PGP (PRETTY GOOD PRIVACY)

Teddy Iskandar & Firman M Priyatna
Officer Development Program (ODP)
Bank Bukopin - ITB

Urusan Teknologi Pengembangan Sistem Informasi (UTPSI)
Bank Bukopin
Jalan MT Haryono Kav 50-51 Jakarta 12770

E-mail : ted@bukopin.co.id, firmanmp@bukopin.co.id

Abstrak

Bila anda suka berkirim surat melalui e-mail, yakinkah anda bila e-mail tersebut "aman" (orang lain tidak dapat baca ?). Siapapun anda, pasti tidak menginginkan e-mail pribadi ataupun data pada file anda dibaca oleh orang lain. Penggunaan password-pun belum mendukung keamanan e-mail tersebut. Selain tentang e-mail, bagaimana perasaan anda bila orang lain membaca data file milik anda pribadi ?. Salah satu solusinya adalah menggunakan program PGP (*Pretty Good Privacy*) yang dapat meng-enkripsi / *encryption* (proses untuk membuat pesan / email dan file tidak dapat dibaca tanpa menggunakan kunci pembuka) dan membuat tanda tangan digital / *digital signature* (sebagai otentikasi) sehingga masalah "pengamanan" dalam berkirim e-mail maupun dalam penyimpanan data file anda terjamin.

***Kata kunci**:e-mail, file, PGP, encryption, digital signature*

1. Pendahuluan

Pada awalnya PGP ditujukan untuk mengamankan pengiriman pesan / email, tapi sekarang ini PGP juga dapat digunakan untuk mengamankan berbagai file dan program pada komputer personal (PC).

PGP diciptakan oleh Zimmermann pada akhir tahun 1980, dalam proses penciptaan PGP Zimmermann melakukan usaha-usaha sebagai berikut :

a. Memilih algoritma kriptografi kunci asimetris / publik (*Public Key Crytography*) terbaik yang ada (IDEA, RSA) dan MD5 (sebagai fungsi *hash*) sebagai komponen dasar pembentuk PGP

b. Mengintegrasikan algoritma-algoritma kriptografi ini ke dalam aplikasi PGP.

c. Membuat paket dan dokumentasinya serta dapat diakses secara gratis melalui internet, *bulletin board* dan jaringan komersial semacam AOL (America On Line).

d. Tersedia gratis ke seluruh dunia dalam berbagai versi yang dapat berjalan dalam berbagai *operating system* / *platform* termasuk DOS, Windows, UNIX, Machintosh dan masih banyak lagi lainnya.

e. PGP tidak dikembangkan atau dikontrol oleh organisasi tertentu maupun oleh pemerintah, sehingga aplikasi PGP menjadi lebih menarik digunakan.

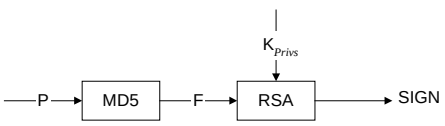
2. Cara Kerja Program PGP

Program PGP melakukan lima operasi utama yaitu :

a. Otentikasi

Selain mengenkripsi pesan / email dan file, PGP juga dapat memberi tanda tangan digital. Adapun tujuan dari proses tersebut adalah sebagai otentikasi dari pesan / file yang bertujuan untuk memastikan / mengecek apakah file tersebut masih asli atau sudah dirubah oleh orang lain atau bisa juga sudah terserang oleh virus ataupun trojan.

Misalnya ada pesan M ditanda tangani A menghasilkan F



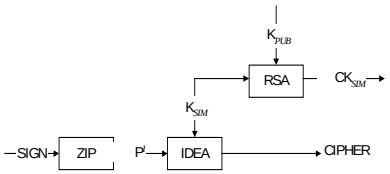
Gambar 1 Tanda tangan digital

Dari gambar terlihat bahwa pesan (P) dimasukkan kedalam fungsi MD5 yang menghasilkan sidik jari (F). Sidik jari tersebut adalah identitas pesan. Sidik jari (F) ditanda tangani oleh pengirim (sumber S) menggunakan kunci privat $K_{Priv\,S}$.

Ingat bahwa kunci yang digunakan untuk menandatangani adalah kunci privat pengirim bukan penerima. Hasil tanda tangan pesan P adalah SIGN. P dan SIGN akan digunakan pada bagian enkripsi dibawah ini.

b. Kerahasiaan

PGP menggunakan algoritma IDEA (*International Data Encryption Algorithm*) dengan kunci 128 bit untuk menyandikan data (pesan / file) dan menggunakan mode *Chiper Fedd Back* (CFB) dengan menggunakan vector awal (*Initialization Vector IV*) nol. Hal yang perlu diperhatikan adalah distribusi kunci dalam PGP, setiap kunci konvensional hanya digunakan sekali. Artinya setiap kali ada pesan yang akan dienkrip dibangkitkan kunci baru 128 bit secara acak. Meskipun dalam dokumentasi kunci ini disebut sebagai kunci rahasia / *simetri*. Karena digunakan Cuma sekali maka kunci *simetri* ini digabungkan dengan pesan yang sudah dienkrip dengan kunci tersebut kemudian dikirim bersama-sama. Dan untuk melindunginya, kunci *simetri* tersebut dienkrip dengan kunci publik penerima.



Gambar 2 Enkripsi pada PGP

Pesan P digabungkan dengan tanda tangan pesan SIGN, dikompres untuk mengurangi karakter berulang sehingga lebih mempersulit *cryptanalyst* untuk membongkar *chiper*nya. Kompresi juga dimaksudkan untuk mengurangi ukuran file sebagai akibat membesarnya file akibat operasi BASE-64.

Hasil kompresi P^I dienkrip oleh fungi IDEA dengan kunci simetri K_{SIM} sehingga menghasilkan cipher. Kemudian K_{SIM} ini dienkrip oleh RSA (nama penemu algoritma tersebut ***R**on Rivest, Adi **S**hamir and Leonard **A**dleman*) supaya dapat dikirimkan ke tujuan. Kunci yang digunakan untuk mengenkrip K_{SIM} adalah K_{PUB} hasil keluarannya adalah CK_{SIM}

c. Kompresi
PGP mengkompres pesan setelah ditanda tangan tapi sebelum diengkripsi.
Adapun alasannya sebagai berikut :
   a. Lebih disukai menandatangani pesan yang belum di kompres sehingga kita tidak perlu menyimpan pesan dalam keadaan terkompres untuk pengecekan tanda tangan.
   b. Algoritma kompresi tidak deterministic (hasil kompresi dengan pesan yang sama oleh software yang berbeda menghasilkan kompresan yang berbeda)
   c. Enkripsi pesan yang dilakukan setelah kompres bertujuan untuk memperkuat keamanan kriptografi.Hal itu dikarenakan pesan yang telah dikompres memiliki sedikit redundansi disbanding plaintext aslinya, sehingga analisis chipernya menjadi lebih sulit.

d. 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). Dan bila layanan keamanan, pesan ditambah tanda tangan (jika ada) dienkrip (dengan kunci IDEA sekali pakai), jadi sebagian atau seluruh blok yang dihasilkan PGP teridiri dari aliran sejumlah okte 8-bit. Namun terdapat system email yang hanya mengijinkan penggunaan blok yang terdiri dari teks ASCI. Untuk mengakomodasi batasan itu, PGP memberikan layanan untuk mengkonversi aliran okte 8-bit menjadi karakter ASCI yang dapat dicetak. Teknik yang digunakan untuk tujuan ini adalah konversi radix 64 (setiap grup yang terdiri dari tiga octet biner (24 bit) dipetakan menjadi empat karakter ASCI (32bit)).

e. Segmentasi.
Fasilitas email sering membatasi maksimum panjang maksimum pesan. Contohnya banyak fasilitas di internet hanya dapat menerima pesan maksimal panjangnnya 50.000 *octets*. Untuk mengakomodasi hal tersebut PGP secara automatis melakukan *subdivides* pesan yang besar kedalam segment yang besarnya cukup untuk dikirim via email. Segmentasi tersebut dijalankan setelah semua proses dijalankan termasuk proses konversi radix 64. Untunglah, kunci simetri dan bagian tanda tangan pesan relative kompak, ditambah pesan sudah dikompres.

3. Kunci – kunci Kriptografi

PGP menggunakan empat macam jenis kunci sebagai berikut :

a. Kunci konvensional simetri satu waktu (*one time key*).
   Algoritma kriptografi yang digunakan adalah IDEA dan digunakan untuk mengenkrip pesan untuk dikirmkan. Setiap kunci simetri hanya digunakan sekali dan dibangkitkan secara acark.

b. Kunci Publik.
   Algoritma kriptografi yang digunakan adalah RSA dan digunakan untuk mengenkrip kunci simetri untuk dikirimkan bersama pesan. Pegirim dan penerima harus mendapatkan kunci publik rekan-rekannya.

c. Kunci Pribadi.
   Algoritma kriptografi yang digunakan adalah RSA dan digunakan untuk mengenkrip sidik jari pesan untuk membentuk tanda tangan digital. Kunci privat ini hanya boleh diketahui oleh pemiliknya.

d. Kunci Turunan Passphrase.
   Algoritma kriptografi yang digunakan adalah IDEA dan digunakan untuk mengenkrip kunci privat yang disimpan oleh pemilik kunci privat.

4. Kesimpulan

Dari analisa dan beberapa literature tentang program PGP dapat disimpulkan sebagai berikut :

a. Keamanan program PGP didapat karena menggunakan system kriptografi kunci-publik (kunci asimetris) yaitu 2 buah kunci (kunci pribadi dan kunci publik) dan didukung juga oleh algoritma kriptografi kunci publik IDEA, RSA dan algoritma MD5 (fungsi hash) yang memang sampai saat ini masih belum ada cara / algortima yang efisisien untuk memecah ketiga algoritma kriptogafi tersebut.

b. Pada prinsipnya program PGP menggunakan dua buah kunci / key, dimana setiap orang secara otomatis akan memiliki dua buah kunci/key masing – masing yaitu :

   a. Kunci Publik (*public key*)
      Kunci ini dapat diberitahukan dan diketahui oleh setiap orang. Gunanya adalah apabila orang lain mau kirim e-mail ke anda, orang itu dapat menggunakan kunci publik tersebut untuk mengenkripsi e-mail tersebut sehingga tidak dapat terbaca oleh orang lain. Anda tidak perlu kuatir, karena hanya anda yang dapat membaca e-mail tersebut. Untuk membaca e-mail yang ter-enkripsi diperlukan kunci pribadi, kunci publik ditambah password yang dikombinasikan bersama-sama oleh program PGP.

   b. Kunci Pribadi (*private key*)
      Kunci ini hanya diketahui oleh anda sendiri. Gunanya adalah apabila anda ingin orang lain tidak dapat membaca data file pribadi maka data tersebut dapat di-enkripsi menggunakan kunci pribadi. Untuk membuka e-mail yang di-enkripsi dengan kunci publik milik anda.

c. Walaupun program PGP sampai saat ini dianggap sebagai program enkripsi yang powerful karena menggunakan algoritma kunci-publik (*Public Key Crytography*) yang baik, tetapi menurut penulis sangatlah tidak tepat dan bijak bila kita terlalu mengandalkannya. Hal ini dikarenakan karena untuk memdapatkan program PGP, kita hanya tinggal mendownloadnya dari internet, dan berarti kita menyerahkan keamanan kita pada orang asing.
   Yakinkah anda bahwa implementasi PGP yang ada di internet itu :

   a. Bebas dari *trapdoor*.

   b. Bebas dari *trojan* yang akan menangkap *passphrase* kita dan selanjutnya akan mengirimkan *passphrase* beserta kunci privat kita pada orang lain.

   c. Bagaimana kita yakin bahwa pembangkitan bilangan acak pada PGP sesuai dengan teorinya.

   d. Bagaimanan kalau PGP yang kita download ternyata selalu hanya membangkitkan bilangan acak pada rentang yang sangat terbatas sehingga dengan mudah dapat difaktorkan.

   e. Bagaimana kita yakin bahwa NSA (*National Security Agency*), Lembaga Keamanan Nasional Amerika belum berhasil menemukan cara membobol algoritma IDEA (salah satu algoritma kriptografi yang di gunakan di aplikasi PGP).

   f. Bagaimana kita yakin bahwa para matematikawan belum menemukan cara pemfaktoran biilangan yang jauh lebih efisien (hal yang menjadi kekuatan dari algoritma kriptografi RSA yang digunakan juga di program PGP).

   g. Mungkin kita berfikir, bukankah PGP mnyediakan source codenya sehingga kita dapat membacanya apakah kode tersebut berisi program yang berbahaya atau tidak ?. Namun banyakkah dari pengguna PGP yang dapat membaca dan mengerti kode tersebut ?, Mungkin hanya para pakarlah yang sanggup membacanya, bahkan Zimmermann, sang pencipta PGP pun mengatakan hal tersebut

Oleh karena itu, penulis menyarankan agar setiap proses PGP dilakukan secara offline, kemudian dicopy-kan ke disket dan dipindahkan ke komputer yang terhubung ke internet. Bila pengiriman ke komputer lain tersebut dilakukan melalui jaringan, maka dikuatirkan Trojan yang ada pada komputer kita (bila ada, tentunya) akan segera bereaksi.
Kalau kita menggunakan program semacam MS Word, mungkin ucapan sebagian orang yang mengatakan “ *kita tidak perlu membuat sendiri MS Word, karena toh mudah diperoleh (secara gratis)*

dan lagi pula lebih bagus dari buatan kita sendiri ”penyataan tersebut tidaklah terlalu salah. Namun bila program tersebut menyangkut masalah keamanan komputer maka sikap ini merupakan tindakan yang sangat keliru.

Bandingkan dengan semangat meneliti bangsa asing. Meskipun sudah mendapat system operasi Windows, mereka mau membuat system operasi lain semacam Linux. Sementara kita mungkin akan berfikir untuk apa susah – susah membuat Windows dan akhirnya kita hanya dapat menjadi pengguna / pemakai (*user*) tanpa ada keinginan untuk dapat menciptakan (*create*) dan mengembangkan (*development*) sendiri program-program yang baru dan system operasi yang baru yang dapat bermanfaat bagi bangsa dan negara serta diterima didunia internasional.

Pustaka

[1] Munir, Rinaldi. *Diktat Bahan Kuliah IF5054 Kriptografi*, 2004.

[2] Kurniawan, Yusuf. *Kriptografi Keamanan Internet dan Jaringan Komunikasi*, Penerbit Informatika Bandung, 2004.

[3] B. Schneier, *Applied Cryptography - Protocol, Algorithm, and Source Code in C*, second edition, John Willey & Sons, 1996.

[4] William Stallings, *Cryptography and Network Security*, Pearson Education, 2003.

[5] http://www.pgp.org

[6] http://www.pgpi.com