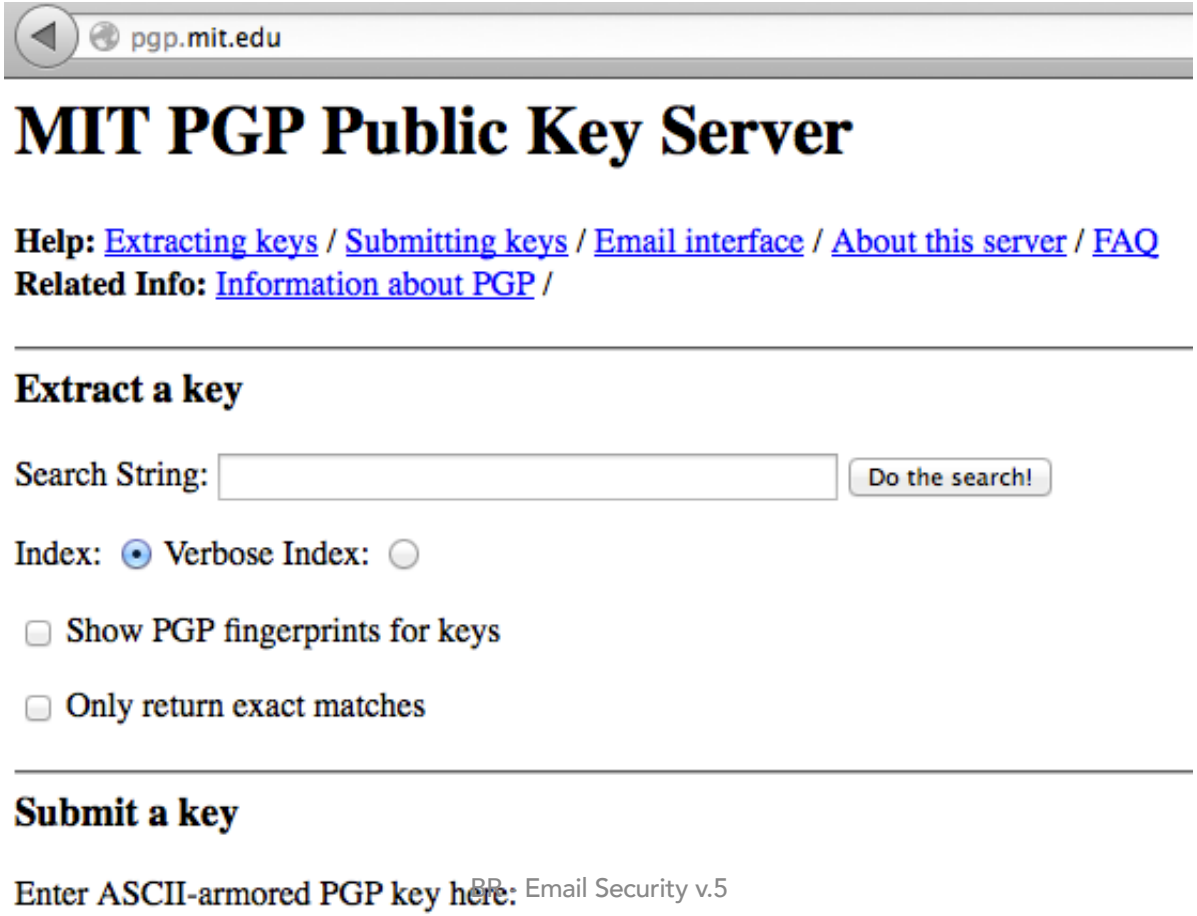
- Key creation
- Setor kunci publik
- Revocation
- Deletion (no!)
- User group

SOFTWARE


Encryption for Everyone
PGP
Pretty Good Privacy
HARDENED
PGP
Simson Garfinkel
O'Reilly & Associates, Inc.


"...THE WORLD'S FIRST USER-FRIENDLY BOOK ON EMAIL PRIVACY...
UNLESS YOU'RE A CRYPTOGRAPHER, OR NEVER USE EMAIL, YOU SHOULD READ THIS BOOK."
—LEN SASSAMAN, CODECON FOUNDER
PGP & GPG
EMAIL FOR THE PRACTICAL PARANOID
Michael W. Lucas
NO STARCH PRESS

pgp.mit.edu


pgp.mit.edu
MIT PGP Public Key Server
Help: Extracting keys / Submitting keys / Email interface / About this server / FAQ
Related Info: Information about PGP /
Extract a key
Search String:
Do the search!
Index: Verbose Index:
Show PGP fingerprints for keys
Only return exact matches
Submit a key
Enter ASCII-armored PGP key here:

Encrypted Email

- Pengirim
  - Membuat email
  - Mencari kunci public tujuan
  - Encrypt email
  - Kirim ke tujuan
- Penerima
  - Buka email