

**TUGAS AKHIR
EC7010 KEAMANAN SISTEM LANJUT**

**PRETTY GOOD PRIVACY (PGP) UNTUK
KEAMANAN E-MAIL**



Dibuat oleh :

Nama : Abdul Wahab Moha

Nim : 23203098

**INSTITUT TEKNOLOGI BANDUNG
2004**

DAFTAR ISI

	Halaman
Daftar Isi.....	i
Abstrak.....	ii
BAB I Pendahuluan.....	3
BAB II Pretty Good Privacy (PGP).....	6
II.1 Ilustrasi Pemakaian Pretty Good Privacy (PGP).....	10
II.2 Enkripsi untuk File-File Biner.....	11
II.3 Implementasi PGP dalam Tanda Tangan Digital.....	11
II.4 Konfigurasi baris Perintah PGP.....	12
II.5 Operasi Pretty Good Privacy (PGP).....	16
II.6 Deskripsi Kunci Privat.....	24
BAB III Penutup.....	27
Daftar Pustaka.....	28

ABSTRAK

PGP adalah suatu metode enkripsi informasi yang bersifat rahasia sehingga jangan sampai diketahui oleh orang lain yang tidak berhak. Informasi ini bias berupa E-mail yang sifatnya rahasia, nomor kode kartu kredit, atau pengiriman dokumen rahasia perusahaan melalui Internet. PGP menggunakan metode kriptografi yang disebut “*public key encryption*”: yaitu suatu metode kriptografi yang sangat *sophisticated*.

Adapun prinsip kerja dari PGP adalah sebagai berikut :

1. PGP menggunakan teknik yang disebut *public key encryption* dengan dua kode. Kode-kode ini berhubungan secara intrinstik, namun tidak mungkin untuk memecahkan satu sama lain,
2. Ketika dibuat satu kunci, maka secara otomatis akan dihasilkan sepanjang kunci,yaitu kunci publik dan kunci rahasia,
3. PGP menggunakan dua kunci, *Pertama*, kunci untuk proses enkripsi (kunci publik). Disebut kunci publik karena kunci yang digunakan untuk enkripsi ini akan diberitahukan kepada umum. Orang yang akan mengirimkan e-mail rahasia kepada kita harus mengetahui kunci publik ini. *Kedua*, kunci untuk proses deskripsi (kunci pribadi). Disebut kunci pribadi karena kunci ini hanya diketahui oleh kita sendiri.
4. Karena dengan *conventional crypto*, di saat terjadi transfer informasi kunci, diperlukan suatu *secure channel*. Jika kita memiliki suatu *secure channel*, mengapa masih menggunakan *crypto*? Dengan *public key system*, tidak akan menjadi masalah siapa yang melihat kunci milik kita, karena kunci yang dilihat orang lain adalah yang digunakan hanya untuk enkripsi dan hanya pemiliknya saja yang mengetahui kunci rahasia tersebut.

BAB I

PENDAHULUAN

Perekembangan teknologi telekomunikasi dan penyimpanan data dengan menggunakan komputer memungkinkan pengiriman data jarak jauh yang relatif cepat dan murah. Di lain pihak pengiriman data jarak jauh melalui gelombang radio ,maupun media lain yang digunakan masyarakat luas (public) sangat memungkinkan pihak lain dapat menyadap dan mengubah data yang dikirimkan. Demikian juga pada sistem jaringan komputer maupun secara luas pada internet dengan jumlah pemakai yang banyak.

Dalam teknologi informasi, telah dan sedang dikembangkan cara-cara untuk menangkal berbagai bentuk serangan semacam itu. Salah satu cara yang ditempuh mengatasi masalah ini ialah dengan menggunakan kriptografi yang menggunakan transformasi data sehingga data yang dihasilkan tidak dapat dimengerti oleh pihak ketiga.

Transformasi ini memberikan solusi pada dua masalah keamanan data, yaitu masalah privasi (privacy) dan keautentikan (authentication). Privasi mengandung arti bahwa data yang dikirimkan hanya dapat dimengerti informasinya oleh penerima yang sah. Sedangkan keautentikan mencegah pihak ketiga untuk mengirimkan data yang salah atau mengubah data yang dikirimkan.

Tujuan

Adapun tujuan dari sistem kriptografi adalah sebagai berikut :

➤ **Confidentiality**

Memberikan kerahasiaan pesan dan menyimpan data dengan menyembunyikan informasi lewat teknik-teknik enkripsi.

➤ **Message Integrity**

Memberikan jaminan untuk tiap bagian bahwa pesan tidak akan mengalami perubahan dari saat ia dibuat sampai saat ia dibuka.

➤ **Non-repudiation**

Memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang apabila ia mencoba menyangkal memiliki dokumen tersebut.

➤ **Authentication**

Memberikan dua layanan. *Pertama*, mengidentifikasi keaslian suatu pesan dan memberikan jaminan keautentikannya. *Kedua*, menguji identitas seseorang apabila ia akan memasuki sebuah sistem.

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dari suatu sistem informasi. Hal ini sangat terkait dengan betapa pentingnya informasi tersebut dikirim dan diterima orang yang berkepentingan. Informasi akan tidak berguna lagi apabila ditengah jalan dibajak atau disadap oleh orang yang tidak berhak.

Keamanan dan kerahasiaan ada apada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Pada garis besarnya, masalah keamanan jaringan dapat dibagi menjadi empat bidang yang saling berhubungan, yakni, kerahasiaan, keaslian, pengakuan, dan kontrol integritas. Kerahasiaan harus dilakukan dengan menjauhkan informasi dari orang-orang yang tidak berhak, Keaslian berkaitan dengan menentukan dengan siapa anda berbicara sebelum memberikan informasi yang sensitife atau memasuki perjanjian bisnis, sedangkan pengakuan berkaitan dengan tanda tangan.

Selain keamanan dan kerahasiaan data dalam jaringan komputer, konsep ini juga berlaku untuk keamanan dan kerahasiaan data pada internet. Informasi yang terkandung di dalam jaringan internet tersebut juga semakin lengkap, akurat, dan penting yang perlu mendapat perlakuan yang lebih spesifik.

Selain itu, kemajuan yang dicapai dalam bidang pengembangan sistem operasi komputer sendiri dan utilitasnya sudah sedemikian jauh dimana tingkat performansi, kehandalan, dan fleksibilitas software menjadi kriteria utama dalam proses pengembanagan software. Dengan semakin penting dan berharganya informasi tersebut dan ditunjang oleh kemajuan pengembangan software, tentunya menarik

minat para pembobol (hacker) dan penyusup (intruder) untuk terus bereksperimen guna menemukan dan mempergunakan setiap kelemahan yang ada dari konfigurasi sistem informasi yang telah ditetapkan.

Untuk menjaga keamanan dan kerahasiaan data dalam suatu jaringan komputer, diperlukan beberapa jenis enkripsi agar data tidak dapat dibaca atau dimengerti oleh sembarang orang kecuali untuk penerima yang berhak.

Berebagai macam layanan komunikasi tersedia di internet, diantaranya adalah web, e-mail, millis, newsgroups, dan sebagainya. Dengan semakin maraknya orang memanfaatkan layanan komunikasi di internet tersebut, maka permasalahan pun bermunculan, apalagi ditambah dengan adanya hacker dan cracker. Banyak orang kemudian berusaha menyiasati bagaimana cara mengamankan informasi yang dikomunikasikannya, atau menyiasati bagaimana cara mendeteksi keaslian dari informasi yang diterimanya.

Seseorang pengirim pesan yang hendak mengirmkan surat elektronik (e-mail) kepada rekannya, menginginkan agar pesannya tidak dibaca oleh orang yang tidak berhak membacanya, padahal bila administrator server e-mail sedang iseng, sangat mungkin dia akan membaca e-mail-e-mail yang ada di servernya. Penerima pun ingin mendapat keyakinan bahwa pengirimnya merupakan orang yang dikenalnya, bukan orang yang berpura-pura sebagai temannya.

BAB II

PRETTY GOOD PRIVACY (PGP)

Pretty Good Privacy (PGP) adalah salah satu software pengaman kriptografi yang cukup tinggi performansinya. PGP yang dikembangkan oleh Phillip Zimmerman ini memiliki 2 versi yaitu “USA version” dan International version”. PGP versi USA hanya digunakan di wilayah USA dan warga negara USA yang menggunakan algoritma RSA dalam enkripsinya. Sedangkan versi International menggunakan algoritma MPILIB yang dapat digunakan oleh siapa saja.

PGP dibuat berdasarkan pada konsep *Public Key Cryptography*. Kriptografi mempunyai konsep secara umum, jika seseorang hendak mengirim e-mail yang bersifat rahasia, maka si pengirim dapat mengkodekannya (enkripsi) menggunakan suatu algoritma tertentu yang hanya si pengirim mail yang tahu.

Mengapa menggunakan PGP

Aspek yang paling umum dari PGP adalah penandaan dan enkripsi dari sebuah e-mail atau sebuah file. Penandaan sebuah dokumen adalah cara membuktikan integritas dari pekerjaan yang asli.

Adapun metode yang digunakan adalah sebagai berikut :

- Buatlah sebuah singkatan atau hash dari sebuah file atau e-mail. Hash adalah algoritma yang menghasilkan output yang bersifat unik dari sebuah input tertentu, misalnya pesan.
- Tambahkan hash pada akhir pesan.
- Ketika seseorang ingin membuktikan bahwa pesan itu belum diubah, mereka akan mengoperasikan algoritma hash pada pesan dan membandingkannya dalam hash pada akhir pesan. Jika tanda tangan sesuai berarti pesan belum diubah.

Contoh pesan yang disertai algoritma hash.

Ambil setiap huruf ketiga dari pesan dan abaikan tanda baca. Ubah setiap huruf menjadi angka (a=1,b=2,...z=26). Tambahkan angka secara bersama-sama.

Pesannya adalah sebagai berikut :

Hello, this is a sample message to demonstrate signatures.

Proses dalam algoritma *hash* :

Hello, This is a sample message to demonstrate signatures

$$12 + 20 + 19 + 1 + 13 + 5 + 19 + 7 + 15 + 13 + 19 + 1 + 19 + 14 + 21 + 19 = 217$$

(nilainya sama dengan 217)

Pesan yang terjadi sesudah menambah nilai hash :

Hello, This is a sample message to demonstrate signatures.

(nilai *hash* sama dengan 360)

Jika pesan diubah, nilai hash tidak akan sama.

Pesan yang diubah:

Hello, This is an altered message to demonstrate signatures

Ciptakan hash yang baru :

Hello, This is an altered message to demonstrate signatures

$$12 + 20 + 19 + 1 + 12 + 18 + 13 + 19 + 5 + 4 + 15 + 20 + 20 + 9 + 1 + 18 = 206$$

(nilai hash adalah 206)

Algoritma *hash* digunakan dalam kata hubung dengan kunci pribadi pengguna dengan cara bahwa tanda tangan mempunyai sifat yang unik, yaitu jika orang yang berbeda ditandai e-mail yang sama, maka tanda tangannya juga berbeda.

Kemudian kunci publik dari pasangan kunci digunakan untuk membandingkan hash yang diciptakan oleh kunci pribadi, dan jika hash cocok, ada dua hal yang terjadi, yaitu pesan tidak dimodifikasi sejak penandaan dan tanda tangan tidak dipalsukan.

Selain itu dalam dunia internet terdapat apa yang disebut *aktivitas sniffing* atau *packet dumping* atau bahkan pengawasan yang dengan program tertentu dapat dengan mudah mengetahui *password* atau apa saja yang dikerjakan orang lain lewat internet. Aktivitas ini tidak membutuhkan keahlian komputer yang tinggi, cukup *download* programnya saja dan tinggal dijalankan.

Dengan semakin luasnya penggunaan e-mail dari urusan rumah tangga sampai ke rahasia perusahaan dan bahkan rahasia negara, maka orang-orang kini mempertanyakan sejauh mana e-mail dapat dipercaya untuk membawa informasi-informasi yang sensitif bagi kita.

Dengan PGP, kita mendapatkan lebih dari sekedar privasi. Kita dapat memastikan bahwa e-mail ini memang berasal dari si pengirimnya dan bukan e-mail palsu dari pembuat surat kaleng yang mengatas namakan orang lain. Sebaliknya, kita juga dapat memastikan bahwa e-mail ini memang berasal dari si pengirimnya tanpa dapat disangkal oleh sipengirim tersebut.

Kita juga dapat memastikan bahwa e-mail yang kita terima atau kirim itu masih utuh tidak kurang satu karakter pun dan masih banyak keuntungan lainnya.

Ada beberapa alasan penting mengapa kita perlu menggunakan PGP untuk mengamankan e-mail dan file kita.

1. Keamanan

Kita dapat menggunakan PGP untuk berkomunikasi secara aman, baik itu rencana bisnis, keuangan, atau hal-hal pribadi lain yang ingin dijaga kerahasiaannya. Kita dapat menggunakan PGP dengan e-mail untuk alasan yang sama pada waktu kita mengirim surat dengan menggunakan amplop.

Mungkin teman seprofesi atau anggota keluarga ingin tahu bahwa informasi yang dikirim terjaga kerahasiaannya dan kiriman benar-benar berasal dari kita.

Barang kali kita pernah mengirim e-mail kepada orang yang salah dan kita ingin mereka tidak membacanya. Hal itu sangat sulit untuk dilakukan, kemungkinan sudah banyak orang yang sudah mengetahui isi dari e-mail kita. Jadi untuk amannya e-mail maupun informasi yang kita kirim hendaknya disertai dengan software PGP.

2. Fleksibel

Karena PGP sudah *plug-in* untuk semua program *browser* dan banyak digunakan oleh semua program e-mail., maka PGP sangat fleksibel untuk digunakan.

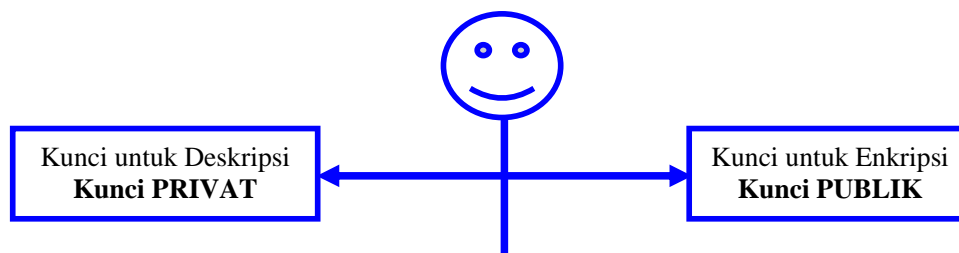
PGP selain melindungi e-mail juga file kita dan berjalan pada semua sistem operasi.

3. Gratis

PGP dapat diperoleh secara gratis untuk penggunaan pribadi. Kita dapat *download* softwarena pada saat kita terhubung dengan internet. Semua kunci pribadi dapat kita peroleh dan tidak ada biaya tambahan yang dibebankan untuk pembuatan sertifikat maupun tanda tangan digital yang disertakan.

Pada PGP untuk melakukan proses enkripsi digunakan kunci rahasia yang berbeda dengan kunci rahasia yang digunakan pada proses deskripsi. Jadi terdapat dua buah kunci rahasia, satu untuk deskripsi, satu untuk enkripsi. Hal inilah yang dikenal dengan kriptografi asimetrik.

Selain asimetrik ada juga kriptografi simetrik yang hanya menggunakan 1 buah kunci rahasia. Gambar dibawah ini menjelaskan kunci deskripsi maupun enkripsi dalam kunci pribadi dan kunci publik.



Gambar 2.1 Kunci untuk deskripsi (kunci pribadi) dan kunci untuk enkripsi (kunci publik)

Kedua buah kunci tersebut adalah unik, artinya untuk setiap kunci rahasia, hanya akan ada tepat satu buah kunci pasangannya. Tidak boleh salah satu dari kedua buah kunci rahasia tersebut digantikan dengan kunci lain.

Dengan demikian, siapa saja yang ingin menggunakan PGP akan membutuhkan 2 buah kunci. *Pertama*, kunci untuk proses enkripsi (kunci publik). Disebut kunci publik karena kunci yang digunakan untuk enkripsi ini akan diberitahukan kepada umum. Orang yang akan mengirimkan e-mail rahasia kepada kita harus mengetahui

kunci publik ini. *Kedua*, kunci untuk proses deskripsi (kunci pribadi). Disebut kunci pribadi karena kunci ini hanya diketahui oleh kita sendiri.

II.1 Ilustrasi Permakiaan Pretty Good Privacy (PGP)

Kunci publik sangat lambat jika dibandingkan dengan yang konvensional. Jadi, PGP akan mengkombinasikan dua algoritma, yaitu RSA dan IDEA, untuk melakukan enkripsi *plaintext* kita.

Sebagai contoh, Ahmad (pemilik PGP) ingin mengenkripsi suatu file yang diberi nama *plain.txt* sedemikian sehingga hanya si Badrun yang dapat mengenkripsinya. Maka Ahmad mengirimkan PGP perintah (*command line*) untuk melakukan enkripsi:

```
pgp -e plain.txt Badrun
```

Pada *command line* ini, *pgp* adalah *file executable* , *-e* berarti memberitahukan PGP untuk mengenkripsi file, *plain.txt* adalah nama *plaintext*, dan Ahmad mempresentasikan kunci publik suatu tujuan (Badrun) yang diinginkan Ahmad untuk mengenkripsi pesannya. PGP menggunakan suatu *random number generator*, dalam file *randseed.bin* untuk menghasilkan suatu kunci sesi *temporary* IDEA. Kunci sesi itu sendiri dienkripsi dengan kunci publik RSA yang dipresentasikan oleh Badrun yang diletakkan pada *plaintext*.

Kemudian, PGP menggunakan kunci sesi untuk mengenkripsi pesan, ASCII –armor dan menyimpan seluruhnya sebagai *cipher.asc*. Bila Badrun ingin membaca pesannya, ia mengetikkan *command*:

```
pgp cipher.asc
```

PGP menggunakan kunci pribadi milik Badrun, yang merupakan kunci RSA, untuk mendeskripsi kunci sesi yang mana, yang jika dipanggil oleh Ahmad akan dienkripsi oleh kunci publik. Kemudian, kriptografi konvensional digunakan dalam bentuk

kunci sesi untuk mendekripsi sisa dari pesan. Prinsip ini digunakan sebagai pengganti dari RSA.

II. 2. Enkripsi untuk file-file Biner

Untuk mereka yang terbiasa bekerja dengan file-file biner, pada *usenet* mengetahui istilah *Uuencode*. *Uuencode* adalah suatu program terutama untuk UNIX, namun sekarang berkembang sehingga dapat mengubah file-file biner seperti .GIF atau .AU menjadi ASCII text yang sesuai dengan format pengiriman *usenet*

Feature ini juga dimiliki oleh PGP. File config.txt (disebut pgp.ini atau .pgprc, tergantung protocol lokal) memiliki sesuatu pilihan untuk berapa banyak baris file ASCII yang dapat dimuat. Jika jumlah tercapai, PGP akan memecah-mecah file armored.asc menjadi .as1, .as2, .as3, ... dan semuanya harus digabungkan satu sama lain secara bersama-sama dan menjalankan PGP dalam suatu file yang besar. Untuk mengenkripsi suatu file biner, gunakan command berikut :

```
pgp -a picture.gif  
atau option TextMode diset ke ON:  
pgp -a picture.gif +textmode=off
```

II.3 Implementasi PGP dalam TandaTanganDigital

PGP mengizinkan kita untuk menandai pesan atau file dengan atau tanpa kunci yang mengenkripsinya. Masing-masing tanda tangan digital dihasilkan secara unik oleh PGP berdasarkan pada isi pesan dan kunci pribadi penanda tangan. Tanda tangan dicek oleh siapa pun yang menggunakan kunci publik penanda tangan. Sejak tanda tangan sebagian didasarkan pada isi pesan, bahkan jika katarakter pesan telah diubah, PGP akan melaporkan bahwa tanda tangan tersebut tidak valid.

Tand tangan juga didasarkan pada kunci pribadi, kunci pribadi hanya dipegang oleh penanda tangan sehingga penerima yakin bahwa pesan dikirim oleh orang yang dimaksud.

Hal penting yang perlu diingat bahwa ketika tanda tangan yang ditulis tangan menurut dugaan bersifat unik untuk setiap orang, tanda tangan digital juga bersifat unik untuk tiap dokumen dan penanda tangan. Tanda tangan yang ditulis dapat disalin dari dokumen satu ke dokumen yang lain dan masih kelihatan valid. Sedangkan tanda tangan digital apabila diberitahukan hal yang sama dengan tanda tangan biasa akan mengalami kegagalan pembuktian apabila diterapkan pada dokumen lain.

Apabila kita berbicara mengenai tanda tanagan digital, maka hal ini berkaitan dengan sertifikat digital pula. Hal-hal pentng yang perlu diperhatikan dalam proses sertifikat, terutama menyangkut kunci publik yang akan menggunakan PGP, antara lain

- Kunci publik itu sendiri.
- Kartu identitas pemakai yang meliputi nama dan alamat e-mail dari pemilik kunci.
- Satu atau lebih tanda tangan digital untuk kunci publik dan kartu identitas pemakai

Tanda tangan memberi kesaksian bahwa kartu identitas pemakai berhubungan dengan kunci publik dan dinyatakan valid. Hal itu dapat terjadi karena adanya kunci pribadi penanda tangan.

II.4 Konfigurasi baris perintah PGP

Sebelum mengirim e-mail yang dienkripsi, PGP perlu dikonfigurasi terlebih dahulu. Langkah-langkah untuk melakukan konfigurasi dalam PGP, sebagai berikut :

1. Buatlah pasangan kunci, kunci publik dan kunci pribadi
2. Bukalah kunci publik
3. Tambahkan kunci publik penerima

Membuat Pasangan Kunci

Pasangan kunci., yaitu kunci pribadi dan kunci publik dapat dipanggil dengan perintah *pgp-kv*. Dalam membuat pasangan kunci, langkah-langkahnya sebagai berikut :

1. Definisikan tipe dari masing-masing kunci
2. Definisikan algoritma dari masing-masing kunci

3. Tentukan ukuran kunci
4. Tentukan identitas publik untuk kunci pemakai
5. Tentukan validitas periode dari penandaan kunci
6. Tentukan passphrase.

Standar tanda tangan digital yang menggunakan algoritma Diffie Hellman adalah algoritma kunci yang direkomendasikan untuk masalah ini. RSA, metode kriptografi yang dibuat oleh *RSA Security Data, Inc* yang menggunakan dua kunci, dapat juga digunakan.

Dibawah ini baris perintah PGP :

```
C:\PGPcmd> -kg
Pretty Good Privacy (tm) Version 6.5.8
© 1999 Network Associates Inc.
Uses the RSAREF (tm) Toolkit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.
```

Membuka Kunci Publik

Kunci publik seharusnya ditukar diantara pengirim dan penerima sebelum mulai berkomunikasi. Kunci publik dapat dibuka di file teks dan didistribusikan ke penerima. Kunci publik tersebut dapat dibuka dengan perintah *pgp-kx userid keyfile*.

Berikut contoh baris perintah PGP :

```
C:\PGPcmd>pgp kx selva.kumar@xpedior.com selva.asc
Pretty Good Privacy (tm) Version 6.5.8
© 1999 Network Associates Inc.
Uses the RSAREF (tm) Toolkit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.

Extracting from keyring C:\winnt\profiles\solvakk\application data\pgp\pkr\
userid "selva.kumar@ xpedior.com.

Key extracted to file 'selva.asc'.
C:\PGPcmd>
```

Penambahan Kunci Publik Penerima

Sebagai bagian dari proses pertukaran kunci, kunci publik penerima seharusnya ditambahkan ke dalam *key ring* pengirim. Kunci publik dapat digunakan dengan perintah *pgp-ka keyfilename*.

Seperti terlihat pada baris perintah PGP berikut ini :

```
C:\PGPcmd>pgp -ka unknown.asc
Pretty Good Privacy (tm) Version 6.5.8
© 1999 Network Associates Inc.
Uses the RSAREF (tm) Toolkit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.
```

```
Looking for new keys...
```

```
DSS 1024/1024 0xD3279E4F 2001/02/26 unknown@xyz.com
```

```
Sig          0xD3279E4F          < Unknown signator, can't be checked
```

```
keyfile contains 1 new, Add these keys to keyring? (Y/n) Y
```

```
New userid: "unknown@ xyz.com"
```

```
New signature from keyID 0xD3279E4F on userid unknown@ xyz.com
```

```
Keyfile contains:
```

```
1 nves key(s)
```

```
1 new signature (s)
```

```
1 new user ID(s)
```

```
New signature from keyID 0xD3279E4F on userid unknown@ xyz.com
```

```
Summary of changes:
```

```
New userid: "unknown@ xyz.com"
```

```
New signature from keyID 0xD3279E4F on userid unknown@ xyz.com
```

```
Keyfile contains:
```

```
1 nves key(s)
```

```
1 new signature (s)
```

```
1 new user ID(s)
```

Setelah melakukan konfirmasi kebenaran kunci publik, kita dapat menandai kunci tersebut. Ketika melakukan enkripsi terhadap file dengan menggunakan ID penerima, kita akan melihat peringatan tentang kebenaran kunci publik. Penandaan akan menghilangkan pesan peringatan selama proses enkripsi pesan. Sebuah kunci dapat ditandai dengan menggunakan perintah *pgp-ks userid*.

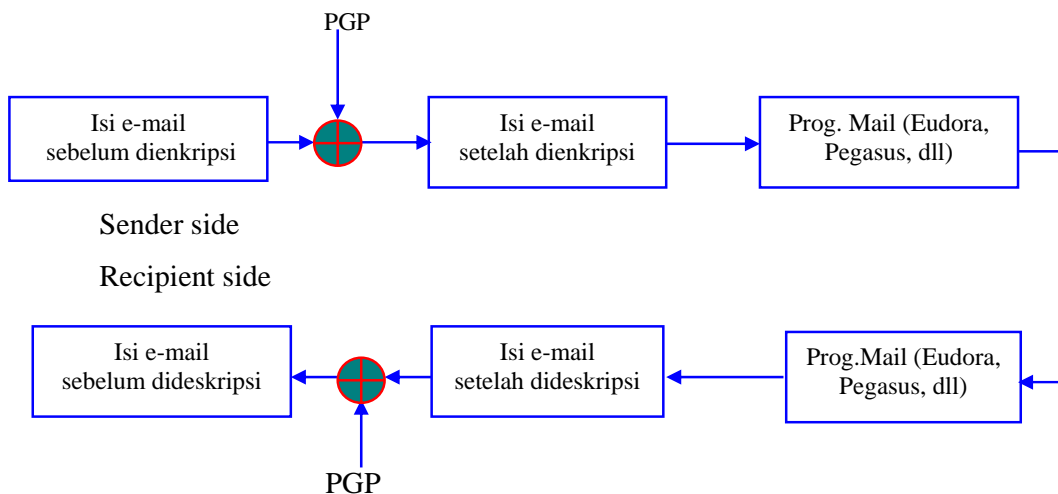
Dengan menggunakan PGP seseorang dapat mengirimkan mail atau file kepada orang lain secara privasi, autentikasi, dan cukup nyaman.

- Secara privasi artinya mail atau file yang dikirimkan hanya dapat dibaca oleh orang yang dituju.
- Autentikasi artinya bahwa pesan yang berasal dari seseorang hanya dapat dikirim oleh orang itu saja.
- Cukup nyaman karena tidak membutuhkan jalur untuk saling menukar tombol masing-masing user, PGP menggunakan teknologi “Public Key”.

Dengan demikian orang dapat meyakinkan bahwa tulisan atau artikel tersebut betul-betul berasal dari penulis.

Pada dasarnya, PGP merupakan program yang digunakan untuk mengenkripsi satu atau lebih dokumen. Dengan PGP tersebut hanya orang-orang tertentu saja yang dapat membaca file-file enkripsi tersebut.

Dibawah ini gambaran pengiriman mail dengan menggunakan PGP.



Gambar 2.2 Proses pengiriman e-mail dengan PGP

PGP dikembangkan oleh Phillip Zimmerman yang melakukan usaha-usaha berikut.

1. Memilih algoritma kriptografi terbaik yang ada sebagai komponen dasar pembentuk PGP
2. Mengintegrasikan algoritma-algoritma ini ke dalam aplikasi serba guna yang independen terhadap sistem operasi dan prosesor yang dijalankan dengan sekumpulan kecil instruksi yang mudah digunakan.
3. Membuat paket dan dokumentasinya, mencakup kode sumber, dapat diakses secara gratis melalui internet, *bulletin board*, dan jaringan komersial semacam *compuserve*.
4. Melakukan perjanjian dengan perusahaan untuk memberikan kompatibilitas yang penuh, versi komersial PGP yang berharga murah.

II.5 Operasi Pretty Good Privacy (PGP)

PGP melakukan beberapa operasi utama yaitu otentikasi, kerahasiaan, kompresi, kompatibilitas email.

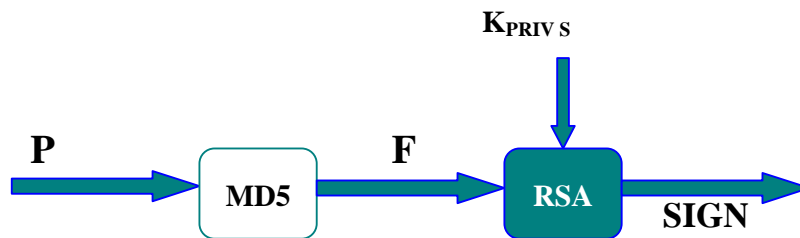
a. Otentikasi

Fungsi	Algoritma yang digunakan	Deskripsi
Enkripsi pesan	IDEA, RSA	Pesan dienkripsi yang menggunakan IDEA dengan kunci sesi sekali pakai yang dibangkitkan pengirim. Kunci sesi dienkrip menggunakan RSA dengan kunci publik <i>penerima</i> dan digabungkan ke dalam pesan.
Tanda tangan digital	RSA, MD5	Kode hash pesan dibuat menggunakan MD5, hash dienkrip menggunakan RSA dengan kunci <i>privat pengirim</i> dan digabungkan ke dalam pesan.
Kompresi	ZIP	Pesan dapat dikompres untuk disimpan atau dikirim dengan ZIP.
Kompatibilitas	Konversi Radix (Base)	Untuk mempermudah penggunaan

e-mail	64	Dalam aplikasi e-mail, pesan yang terenkrip, dapat dikonversi ke dalam string ASCII menggunakan konversi radix (base) 64.
Segmentasi		Untuk mengakomodasi batasan ukuran pesan maksimum, PGP melakukan segmentasi dan penyusunan ulang

Gambar 2.3 Tabel Fungsi dalam PGP

Tanda tangan umumnya ditempelkan ke pesan atau file yang ditandatangani, tanda tangan yang terpisah dapat disimpan dan dikirim secara terpisah dari pesannya. Misalnya ada pesan M ditandatangani A menghasilkan F_A , kemudian pesan M ditandatangani B menghasilkan F_B . Tanda tangan dapat juga digunakan secara bertingkat. Misalnya ada pesan M yang ditandatangani A menghasilkan F_A , F_A digabung dengan M sekaligus ditandatangani B menghasilkan F_{AB} dan seterusnya.

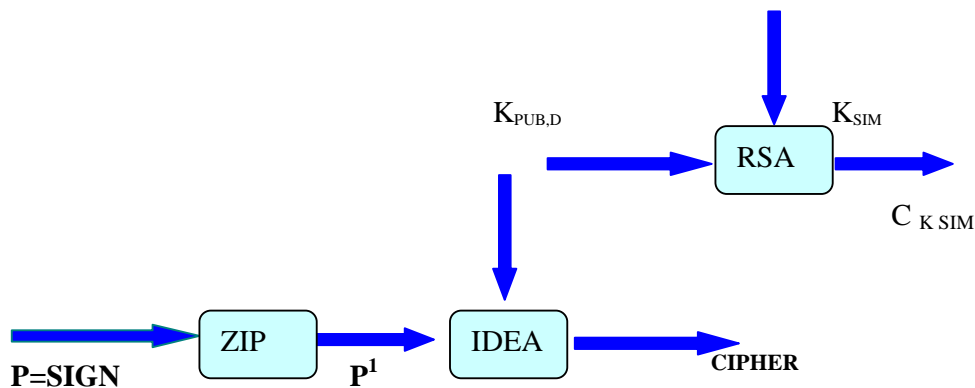


Gambar 2.4 Tanda tangan Digital

Pada gambar terlihat, bahwa pesan (plaintext P) di masukkan ke dalam fungsi MD5 yang menghasilkan sidik jari (Fingerprint F). Sidik jari merupakan identitas pesan yang ditandatangani oleh pengirim (sumber S) menggunakan kunci privat $K_{PRIV S}$. kunci yang digunakan untuk menandatangani adalah kunci privat pengirim S yang menunjukkan bahwa kunci privat digunakan sebagai identitas penandatanganan. Hasil tanda tangan pesan P adalah sign (signature).

b. Kerahasiaan

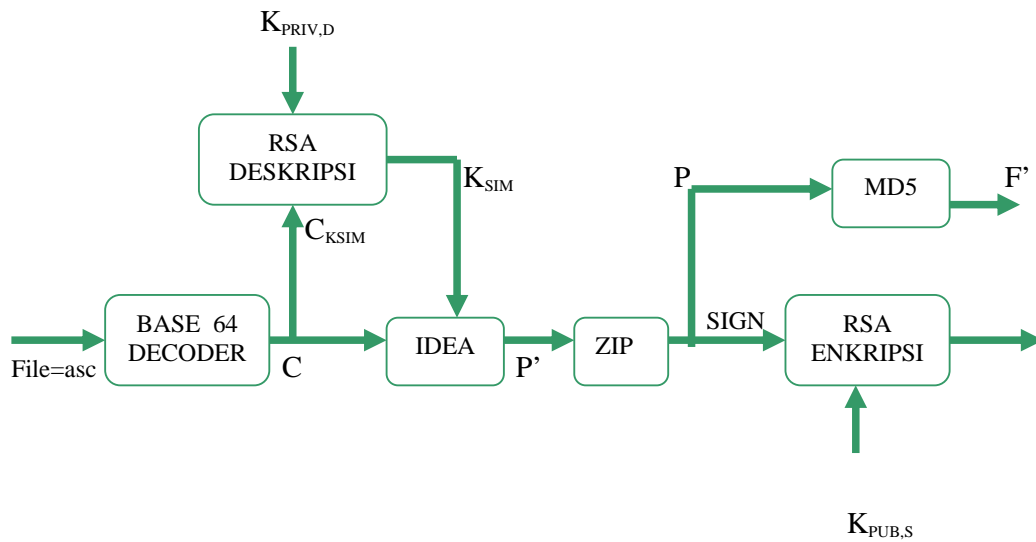
Pretty Good Privacy menggunakan IDEA dengan kunci 128 bit untuk menyandikan data dan menggunakan mode *Cipher Feed Back* (CFB) dengan vektor awal nol. Pada PGP kunci hanya dapat digunakan sekali yang digabungkan dengan pesan yang sudah dienkrip dengan kunci publik *penerima* tersebut kemudian dikirim bersama-sama.



Gambar 2.5 Enkripsi pada PGP

Pesan P digabungkan dengan tanda tangan pesan $SIGN$, dikompres untuk mengurangi karakter berulang sehingga lebih mempersulit *cryptanalist* untuk membongkar *ciphernya*. Kompresi dimaksudkan untuk mengurangi ukuran file akibat operasi BASE 64. Hasil kompresi P' dienkrip oleh fungsi IDEA dengan kunci simetri K_{SIM} sehingga menghasilkan cipher. Kemudian K_{SIM} ini dienkrip oleh RSA supaya dapat dikirimkan ke tujuan D (destination). Kunci yang digunakan untuk mengenkrip K_{SIM} adalah K_{PUBLIK} penerima D yaitu $K_{PUB D}$. Hasil keluarannya adalah $C_{K_{SIM}}$ yang merupakan cipher dari kunci simetri IDEA K_{SIM} . K_{SIM} ini hanya digunakan satu kali untuk setiap pesan. Setelah itu tidak dapat digunakan lagi.

Pada penerima, proses inversi dilakukan seperti pada gambar berikut :



Gambar 2.6 Proses Deskripsi dan verifikasi sign pada PGP

Proses Mendapatkan Pesan (Deskripsi)

1. Penerima menerima file berekstensi asc.
2. File dimasukkan ke dalam decoder base64 dan menghasilkan C dan $C_{K,SIM}$
3. $C_{K,SIM}$ didekrip dengan RSA menggunakan kunci privat penerima $K_{PRIV,D}$. Jadi hanya penerima D saja yang memperoleh kunci simetri IDEA K_{SIM} , karena hanya D yang mempunyai kunci privat $K_{PRIV,D}$.
4. K_{SIM} yang dihasilkan dari langkah ketiga di atas, digunakan untuk mendekrip cipher C dengan algoritma IDEA untuk menghasilkan pesan P' .
5. P' dimasukkan UNZIP untuk mendapatkan P dan SIGN .

Proses Pemeriksaan Tanda Tangan Digital

Keluaran UNZIP berupa P dan SIGN, P dimasukkan ke fungsi MD5 dan menghasilkan keluaran F' . Sedangkan SIGN dienkrip menggunakan RSA dengan kunci publik pengirim $K_{PUB,S}$. Kalau ternyata memang benar S yang menandatangani dengan $K_{PRIV,S}$, maka SIGN ini tentu dapat dibuka dengan $K_{PUB,S}$, tetapi kalau tidak berarti bukan S yang menandatangani pesan tersebut. Hasil dari proses ini adalah F (Fingerprint yang ditandatangani S). Bila $F = F'$ maka tanda tangan valid. Tetapi bila

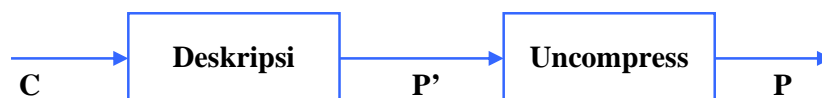
tidak sama, maka berarti pesan P yang ditandatangani S tidak sama dengan pesan yang diterima D.

c. Kompresi

Pretty Good Privacy mengkompresi pesan setelah dilakukan tanda tangan, namun sebelum enkripsi. Hal ini dilakukan demi penghematan ruang untuk pengiriman e-mail dan penyimpanan file.

Tanda tangan dibangkitkan sebelum kompresi dengan alasan :

- Lebih disukai menandatangani pesan yang belum dikompres kita tidak perlu menyimpan pesan dalam keadaan terkompres untuk pengecekan tanda tangan berikutnya. Bila seseorang menandatangani pesan yang terkompres, maka diperlukan menyimpan pesan dalam keadaan terkompres atau mengkompres ulang pesan ketika akan melakukan verifikasi..
- Algoritma kompresi tidak deterministik. Artinya hasil kompres terhadap pesan yang sama oleh software yang berbeda dapat memberikan hasil yang tidak sama. Hal ini dapat terjadi karena program kompresi memberikan pilihan antara kecepatan kompresi dengan rasio kompresi. Namun algoritma yang berda-beda dapat saling beroperasi bersama, karena setiap versi algoritma dapat dengan tepat mendekompres keluaran versi lainnya. Menjalankan fungsi hash dan tanda tangan setelah kompres akan membatasi seluruh implementasi PGP untuk menggunakan algoritma kompresi yang sama persis.
- Enkripsi pesan yang dilakukan setelah kompresi untuk memperkuat keamanan kriptografi. Karena pesan yang dikompres memiliki sedikit reduansi dibanding plaintext aslinya, sehingga analisis ciphernya menjadi lebih sulit.



Gambar 2.7 Cyptanalysis dengan kompresi

Bila C dianalisis untuk mendapatkan P,' jelas hal ini agak sulit, karena kita tidak dapat memastikan apakah P' yang kita peroleh memang benar atau tidak. Tetapi kalau kita analisis C untuk mendapatkan P, dan mengingat kompresi tidak melakukan penyandian yang sebenarnya, sehingga cukup dengan memasang program uncompress antara P dan P'. maka kompresi tidak benar-benar mempersulit analisis sandi.

b. Kompatibilitas E-mail

Ketika PGP digunakan, paling sedikit satu blok yang dikirim dienkrip. Jika hanya layanan tanda tangan yang digunakan, maka *message digest dienkrip* (dengan kunci privat RSA pengirim).

Bila layanan keamanan, pesan ditambah tanda tangan (jika ada) dienkrip (dengan kunci IDEA sekali pakai). Jika sebagian atau seluruh blok yang dihasilkan PGP, terdiri dari aliran sejumlah oktet 8-bit. Namun terdapat sistem e-mail yang hanya mengizinkan penggunaan blok yang terdiri dari teks ASCII. Untuk mengakomodasikan batasan ini, PGP memberikan layanan konversi aliran biner 8-bit menjadi karakter ASCII yang dapat dicetak

Teknik yang digunakan adalah konversi radix 64. Setiap grup terdiri dari tiga oktet biner (24 bit) dipetakan menjadi empat karakter ASCII (32 bit). Format ini juga menambahkan CRC untuk mendeteksi kesalahan transmisi. Penggunaan radix 64 menambah ukuran pesan sebanyak 33,33%.

c. Kunci-Kunci Kriptografi

Pretty Good Privacy menggunakan empat macam kunci yaitu, kunci konvensional sesi satu waktu (one time key), kunci publik, kunci privat dan kunci konvensional turunan passphrase.

Setiap pemegang kunci PGP harus menjaga file berisi pasangan kunci publik/privat miliknya serta file yang berisi kunci publik relasinya.

1. Kunci sesi dengan algoritma enkripsi IDEA digunakan untuk mengenkrip pesan untuk dikirim. Setiap kunci sesi hanya digunakan sekali dan dibangkitkan secara acak.
2. Kunci publik dengan algoritma enkripsi RSA digunakan untuk mengenkrip kunci sesi untuk dikirimkan bersama pesan. Pengirim dan penerima harus mendapatkan kunci publik rekan-rekannya.
3. Kunci privat dengan algoritma enkripsi RSA digunakan untuk mengenkrip sidik jari pesan untuk membentuk tanda tangn digital. Kunci privat hanya boleh diketahui oleh pemiliknya.
4. Kunci turunan passphrase dengan algoritma enkripsi IDEA digunakan untuk mengenkrip kuinci privat yang disimpan oleh pemilik kunci privat

Setiap kunci sesi dikaitkan dengan satu pesan dan digabungkan hanya untuk tujuan enkripsi dan deskripsi pesan tersebut. Enkripsi dan deskripsi pesan dilakukan dengan algoritma enkripsi simetri IDEA yang menggunakan kunci 128 bit.

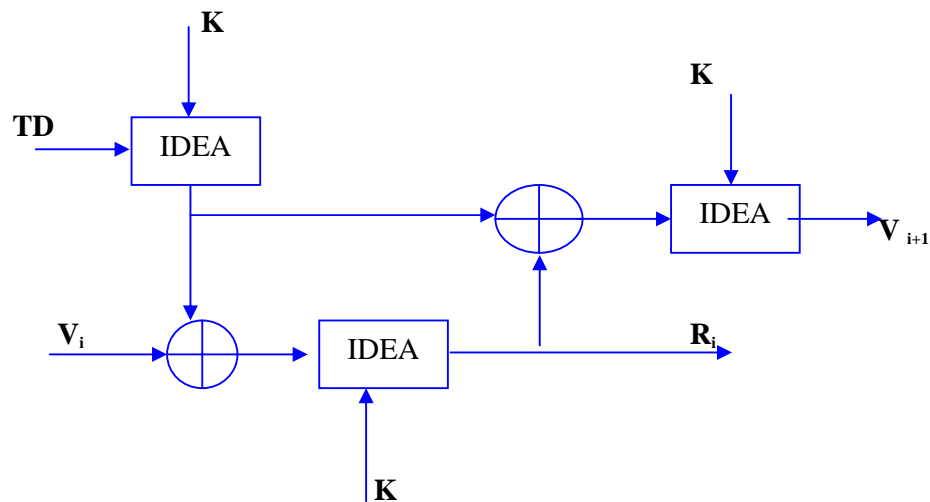
PGP menjaga bufer 256 byte sebagai bilangan acak yang sebenarnya. Setiap kali memerlukan ketikan keyboard, PGP mencatat waktu dalam format 32 bit, kemudian menunggu ketikan berikutnya. Pada saat menerima ketikan berikutnya, PGP mencatat waktu ketukan tombol keyboard dan nilai (8-bit) yang diketikkan.

Waktu dan informasi ketukan digunakan untuk membangkitkan kunci berikutnya. Bilangan acak dibangkitkan menggunakan IDEA pula. Masukkan ke pembangkit bilangan acak terdiri dari kunci simetri 128 bit dan dua blok 64 bit yang diperlakukan sebagai plaintext untuk dienkrip., yang diambil dari file bufer. Dengan mode CFB, IDEA menghasilkan dua blok ciphertext 64 bit yang digabungkan untuk membentuk kunci sesi 128 bit. Algotima yang digunakan didasarkan pada spesifikasi ANSI X9.17.

d. ANSI X9.17

ANSI X9.17 merupakan standar pembangkitan bilangan semi acak yang menggunakan 3DES sebagai algoritma utamanya. PGP mengganti 3DES dengan IDEA yang dianggap lebih terpercaya. Masukkan terdiri dari TD (Time Date) yang merupakan jam, menit, detik, milidetik, tanggal, bulan dan tahun saat pembangkitan bilangan semi acak. Dengan masukkan seperti ini, diharapkan setiap keluaran R_i (64 bit) akan selalu bergantung waktu, sehingga lebih acak keluarannya. Jam komputer dikonversi ke dalam 64 bit masukan TD.

V_{i+1} dijadikan masukan bagi V_i , atau nilai V_i sekarang merupakan nilai V_{i+1} sebelumnya. K merupakan kunci IDEA sepanjang 128 bit. Setiap IDEA dapat diberi kunci yang berbeda dari IDEA lainnya untuk meningkatkan keamanannya.



Gambar 2.8 ANSI X9.17 Modifikasi

Algoritma pembangkit bilangan semi acak yang baik akan menyulitkan lawan untuk mendapatkan bilangan semi acak berikutnya atau sebelumnya bila dia mendapatkan satu deretan bilangan tersebut. Untuk itu, ANSI X9.17 menggunakan enkripsi yang berbeda untuk menghasilkan V dan R . Bila lawan mendapatkan 64 bit keluaran bilangan semi acak R_i , maka dia masih akan sangat

kesulitan untuk mendapatkan R_{i+1} berikutnya, karena R_{i+1} bukan sekedar fungsi R_i , namun juga fungsi TD dan V yang tidak diketahuinya.

Perlu diingat bahwa bilangan acak yang sejati adalah deretan bilangan yang tidak dapat dibangkitkan lagi selamanya, termasuk oleh si pembangkit bilangan acak tersebut. Untuk itulah ditambahkan TD agar tidak dapat ditiru lagi masukan TDnya, kecuali bila anda menset supaya program tersebut bekerja pada detik, milidetik yang sama dengan sebelumnya. Tanpa dapat menset milidetik dengan tepat mengulang pembangkitan bilangan semi acak ANSI X9.17 ini.

Passphrase

Passphrase digunakan untuk melindungi kunci privat yang tersimpan dalam disk. Berikut ini dijelaskan proses enkripsi kunci privat.

Pengguna mengetikkan passphrase yang digunakan untuk mengenkrip kunci privat..

Ketika sistem membangkitkan pasangan kunci publik/privat baru dengan RSA, PGP menanyakan passphrase pengguna. Passphrase dimasukkan MD5 untuk membangkitkan kode hash 128 bit.

Passphrase dibuang.

Kunci privat dienkrip menggunakan IDEA dengan kunci yang berasal dari kode hash di atas. Kode hash dibuang, dan kunci privat yang terenkrip disimpan pada ring kunci privat.

II.6 Deskripsi Kunci Privat

Pada saat pengguna akan memakai kunci privatnya, PGP akan memintanya memasukkan passphrase. PGP memasukkan passphrase ini ke dalam MD5 dan dihasilkan kode hash. Kode hash digunakan untuk membuka enkripsi kunci privat RSA dengan IDEA. Kunci privat RSA digunakan untuk membuka kunci sesi IDEA yang terenkrip dengan kunci publik RSA.

Keamanan kunci privat ini sangat tergantung pada keamanan passphrase. Untuk itu diharapkan memilih passphrase yang mudah diingat, namun sulit ditebak orang lain. PGP memiliki dua macam bilangan acak :

1. Bilangan acak yang sebenarnya

- Digunakan untuk membangkitkan pasangan kunci RSA
- Memberikan masukan awal untuk pembangkit bilangan acak semu
- Memberi masukan tambahan selama pembangkitan bilangan acak semu
- Dinamakan bilangan acak yang sebenarnya karena tidak dapat dibangkitkan kembali.

2. Bilangan acak semu

- Digunakan untuk membangkitkan kunci sesi
- Digunakan untuk membangkitkan vektor inisialisasi untuk digunakan dengan kunci sesi dalam enkripsi mode CFB
- Dinamakan bilangan acak semu karena dapat dibangkitkan kembali.

Bilangan acak sebenarnya

PGP menyimpan 256 byte buffer atau bit-bit acak. Setiap memerlukan bit-bit ini, PGP akan merekam waktu komputer dalam format 32 bit, lalu menunggu pengguna mengetikkan ketikan acak. Ketika menerima ketikan pengguna PGP merekam waktu pengetikan.

Bilangan acak semu

Bilangan acak semu menggunakan seed 24 oktet (1 oktet = 8 bit) dan menghasilkan kunci sesi 16 oktet, vektor inisialisasi 8 oktet dan seed baru untuk digunakan bagi pembangkitan bilangan semi acak berikutnya. Algoritma didasarkan pada algoritma ANSI X9.17 dengan IDEA sebagai algoritma intinya menggantikan 3DES untuk enkripsinya. Algoritma menggunakan struktur data berikut:

➤ Input

File randseed.bin (24 oktet): Bila kosong, diisi dengan 24 oktet bilangan acak yang sebenarnya.

Pesan: Kunci sesi dan IV yang akan digunakan untuk mengenkrip pesan.

➤ Output

Struktur data internal.

BAB III

PENUTUP

Setiap orang mempunyai 2 kunci, yaitu kunci publik dan kunci pribadi. Ketika seseorang ingin mengirim sesuatu pada si penerima, pengirim mengenkrip dengan kunci publik si penerima. Namun, cara untuk mendekripnya dengan kunci pribadi si penerima. Salah satu keuntungan lain dari PGP adalah mengizinkan pengirim menandai pesan-pesan mereka. Ini membuktikan bahwa pesan datang dari pengirim dan belum ada perubahan selama perjalanan.

Berdasarkan pada teori ini, PGP mengizinkan seseorang untuk mengumumkan kunci publik mereka dan menjaga kunci pribadi yang sifatnya rahasia. Hasilnya, seseorang dapat mengenkrip pesan kepada orang lain sepanjang mereka mempunyai kunci publik.

PGP adalah suatu metode enkripsi informasi yang bersifat rahasia sehingga jangan sampai diketahui oleh orang lain yang tidak berhak. Informasi ini bias berupa E-mail yang sifatnya rahasia, nomor kode kartu kredit, atau pengiriman dokumen rahasia perusahaan melalui Internet. PGP menggunakan metode kriptografi yang disebut “*public key encryption*”: yaitu suatu metode kriptografi yang sangat *sophisticated*.

Adapun prinsip kerja dari PGP adalah sebagai berikut :

1. PGP, seperti yang telah dijelaskan sebelumnya, menggunakan teknik yang disebut *public key encryption* dengan dua kode. Kode-kode ini berhubungan secara intrinstik, namun tidak mungkin untuk memecahkan satu sama lain,
2. ketika dibuat satu kunci, maka secara otomatis akan dihasilkan sepanjang kunci, yaitu kunci publik dan kunci rahasia,
3. mengapa menggunakan dua kunci? Karena dengan *conventional crypto*, di saat terjadi transfer informasi kunci, diperlukan suatu *secure channel*. Jika kita memiliki suatu *secure channel*, mengapa masih menggunakan *crypto*? Dengan *public key system*, tidak akan menjadi masalah siapa yang melihat kunci milik kita, karena kunci yang dilihat orang lain adalah yang digunakan hanya untuk enkripsi dan hanya pemiliknya saja yang mengetahui kunci rahasia tersebut.

DAFTAR PUSTAKA

- [1] Aninymous, *Memahami Model Enkripsi dan Security Data*, Wahana Komputer Semarang dan Andi Yogyakarta, 2003
- [2] Kristianto A., *Keamanan Data Pada Jaringan Komputer*, Gava Media Yogyakarta, 2003
- [3] Utdirartatmo F., *Analisa Keamanan dan Vulnerabilitas Jringan Komputer*, Gava Media Yogyakarta, 2004
- [4] Kurniawan Y.Ir.MT., *Kriptografi Keamanan Internet dan Jaringan Komunikasi*, Informatika Bandung, 2004
- [5] McClure S, Shah S, Shah S., *Web Hacking Serangan dan Pertahanannya*, Andi Yogyakarta, 2003
- [6] arya@kde.org, <http://ariya.pandu.org/>)
- [7] <http://www.pgp.org/>
- [8] <http://www.ifi.uio.no/pgp/utills.shtml>.
- [9] <http://mt.direktif.web.id/cgi-bin/mt-tb.cgi/212>