RESUME #3

Chapter 15 – Electronic Mail Security

Nama : Jordan Abdul Aziz

NIM : 150535604444

Prodi : S1 Teknik Informatika / B

15. Electronic mail security

Di hampir semua jaringan terdistribusi, elektronik mail atau biasa di singkat email merupakan aplikasi berbasis jaringan yang paling banyak digunakan. Tapi saat ini isi dari pesan bisa dibilang tidak aman yang di sebabkan oleh beberapa hal berikut :

- Terserang virus pada saat transmisi pengiriman ke tujuan.
- pengguna yang ilegal secara sengaja masuk ke sistem untuk melakukan serangan

Dengan ketergantungan yang semakin kuat terhadap email untuk melakukan setiap transaksi ataupun komunikasi, disana tumbuh permintaan untuk layanan authentication dan kerahasiaan. Sehingga dua skema muncul sebagai pendekatan yang dapat digunakan secara luas yaitu :

- Pretty Good Privacy (PGP)
- S/MIME.

Dan beberapa perangkat tambahan keamanan seperti :

Confidentiality ,Authentication ,Message integrity ,Non-repudiation of origin

15.1. Pretty Good Privacy PGP

Pretty Good Privacy adalah keamanan yang di tulis oleh Phil Zimmermann, berdasarkan algoritman IDEA untuk enkripsi plaintext dan menggunakan RSA public key untuk enkripsi privacy key. PG menyediakan layanan kerahasiaan dan authentication yang bisa digunakan untuk aplikasi penyimpanan email dan arsip. Dapat berjalan pada berbagai macam platform baik gratis maupun berbayar. Pada dasarnya PGP merupakan:

1. Pemilihan algoritma terbaik yang berfungsi seperti blok-blok bangunan

2. Mengintegrasi algoritma tersebut sehingga tidak bergantung pada system operasi dan prosesor.
3. Membuat paket – paket beserta dokumentasinya, termasuk source code yang tersedia gratis di internet, dan jaringan komersial seperti America On Line
4. Disetujui suatu perusahan (Viacrypt) untuk memberikan versi komersial PGP yang kompatibel dengan biaya rendah

Beberapa alasan PGP dapat berkembang secara pesat ialah:

1. Multiplatform
2. PGP didasarkan pada algoritma yang sangat aman
3. Mudah diterapkan dalam skala besar
4. Tidak dikembangkan dan tidak dikendalikan oleh perseorangan atau suatu perusahaan
5. PGP berada di atas Internet standards track (RFC 3156)

15.1.1. Notation

Simbol – symbol yang digunakan dalam PGP

Ks	= session key yang digunakan dalam skema enkripsi simetris
PRa	= private key untuk user A, digunakan dalam skema enkripsi public key
PUa	= public key untuk user A, digunakan dalam skema enkripsi public key
EP	= enkripsi public key
DP	= dekripsi public key
EC	= enkripsi simetris
DC	= dekripsi simetris
H	= fungsi hash
||	= serangkaian hal atau peristiwa yang saling berhubungan
Z	= kompresi yang menggunakan algoritma ZIP
R64	= konversi ke radix 64 ASCII format

15.1.2. Operational Description

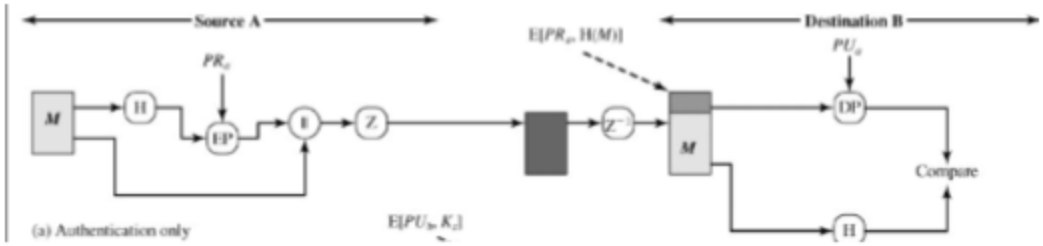
Operasi PGP yang sebenarnya terdiri dari 4 services : authentication, confidentiality, compression, and e-mail compatibility. Berikut adalah tampilan tabel dari 4 services

Function	Algorithms	Used Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed, for storage or transmission, using ZIP.
Email compatibility	Radix 64 conversion	To provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix 64 conversion.
Segmentation		To accommodate maximum message size limitations, PGP performs segmentation and reassembly.

- Authetication

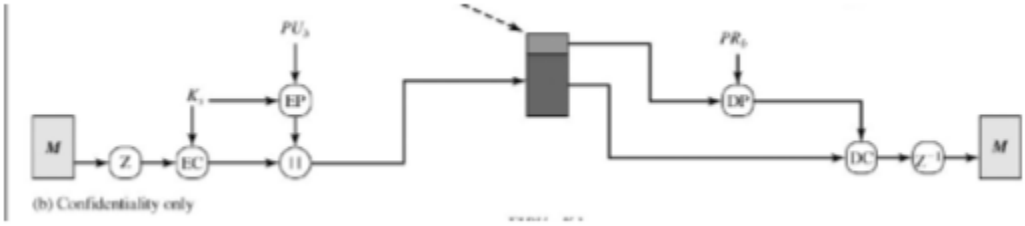
Penggunaan RSA digital signature, dibuat dengan menggunakan private key pengirim, dan di verifikasi dengan public key pengirim. Versi PGP terbaru juga mendukung penggunaan DSS signature. Penggunaannya juga bisa terlepas dari pesan/file dan dikirim/disimpan secara terpisah. Ini berguna untuk menyimpan log dari semua pesan yang dikirim atau diterima, atau pada program yang dapat dieksekusi untuk mendeteksi virus berikut adalah tahapannya :

1. Pengirim membuat pesan
2. Membuat pesan SHA-1160-bit hash
3. Terlampir pesan RSA signed hash
4. Penerima mendeskripsikan dan memulihkan hash code
5. Penerima memverifikasi pesan hash yang diterima



- Confidentiality

Layanan lain yang disediakan oleh PGP adalah confidentiality, yang disediakan dengan mengenkripsi pesan saat dikirim atau disimpan secara local menjadi file. Penggunaan symmetric algoritma CAST-128, IDEA atau 3DES in 64bit cipher feedback (CFB) mode. Pemiliha session key secara acak digunakan untuk dikirim menggunakan enkripsi RSA key. Untuk lebih jelasnya seperti ilustrasi di bawah ini

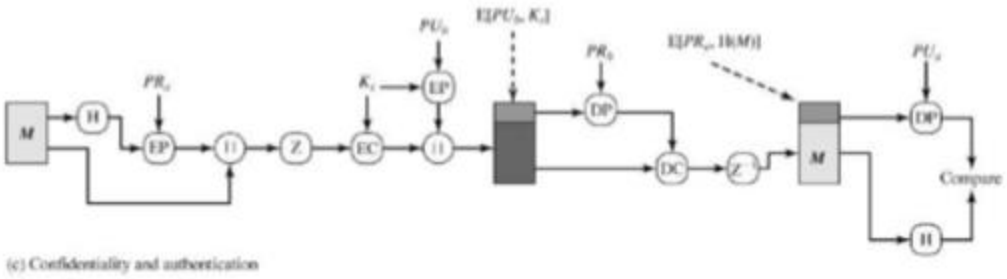


- Confidentiality & authentikasi

Kedua layanan ini digunakan utuk pesan yang sama. Pertama adalah signature dihasilkan untuk pesan plainteks dan ditambahkan ke dalamnya. Lalu pesan plainteks ditambah signature di enkripsi menggunakan CAST-128 (or IDEA or 3DES), dan session key di enkripsi menggunakan RSA (or ElGamal).

Kapan kedua layanan tersebut digunakan :

1. Pengirim pertama kali menandai pesan dengan private key miliknya.
2. Lalu pesan di enkripsi dengan sebuah session key.
3. Dan akhirnya session key di enkripsi dengan penerimanan public key.



(c) Confidentiality and authentication

- PGP compression
  - Sebagai default, PGP mengkompres pesan sesudah menerapkan signature tapi sebelum enkripsi.
  - Berguna untuk menghemat baik untuk penyimpanan email dan untuk penyimpanan file
  - Penempatan algoritma kompresi sangant penting

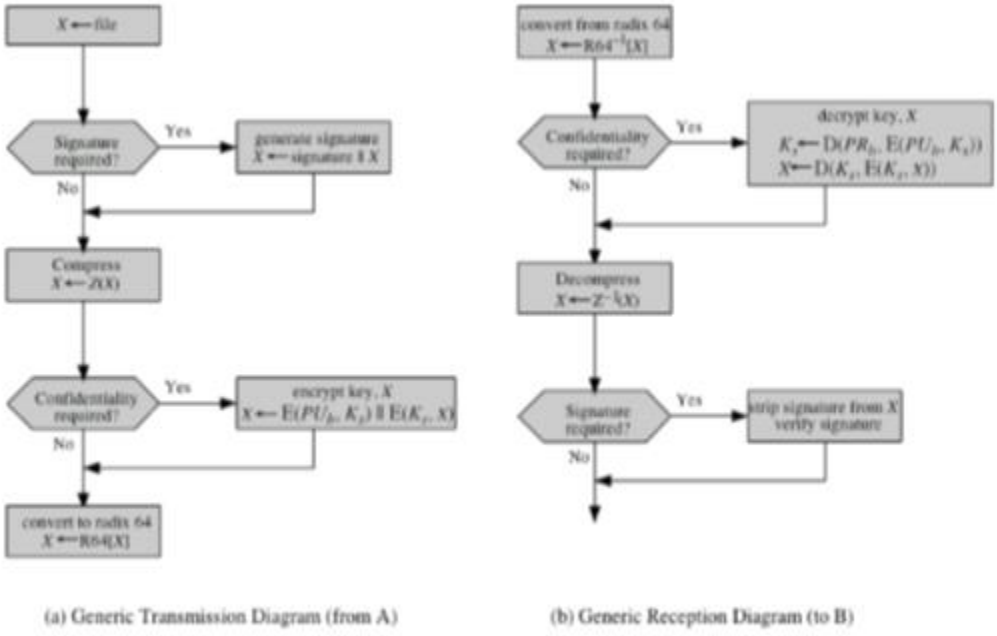
    Menerapkan hash function dan signature setelah kompresi akan membatasi semua implementasi PGP ke semua versi yang sama dengan kompresi algoritma.
  - Pesan enkripsi diterapkan setelah kompresi untuk memperkuat security kriptografi.
  - Algoritma yang digunakan sendiri adalah ZIP

- Email Compability

  Banyak email system yang hanya mengizinkan penggunaan block yang terdiri dari

  ASCII text

  - Untuk mengakomodasi pembatasan ini, PGP menyediakan layanan untuk mengubah aliran biner 8-bit raw menjadi aliran karakter ASCII
  - Skema ini digunakan untuk tujuan konversi radix-64
    - Setiap kelompok tiga oktet data biner dipetakan ke dalam empat karakter ASCII
    - Format ini juga menambahkan CRC untuk mendeteksi kesalahan Transmisi



(a) Generic Transmission Diagram (from A) (b) Generic Reception Diagram (to B)

Figure 19.2 Transmission and Reception of PGP Messages

Menggambarkan operasi umum dari PGP, dana hubungan antara layanan yang dibahas.

- Session keys

  PGP menggunakan empat type kunci : one-time session symmetric key, public keys, private keys, dan passphrase-based symmtric keys. Setiap session key dikaitkan dengan satu pesan dan hanya digunakan untuk mengenkripsi dan mendeskripsi pesan itu. Angka acak dihasilkan menggunakan generator ANSI X12.17, dengan masukan berdasarkan input keystroke dari pengguna, di mana kedua timing keystroke dan tombol yang sebenarnya dipukul digunakan untuk menghasilkan aliran angka secara acak. Stallings Lampiran 15C membahas teknik pembangkitan angka acak PGP secara lebih rinci.

- PGP public dan private key

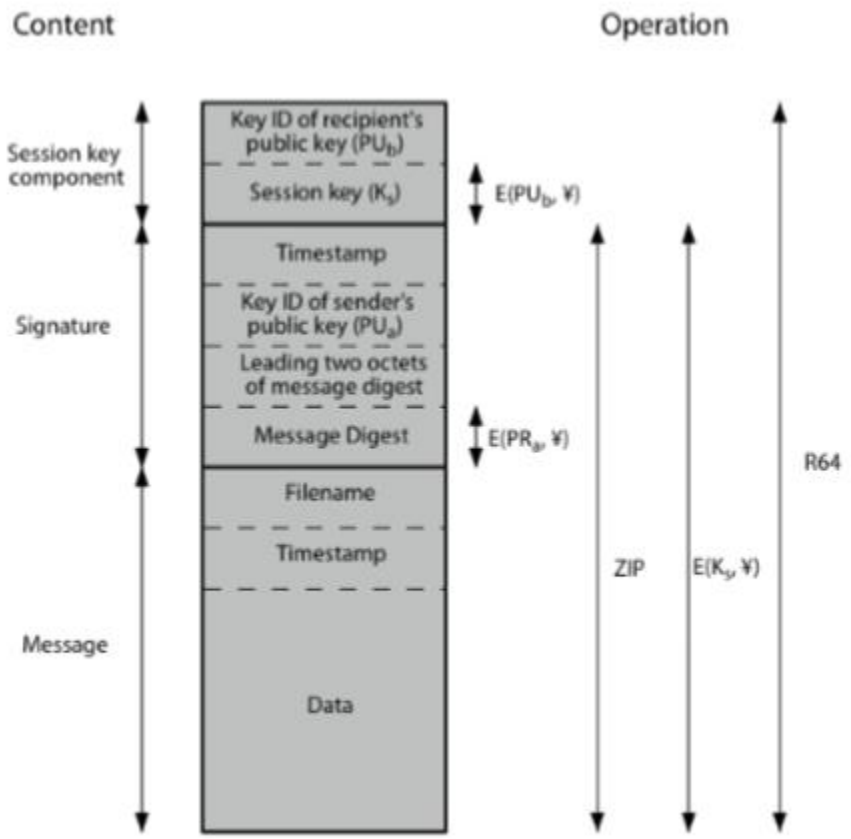
  Banyaknya public/private key yang mungkin digunakan, perlu identifikasi yang sebenarnya digunakan untuk mengenkripsi session keys dalam sebuah pesan

  - Dapat mengirim public key di setiap pesan
  - Tapi ini tidak effective

  Bukan menggunakan identifier key berdasarkan kunci

- Paling tidak berarti 64bit key
- Bersifat unique

Juga menggunakan ID dalam signature



- PGP key rings

  Setiap pengguna PGP mempunyai sepasang keyrings :

  - Public-key ring berisi semua public key pengguna PGP lain yang diketahui pengguna ini, yang di index oleh key ID.
  - Private-key ring berisi sepasang public/private key untuk pengguna ini, di indek oleh key ID dan kunci terenkripsi oleh frasa sandi hash

  Keamanan private key tergantung pada keamanan pass-phrase security

Private Key Ring

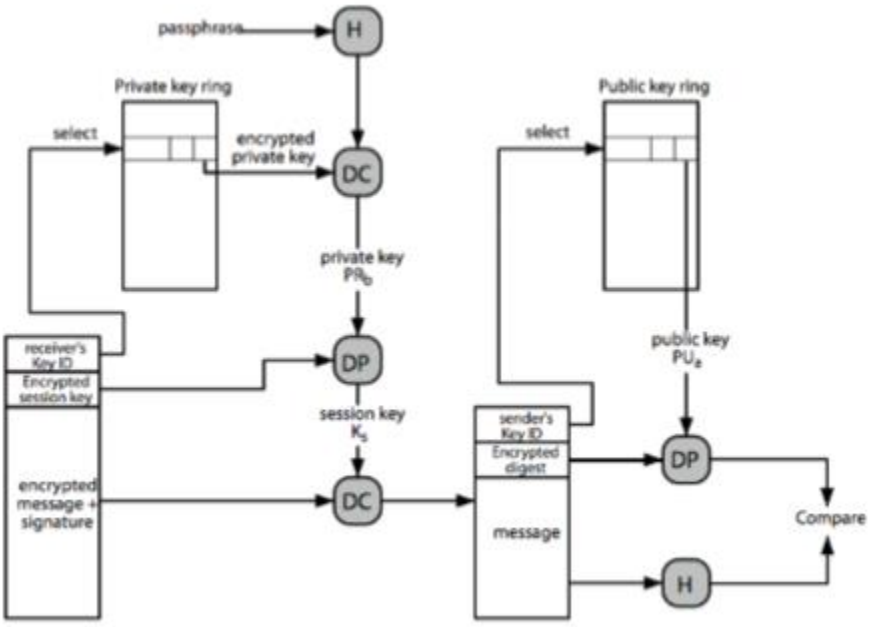
Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
. . .	. . .	. . .	. . .	. . .
T_i	PU_i mod 2^{64}	PU_i	$E(H(P_i), PR_i)$	User i
. . .	. . .	. . .	. . .	. . .

Public Key Ring

Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
T_i	PU_i mod 2^{64}	PU_i	$trust\_flag_i$	User i	$trust\_flag_i$		
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .

* = field used to index table

PGP message generation

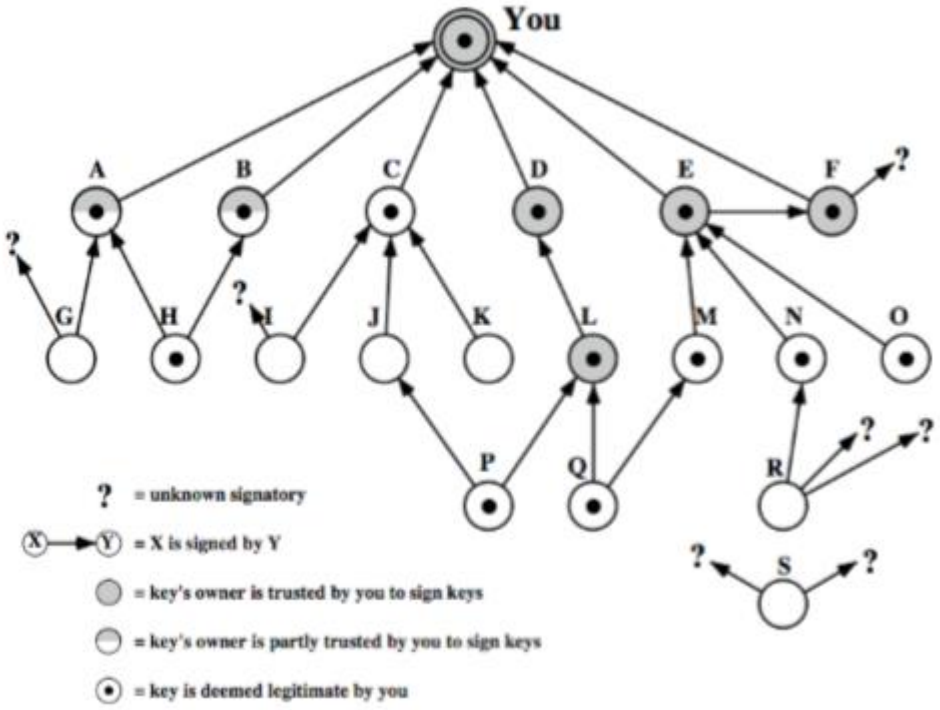


15.1.4. Public-Key Management

Dalam PGP setiap pengguna CA dapat memberi sign keys untuk pengguna yang mereka tahu sehingga membentuk “Web of Trust”, trust key telah ditandai dapat diidentifikasi oleh pengguna lain yang masuk dalam rantai signature. Key ring mengandung indicator dari Web of Trust.

Pengguna juga dapat mencabut kunci yang mereka miliki dalam rantai signature Web of Trust tersebut.

Contoh model Trust PGP



15.2. S/MIME (Secure/Multipurpose Internet Mail Extensions)

15.2.1. Definisi dari S/MIME yaitu perangkat tambahan keamanan dengan standar format email MIME internet, yang pada gilirannya memberikan dukungan untuk berbagai jenis konten dan multi-part messages selama teks hanya mendukung internet asli RFC822(sekarang menjadi RFC5322) untuk standar email. MME memungkinkan pengkodean data biner ke bentuk tekstual untuk transportaso melalui sistem email RFC822. Dukungan S/MIME sekarang termasuk dalam banyak agen email

15.2.2. S/MIME Functionality

1. Enveloped adalah data Konten yang telah dienkripsi dan kunci terkait
2. Signed data adalah Encoded message + Signed digest
3. Clear-signed data = Cleartext message + Encodedd signed digest
4. Signed & enveloped data adalah Nesting of signed + Entiti yang dienkripsi

15.2.3. S/MIME Cryptographic Algorithms

Digital Signatures: DSS & RSA Hash Functions: SHA-1 & MD5

Session Key Encription: ElGamal & RSA

Message Encription: AES, 3DES, RC2/40 dll

MAC: HMAC dengan SHA-1

15.2.4. S/MIME Messages S/MIME memberikan keamanan ke entity MIME dengan menggunakan signature, enkripsi maupun keduanya. Membentuk suatu MIME yang dibungkus objek PKCS. Memiliki beberapa jenis konten, yaitu:

1. Enveloped data
2. Signed data
3. Clear-signed data
4. Registration request
5. Certificate only message

15.2.5. S/MIME Certificate Processing

S/MIME menggunakan X.509 v3 certificates. Telah menggunakan hybrid X.509 CA hierarchy dan Web of Trust PGP. Setiap klien mempunyai daftar sertifikat CA's yang terpercaya, dan mempunyai pasangan public/private key. Sertifikat harus ditandai oleh CA yang terpercaya.

15.2.6. Enhanced Security Service

Tiga tujuan peningkatan keamanan layanan:

1. Signed receipts Tanda yang ada untuk membuktikan bahwa pesan telah diterima dan asli
2. Security labels Digunakan untuk mengontrol akses yang dapat mengatur pengguna yang diberi akses ke suatu objek.
3. Secure mailing lists Memberikan suatu keamanan dalam daftar pesan