# PGP, Aplikasi Pengaman Data

Ade Setyawan
*Program Studi Teknik Informatika*
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung, Jl Ganesha 10 Bandung 40132, Indonesia*
*13509075@std.stei.itb.ac.id*

**Abstrak**

PGP adalah Suatu metode program enkripsi informasi yang memiliki tingkat keamanan cukup tinggi bersifat rahasia dengan menggunakan "Private-Public Key" sebagai dasar autentifikasinya sehingga jangan sampai dengan mudah diketahui oleh orang lain yang tidak berhak. Informasi ini biasanya berupa surat elektronik (E-mail) yang sifatnya rahasia, nomor kode kartu kredit, atau pengiriman dokumen rahasia perusahaan melalui internet. Pada dasarnya PGP merupakan program yang digunakan untuk mengenkripsi satu atau lebih dokumen. Dengan PGP tersebut, hanya orang tertentu saja yang bisa membaca file – file enkripsi tersebut. Kesimpulannya yaitu PGP berguna untuk mengamankan data pada suatu email dan PGP bekerja dengan cara mengenkripsi dan dekripsi.

Kata kunci :enkripsi, dekripsi

## 1. PENDAHULUAN

Email telah menjadi sesuatu yang sangat penting aplikasinya di abad ini, penerapannya dapat kita temukan dalam kehidupan sehari-hari. Isi dari email pun beragam, mulai sekedar obrolan antar sahabat, perjanjian perdagangan, sampai dengan rahasia Negara. Oleh karena semakin pentingnya data-data yang terdapat dalam email, maka diperlukan suatu aspek keamanan yang dapat menjamin keaslian dari suatu data tersebut ( bentuk dan isi) dan kerahasiaan dari data tersebut. Ilmu yang mempelajari mengenai cara untuk menjaga keamanan dari suatu data disebut kriptografi. Salah satu aplikasi dari kriptografi ini adalah enkripsi-dekripsi.

Untuk memastikan bahwa data yang dikirim adalah asli, maka ditiap data tersebut diberikan suatu tanda digital (digital signature). Tanda tersebut mempunyai sifat unik sehingga dia mempunyai kemampuan untuk membedakan data antara satu pengirim dengan pengirim lainnya. Selain itu dia juga mempunyai sifat sulit di tiru orang lain serta dapat menjaga integritas pesan yang ditandai. Pemberian digital signature dapat dilakukan melalui dua cara, yaitu

1. Enkripsi pesan melalui algoritma kunci simetri maupun dengan algoritma kunci public.

2. Melakukan fungsi hash terhadap pesan. Hasil fungsi hash merupakan digital signature atas pesan dan di tambahkan ke dalam pesan.

Sifat ini bertujuan agar tidak terjadinya pengubahan isi pesan oleh pihak ketiga di tengah jalan.

Untuk menjalankan proses di atas (enkripsi-dekripsi/kriptografi), terdapat suatu alat bantu yaitu PGP. PGP berfungsi untuk mengamankan suatu data dari email dengan menggunakan system 2 kunci,yaitu kunci privat (mengubah suatu pesan menjadi pesan yang telah di enkripsi) dan kunci public (mengubah pesan terenkripsi menjadi pesan sesungguhnya).

## 2. PENJELASAN MENGENAI PGP

**PGP** (*Pretty Good Privacy*) adalah suatu metode program enkripsi informasi yang memiliki tingkat keamanan cukup tinggi bersifat rahasia dengan menggunakan "Private-Public Key" sebagai dasar autentifikasinya sehingga jangan sampai dengan mudah diketahui oleh orang lain yang tidak berhak. **PGP** dikembangkan oleh **Phill Zimmermann** pada akhir tahun1980. pada awal mulanya , PGP digunakan untuk melindungi surat elektronik (*e-mail*) dengan memberikan perlindungan kerahasiaan (*enkrips*i) dan otentikasi (*tanda – tangan digital*). Untuk itu Phill Zimmermnn membuat sebuah program yang digunakan agar dapat melindungi informasi data dengan kerahasiaan. Program yang dibuat oleh Phill Zimmerann memiliki 2 versi yaitu "*USA Version* " dan "*International Version*". PGP versi USA hanya dapat digunakan di wilayah USA dan oleh warganegara USA saja. PGP versi USA ini menggunakan algoritma **RSA** (yang telah menjadi hak paten) dalam enkripsinya. Sedangkan versi internasional menggunakan algoritma **MPILIB** yang diciptakan khusus oleh Phill Zimmermann sendiri. PGP Versi internasional bisa digunakan oleh seluruh dunia.

Pada dasarnya, PGP merupakan program yang digunakan untuk mengenkripsi satu atau lebih dokumen. Dengan PGP tersebut, hanya orang – orang tertentu saja yang bisa membaca file – file enkripsi tersebut. Bagaimana PGP sebagai program enkripsi dokumen bisa digunakan untuk pengiriman e-mail? Sebenarnya, program PGP mengenkripsi isi mail yang kita tulis menjadi sebuah file. File tersebut dibaca oleh program mail yang kemudian dikirimkan ke tujuan.

Penerima e-mail harus menyimpan mail tersebut ke dalam sebuah file. File tersebut dideskripsi sehingga isi mail aslinya akan terlihat. Jadi, mail yang dikirimkan adalah dalam bentuk terenkripsi sehingga tidak dapat dibaca dengan mudah oleh orang – orang yang tidak memiliki akses membaca mail tersebut.

Kekuatan PGP terletak pada lamanya waktu yang diperlukan untuk membongkar kunci-kunci PGP. Untuk membongkar satu kunci PGP memerlukan waktu prosesor computer jutaan tahun bahkan milyaran tahun. Mungkin saja kecepatan processor computer berkembang 100 kali lipat dari sekarang, namun tetap membutuhkan waktu lebih dari 1000 tahun. Kalaupun berhasil di pecahkan, informasi tersebut tidak ada gunanya lagi. Selain itu kekuatannya juga terletak pada system kunci 1024 bit bahakan hingga 4096 bit. Kalau dihitung secara matematis, anda akan memiliki kunci kombinasi dengan angka sebesar 300 digit.

Berikut ini merupakan alasan menggunakan PGP :

◆ 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 si pengirim 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.

◆ PGP dapat diperoleh secara gratis untuk penggunaan pribadi. Kita dapat mendownload softwarenya 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

Walaupun system enkripsi/dekripsi PGP sangat kuat, namun ada faktor-faktor di luar PGP yang bias melemahkannya. Misalkan data recovery dari swap file serta kehilangan private key dan pass-phrase. Selain itu, karena programnya adalah open source, maka siapa saja bisa mengambil source code dan menyisipkan semacam program kecil (untuk mengintip bahkan mencuri rahasia) dan kemudian menyebarkannya kembali secara umum. Untungnya, untuk mengatasi masalah ini PGP sudah dilengkapi dengan signature sehingga anda bisa memeriksa apakah PGP yang anda download adalah asli atau bukan.

## 3. METODE KERJA PGP

PGP bekerja dengan menggabungkan beberapa bagian yang terbaik dari kunci privat(simetrik) dan kunci public., sehingga sering disebut hybrid chryptosystem..Ketika seorang pengguna mengenkrip sebuah plaintext dengan menggunakan PGP, maka awal PGP akan mengkompress plaintext ini.. Data yang dikompress menghemat waktu, media transmisi dan yang lebih penting adalah keamanan kriptografi yang kuat. Kebanyakan teknik analisis sandi mengeksplotasi pola yang ditemukan dalam plaintext untuk men-crack chipper. Kompressi mengurangi pola-pola ini dalam plaintext dengan cara demikian perbaikan yang lebih baik untuk menghambat analisa kode-kode.

PGP membuat sebuah session key, yaitu sebuah kunci rahasia berupa bilangan acak pada saat itu. Session key ini berkerja dengan sangat aman, algoritma enkripsi konvesional yang cepat untuk meng-enkrip plaintext. Hasilnya adalah berupa chipper text. Sekali data dienkripsi, lalu session key ini dienkripsi lagi menggunakan kunci publik penerima.Session key yang terenkripsi kunci publik penerima dikirim dengan chipertext ke penerima

Proses deskripsi bekerja sebaliknya, penerima menerima pesan lalu membuka pesan tersebut dengan kunci pribadinya, namun pesan tersebut masih terenkripsi dengan session key. Dengan menggunakan PGP, penerima mendekrip chipertext*t* yang terenkripsi secara konvensional.

Sebuah kunci (key) adalah sebuah nilai yang bekerja dengan sebuah algoritma kriptografi untuk menghasilkan sebuah chipertext*t* yang spesifik. Kunci pada dasarnya adalah bilangan yang besar.

Ukuran kunci publik dan ukuran kunci rahasia kriptograpi tidak saling barhubungan. Sebuah kunci 80-bit konvensional memiliki kekuatan setara dengan kunci publik 1024-bit. Sebuah kunci 128-bit konvensional setara dengan kunci publik 3000-bit. Jadi semakin besar kunci semakin aman, tetapi algoritma yang digunakan tiap tipe kriptograpi sangat berbeda dan perbedaan ini seperti orang membandingkan antara apel dengan jeruk.

Sementara secara matematis kunci publik dan pribadi berhubungan. Sangat sulit mendapatkan kunci pribadi hanya dengan memberikan kunci publiknya, tetapi mendapatkan kunci pribadi selalu memungkinkan jika diberikan waktu yang cukup dan kekuatan komputasi cukup.

Hubungan antara kunci public dan kunci pribadi dapat dijelaskan oleh algoritma RSA. Penjelasan mengenai algoritma RSA terdapat di akhir dari penjelasan mengenai metode kerja PGP.

Kunci disimpan dalam bentuk terinkripsi. PGP menyimpan kunci dalam 2 file pada dihardisk, satu untuk kunci publik dan satunya lagi untuk kunci pribadi. File-file ini disebut dengan keyrings. Dalam menggunakan PGP, secara khusus akan ditambahkan kunci publik penerima ke keyring publik. Kunci pribadi disimpan pada keyring pribadi. Jika kehilangan keyring pribadi, maka tidak akan dapat melakukan dekripsi terhadap informasi yang telah terenkripsi pada ring tersebut

**Prinsip – prinsip kerja dari PGP itu sendiri adalah :**

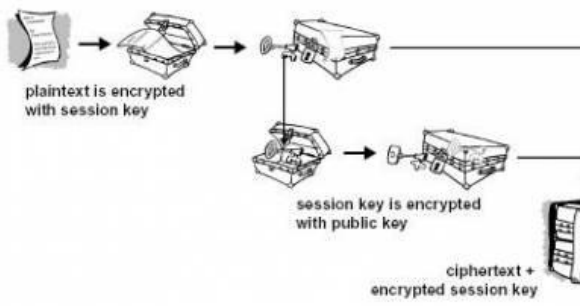
**1.** PGP menggunakan teknik yang disebut Public-key encryption dengan dua kode yang saling berhubungan secara intrinsik, namun tidak mungkin untuk memecahkan satu dan yang lainnya.

**2.** Jika membuat suatu kunci, secara otomatis akan dihasilkan sepasang kunci yaitu public key dan secret key. Kita dapat memberikan public key ke manapun tujuan yang kita inginkan, melalui telephone, internet, keyserver, dsb. Secret key yang disimpan pada mesin kita dan menggunakan messager decipher akan dikirimkan ke kita. Jadi orang yang akan menggunakan public key kita (yang hanya dapat didekripsi oleh oleh secret key kita), mengirimkan messages kepada kita , dan kita akan menggunak an secret key untuk membacanya.

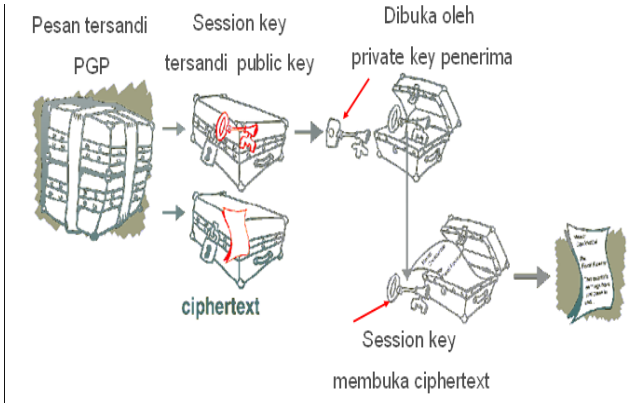
**3.** PGP menggunakan dua kunci yaitu kunci public (proses enkripsi) dan privet (proses deskripsi).

**4.** Menggunakan dua kunci tersebut dikarenakan adanya conventional crypto, disaat terjadi transfer informasi kunci, suatu secure channel diperlukan. Dan jika kita memiliki suatu secure channel, tapi mengapa kita menggunakan crypto? Namun dengan public-key syistem, tidak akan menjadi masalah siapa yang melihat kunci milik kita, karena kunci yang dilihat oleh orang lain adalah yang digunakan hanya untuk enkripsi dan hanya pemiliknya saja yang mengetahui kunci rahasia tersebut

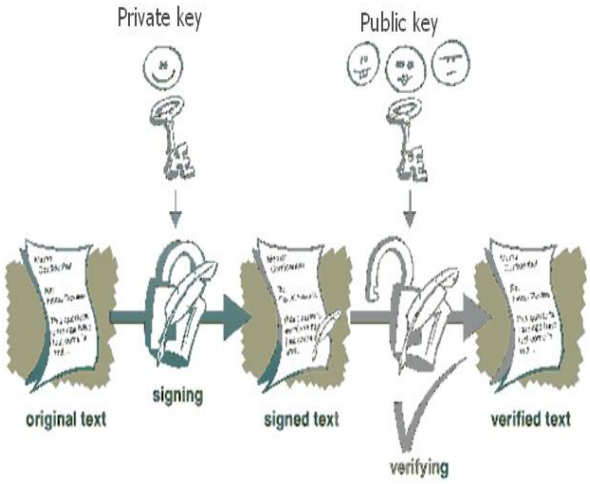
Penyandian PGP




Membuka sandi PGP




Digital Signature




**Penjelasan Mengenai Algoritma RSA**

Algortima RSA dijabarkan pada tahun 1977 oleh tiga orang : Ron Rivest, Adi Shamir dan Len Adleman dari Massachusetts Institute of Technology. Huruf RSA itu sendiri berasal dari inisial nama mereka (Rivest—Shamir—Adleman).

Besaran-besaran yang digunakan pada algoritma RSA:

1. p dan q bilangan prima (rahasia)
2. $r = p \cdot q$ (tidak rahasia)
3. $m = (p – 1)(q – 1)$ (rahasia)
4. PK (kunci enkripsi) (tidak rahasia)
5. SK (kunci dekripsi) (rahasia)
6. X (plainteks) (rahasia)
7. Y (cipherteks) (tidak rahasia)

Prosedur membuat pasangan kunci dapat dijelaskan melalui beberapa langkah di bawah ini

1. Hasilkan dua buah integer prima besar, p dan q untuk memperoleh tingkat keamanan yang tinggi pilih p dan q yang berukuran besar, misalnya 1024 bit.

2. Hitung m = (p-1)*(q-1)
3. Hitung n = p*q
4. Pilih d yg relatively prime terhadap m e relatively prime terhadap m artinya faktor pembagi terbesar keduanya adalah 1, secara matematis disebut gcd(e,m) = 1. Untuk mencarinya dapat digunakan algoritma Euclid.
5. Cari d, sehingga e*d = 1 mod (m), atau d = (1+nm)/e Untuk bilangan besar, dapat digunakan algoritma extended Euclid.
6. Kunci publik : e, n Kunci private : d, n

Misalkan B akan mengirim pesan ke A, maka yang harus dilakukan oleh B adalah:

1. Ambil kunci publik A yg otentik (n, e)
2. Representasikan message sbg integer M dalam interval [0,n-1]
3. Hitung C = M ^ e (mod n)
4. Kirim C ke A

Sedangkan untuk proses dekripsi, A harus menggunakan kunci pribadi d untuk menghasilkan
M = C^(d) (mod n)

## 4. 1. CARA MENDAPATKAN PGP

Program PGP "*International version*" merupakan shareware dan dapat didownload dari beberapa ftp server sebagai berikut :

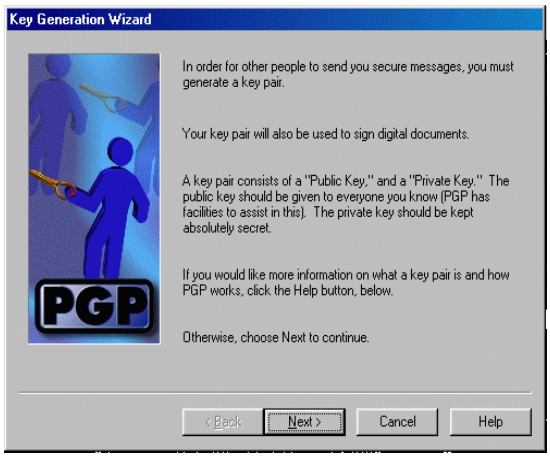
- **ftp://ftp.ifi.uio.no/pub/pgp/(primary)**
- **ftp://ftp.ox.ac.uk/pub/crypto/pgp/**
- **ftp://ftp.dsi.unimi.it/pub/security/crypt/PGP/**
- **ftp://ftp.informatik.uni-hamburg.de/pub/virus/crypt/pgp/**

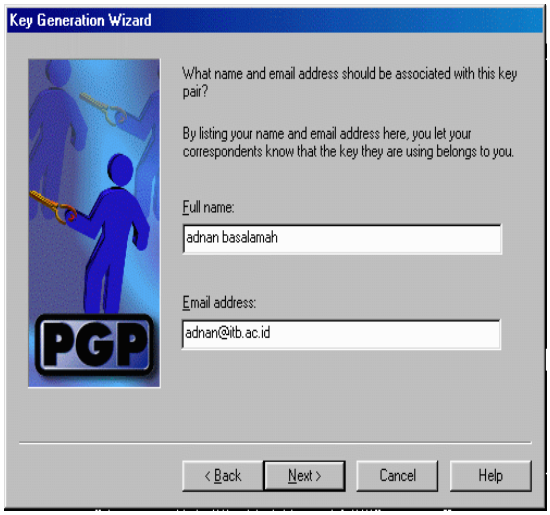
Program PGP tersedia dalam berbagai platform seperti MS-Dos, Macintosh, Unix, VMS, OS/2, Atari, dlsb. Untuk platform MS-Dos sendiri, terdapat dua jenis yaitu *pgp263i.zip* (16 bit) dan *pgp263ix.zip* (32 bit). Untuk versi 32 bit, terdapat perbedaan pada kecepatan proses enkripsi dan pembuatan key dibandingkan dengan versi 16 bit.

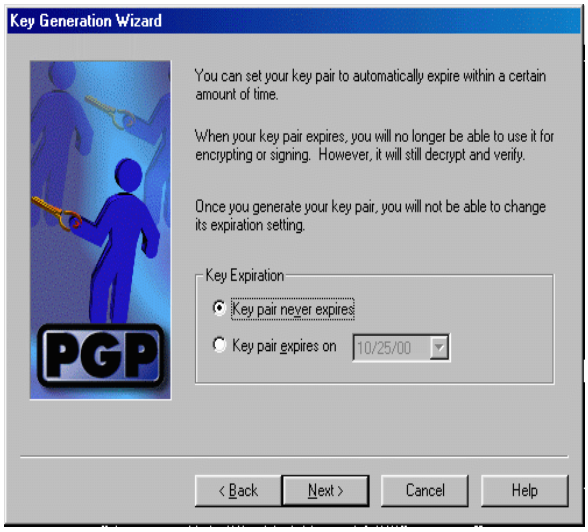
PGP juga tersedia sebagai *freeware* maupun sebagai paket komersil dalam berbagai versi yang dapat dioperasikan dalam berbagai sistem operasi (DOS, Windows, UNIX, Mac). Program PGP dapat didownload gratis dari situs www.pgp.org atau www.pgpi.org.

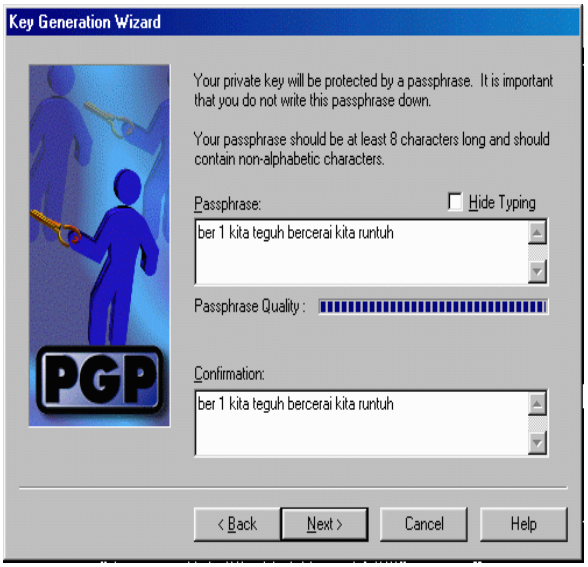
## 4.2. CARA MENGGUNAKAN PGP

Membuat Public Private Key

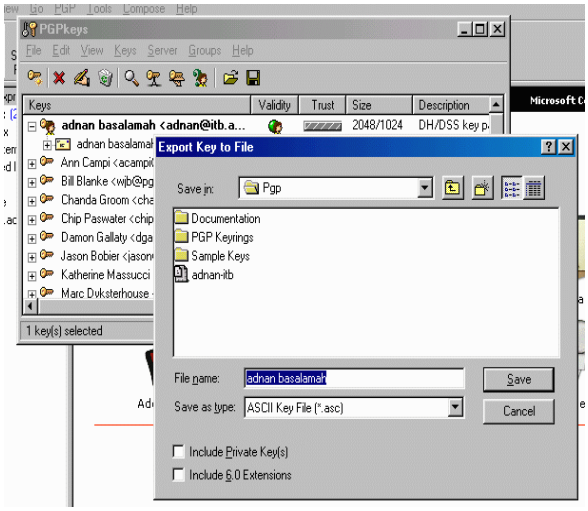


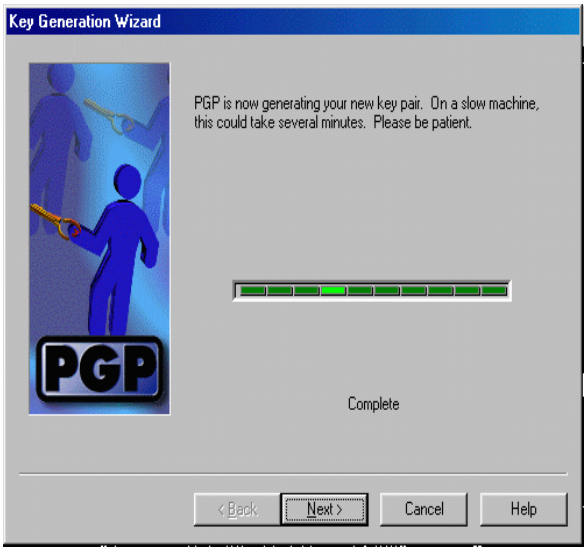



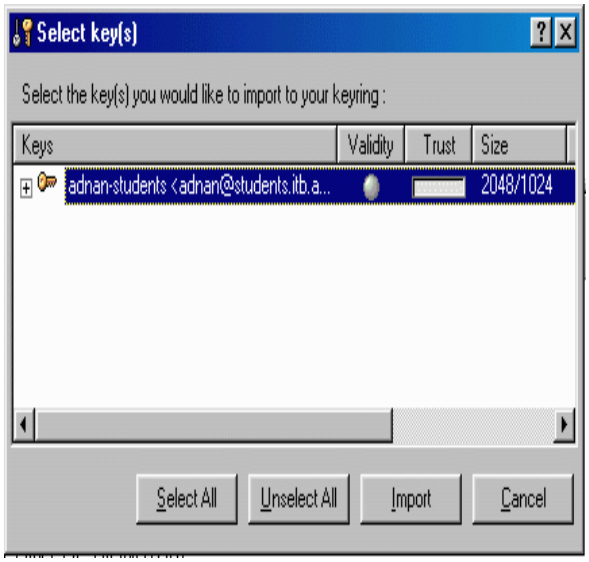


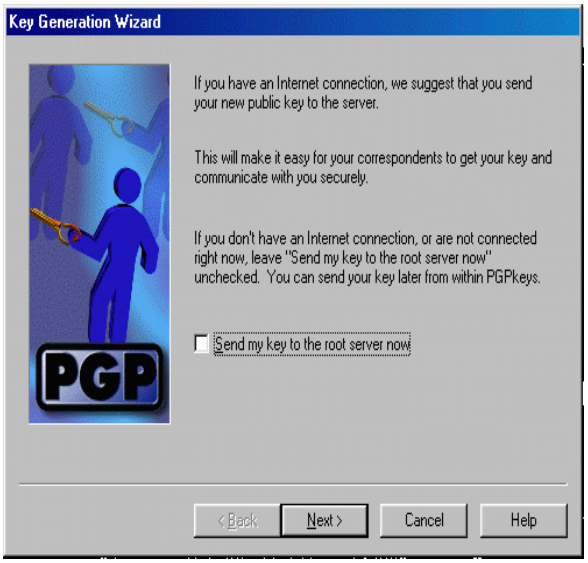

Mengeksport public key



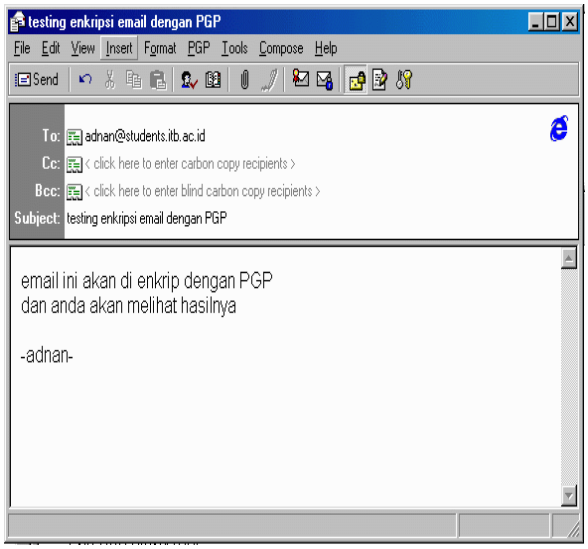



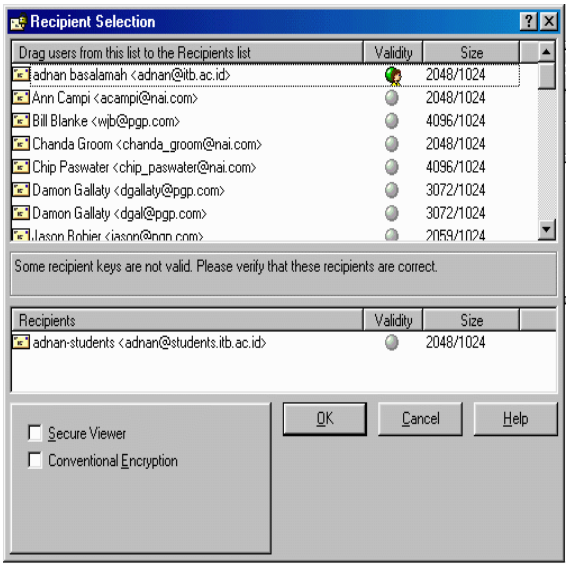

Mengimport public key

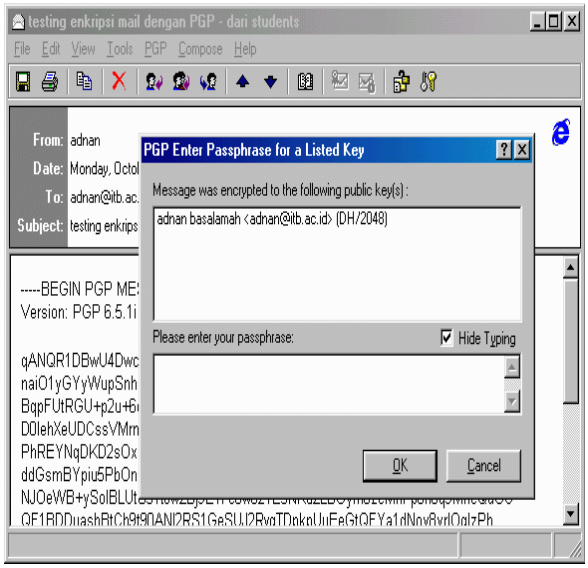


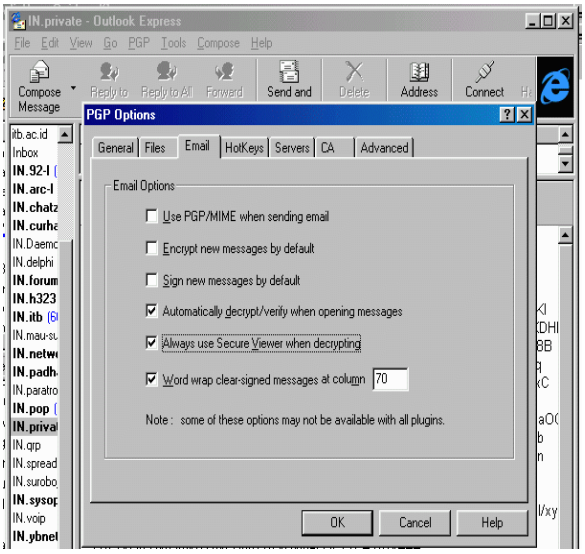

Mengirim email

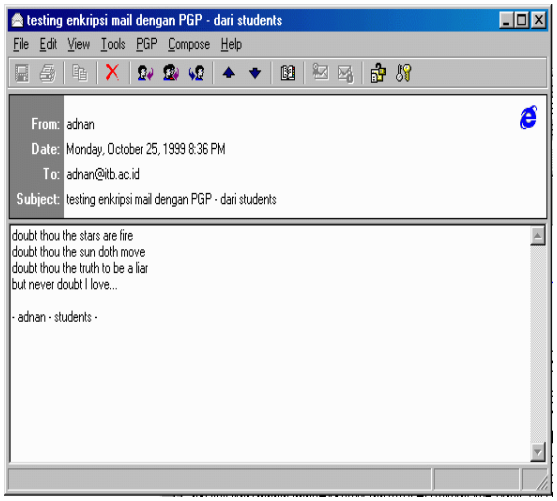





Membaca email





## 6. KESIMPULAN

- PGP berguna untuk mengamankan data pada suatu email
- PGP bekerja dengan cara mengenkripsi dan dekripsi

## DAFTAR PUSTAKA


[1] http://www.wikipedia.org. 9 Desember 2010 11:32

[2] http://i-solution.web.id. 11 Desember 2010 11:00

[3] http://lecturer.eepis-its.edu. 11 Desember 2010 8:00

[4] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung

[5] http://kuliahprogram.blogspot.com 10 Desember 2010 17:00

[6] http://google.com 9 Desember 2010 20:00

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 29 April 2010

Ade Setyawan
13509075