Jurnal Cendikia Vol. 13 No. 2 Cendikia 2017 ISSN: 0216-9436
Bandar Lampung, April 2017

PERBANDINGAN SISTEM PENGAMANAN EMAIL MENGGUNAKAN TEKNIK *PUBLIC KEY ENCRYPTION* DAN *PRETTY GOOD PRIVACY* (PGP) (Studi Kasus: AMIK Dian Cipta Cendikia Bandar Lampung)

Andre Febrianto, Junaida Apriani

Jurusan Manajemen Informatika, AMIK Dian Cipta Cendikia Bandar Lampung
Jl. Cut Nyak Dien No. 65 Palapa Durian Payung- Bandar Lampung
E-mail: andre@dcc.ac.id

ABSTRAK

Pada AMIK Dian Cipta Cendikia dalam pengamanan email masih belum menggunakan manajemen perusahaan, sehingga dikhawatirkan ada seseorang atau sekelompok orang yang dengan sengaja merusak atau mengubah isi data keuangan tersebut. Salah satu metode pengamanan sistem informasi yang umum diketahui oleh banyak orang adalah password. Tanpa disadari password mempunyai peranan penting dalam mengamankan informasi-informasi yang sifatnya pribadi (*confidential*). Dalam penelitian yang dilakukan di AMIK Dian Cipta Cendikia, metode pengamanan email yang digunakan yaitu observasi (penelitian langsung) dan implementasi (penerapan dan pelaksanaan) dengan menggunakan dua software yaitu *Public Key Encryption* dan Teknik *Pretty Good Privacy* (PGP) pada AMIK Dian Cipta Cendikia Bandar Lampung. Dari hasil penelitian yang dilakukan maka dapat disimpulkan bahwa pada AMIK Dian Cipta Cendikia dalam pengamanan email masih belum menggunakan manajemen pengamanan sehingga dibutuhkan pengamanan email dengan menggunakan *Public-Key Encryption* dan Teknik PGP, khususnya bagian keuangan. Karena dikhawatirkan ada seseorang atau sekelompok orang yang dengan sengaja merusak atau mengubah isi data keuangan tersebut. Berdasarkan dari uji coba yang telah dilakukan dapat disimpulkan bahwa *Public-Key Encryption* lebih mudah digunakan untuk mengamankan email dibandingkan teknik PGP. Selain itu, pengguna *Public-Key Encryption* lebih banyak dibandingkan Teknik PGP.

Kata Kunci: Password, Sistem Keamanan, *Hacker*

1. PENDAHULUAN

1.1 Latar Belakang

Doni Ariyus 2006. Halaman 45 ("*computer security*"), informasi sangat penting artinya karena tanpa informasi, hampir semua tidak dapat dilakukan dengan baik. Saat ini komputer sudah memasuki hampir setiap kehidupan manusia. Kemajuan teknologi komputer telah mengubah gaya hidup manusia. Banyak hal yang dahulu dilakukan manusia secara manual sekarang telah digantikan oleh komputer. Akan tetapi, kemajuan teknologi komputer tidak hanya memiliki dampak positif terhadap kehidupan manusia. Kejahatan-kejahatan baru yang menggunakan keahlian dibidang komputer telah mengubah gaya kejahatan konversional menjadi kejahatan modern. Dimedia masa, baik elektronik maupun nonelektronik, banyak terjadi perusakan, pencurian, dan lain sebagainya dengan menggunakan teknologi komputer.

Banyaknya kejahatan komputer memunculkan istilah-istilah bagi mereka yang menggunakan teknologi untuk melakukan kejahatan. Istilah hackers sendiri masih belum baku karena disatu sisi hackers memiliki konotasi positif, sedangkan disisi lain memiliki konotasi negative. Bagi kelompok yang pertama *(old school),* pelaku yang jahat biasanya disebut *crackers.* batas antara hacker dan *cracker* sangat tipis. Batas itu ditentukan oleh etika, moral, dan integritas dari pelaku itu sendiri. perkembangan teknologi informasi tersebut diiringi pula dengan semakin bertambahnya jumlah pengguna jaringan komputer dalam mengirim dan melakukan komunikasi data. Dalam dunia komunikasi dari global dan perkembangan teknologi informasi yang senantiasa berubah serta cepatnya perkembangan *software*, keamanan merupakan suatu isu yang sangat penting, baik itu keamanan fisik, keamanan data maupun keamanan aplikasi. Perlu kita sadari bahwa untuk mencapai suatu keamanan itu adalah suatu hal yang sangat mustahil, seperti yang ada dalam dunia nyata sekarang ini.

Salah satu kode pengamanan sistem informasi yang umum diketahui oleh banyak orang adalah ***password*.** Tanpa disadari *password* mempunyai peranan penting dalam mengamankan informasi-informasi yang sifatnya pribadi *(confidential).* Pada beberapa aplikasi yang berhubungan dengan piranti lunak, seperti Hp, kartu ATM, dll. Ada juga sistem pengamanannya yang fungsinya mirip dengan *password*, biasa dikenal dengan kode PIN. Walaupun hanya terdiri dari angka, namun kegunaannya sama seperti *password,* yaitu untuk mengamankan informasi. Informasi yang disimpan tersebut biasanya sudah berbentuk digital.

Email adalah singkatan dari *electronic mail* merupakan metode untuk mengirim dan menerima pesan melalui system komunikasi elektronik/internet. Sistem enkripsi PGP merupakan sistem *hybrid* Menggabungkan kecepatan enkripsi sistem Untuk Mengenkripsi suatu pesan mula-mula PGP Memampatkan pesan tersebut untuk dengan tujuan Menghemat *bandwidth* dan *disk space* sekaligus Menghilangkan pola pesan yang biasanya dimanfaatkan kriptanalis, kemudian PGP membuat Suatu pesan Yang telah dimampatkan kemudian dienkripsi dengan *Session key* tersebut yang hanya dipergunakan sekali, Terakhir *session key* tersebut dienkripsi dengan kunci Publik penerima pesan dan dimasukkan dalam pesan. Untuk mendekripsi pesan dilakukan kebalikannya Penerima pesan mendekripsi *session key* Menggunakan kunci privatnya, kemudian *session key* Itu digunakan untuk mendekripsi pesan. Tanda tangan digital pada PGP memiliki format yang Sama yaitu merupakan hasil enkripsi *hash* dari pesan Dengan menggunakan kunci privat pengirim.

Tetapi banyak dari para pengguna *password* yang membuat *password* secara sembarangan tanpa mengetahui kebijakan pengamanan *(password policy)* dan bagaimana membuat *password* yang kuat *(strong password).* Mereka tidak sadar dengan bahayanya para 'penyerang' (*attacker*) yang dapat mencuri atau mengacak-acak informasi tersebut.

Dilihat dari bentuknya sistem pengamankan email memerlukan manajemen perusahaan dalam pengamankan email dengan menggunakan *public key encryption* email dan teknik PGP. Karena khawatirkan ada seseorang atau sekelompok orang yang dengan sengaja merusak atau mengubah password email tersebut selain itu, bagian terpenting dari public key encryption harus bisa memilih dan membandingkan *software* untuk *encryption email* yang dapat mengamankan email dengan mempassword secara kuat.

Tujuan adanya teknik sistem pengamanan email ini bukan untuk menutup semuanya melainkan memperlambat seseorang untuk bisa masuk ke email dan mengambil data penting serta memperlambat untuk mengubah-ubah *password* tersebut.

1.2 Referensi

a. Menurut Mico Pardosi (2006:13). Email adalah singkatan dari electronic mail merupakan metode untuk mengirim dan menerima pesan melalui system komunikasi elektronik/internet. Dengan adanya email, maka kita bisa mengirim surat ke orang lain dengan mudah, mengirim file, mengirim gambar dan lain-lain. Sebab saat ini, sudah banyak perusahaan Indonesia (temasuk bank) yang mencari tenaga kerja via internet, termasuk perusahaan-perusahaan luar negeri. Dengan adanya Email, kita juga bisa 'surat-suratan' dengan teman, keluarga, kenalan lain-lain. Itulah Email mengirim surat tanpa amplopdan tanpa perangko.
b. Dony Ariyus (2006:34-36). Keamanan komputer adalah berhubungan dengan pencegahan diri dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam system komputer. Empat langkah keamanan komputer:
    1. Aset: perlindungan Aset merupakan hal yang paling penting sekali dan merupakan langkah awal dari berbagai implementasi keamanan komputer. Contohnya, ketika mendesain sebuah website e-commerce, yang perlu dipikirkan adalah keamanan konsumen.
    2. Analisis resiko: adalah tentang identifikasi akan resiko yang mungkin terjadi, sebuah even yang potensial yang bisa mengakibatkan suatu sistem yang dirugikan.
    3. Alat atau tool: yang digunakan pada suatu komputer merupakan peran penting dalam hal keamanan karena tool yang digunakan harus benar-benar aman. Banyak software bajakan yang tersedia dipasaran dan software atau tool gratisan yang tersedia di internet tidak terjamin keamanannya.
    4. Prioritas: perlindungan komputer secara menyeluruh. Jika keamanan jaringan merupakan suatu prioritas. Suatu jaringan komputer pada tahap

awal harus diamankan dengan firewall atau lainnya yang mendukung suatu sistem keamanan

c. Dony Ariyus (2006:159). Salah satu kesulitan utama dari enkripsi konversional adalah perlunya mendistribusikan kunci yang digunakan dalam keadaan aman. Sebuah cara yang tepat telah ditemukan untuk mengatasi kelemahan tersebut dengan suatu model enkripsi yang secara mengejutkan tidak memerlukan sebuh kunci untuk mendistribusikan. Metode itu dikenal dengan nama enkripsi public key dan pertama kali di perkenalkan pada tahun 1976.
d. Dony Ariyus (2006:187). PGP adalah sistem enkripsi hybrid yang memanfaatkan, baik public key maupun algoritma enkripsi konversional. Untuk mengenkripsikan suatu pesan, suatu kunci rahasia diciptakan dan digunakan untuk mengenkripsikan pesan itu. Kunci tersebut kemudian dienkripsi dengan public key dari penerima pesan. PGP juga digunakan sebagai digital signature yang memastiakn bahwa suatu pesan memang pesan asli dari pengirimnya. Sejak diluncurkan, PGP berkembang dengan pesat dan banyak digunakan oleh masyarakat di Amerika.
e. Rudy Siahaan (2002:35). Email berbeda dengan pembicaraan tatap muka. Pada pembicaraan tatap muka, anda dapat menggunakan intonasi nada suara (nada tinggi dan rendah) dan bahasa tubuh (body language). Sedangkan pada email, yang ada hanya teks. Teks ini digunakan untuk menyatakan intonasi dan tubuh. Pembicaraan tatap muka bersifat interaksi, sedangkan email harus bergantian. Inilah perbedaan utama antara email dengan pembicaraan tatap muka. Oleh karena itu, untuk menyampaikan pesan dengan email memerlukan pengetahuan khusus. Kesimpulan email adalah email menghubungkan kita dengan siapa saja yang terhubung diinternet diseluruh dunia, Dapat mengirim kepada lebih dari satu orang dengan saat bersamaan, digunakan untuk berlangganan informasi tertentu secara periodik.

2. METODE PENELITIAN

2.1 Analisis Kebutuhan Sistem

Analisis sistem merupakan tahap yang bertujuan untuk memahami sistem, mengetahui keunggulan dan kelemahan dari sistem ditinjau dari sisi pengguna. Dengan menganalisis prosedur sistem yang sering digunakan, maka sistem yang sering dipakai dapat dievaluasi sehingga dapat dijadikan sebagai acuan untuk membangun suatu sistem yang baru dari hasil evaluasi tersebut.

PGP bekerja dengan menggabungkan beberapa bagian yang terbaik dari *key* konvensional dan *public key cryptography*, jadi PGP ini adalah sebuah *a hybrid cryptosystem*. Ketika seorang pengguna mengenkrip sebuah plaintext dengan menggunakan PGP, maka awal PGP akan mengkompress plaintet ini. Data yang dikompress menghebat waktu dan media transmisi dan lebih penting adalah keamanan kriptograpik yang kuat. Kebanyakan teknik analisis sandi mengeksplotasi pola yang ditemukab dalam plaintext untuk men-crack chipernya. Kompressi mengurangi pola-pola ini dalam plaintext, dengan cara demikian perbaikan yang lebih baik untuk menghambat analisa kode-kode.

PGP membuat sebuah *session key*, dimana sebuah kunci rahasia pada saat itu. Kunci adalah sebuah bilangan acak yang dihasilkan dari gerakan acak dari mouse dan tombol yang anda tekan. Session Key ini berkerja dengan sangat aman, algoritma enkripsi konvesional yang cepat untuk meng-enkrip *plaintext*. Hasilnya adalah berupah chiper text. Sekali data dienkripsi, lalu *session key* ini dienkripsi lagi menggunakan kunci publik penerima. *session key* yang terenkripsi kunci publik key penerima dikirim dengn *chipertext* ke penerima. Cara kerja enkripsi PGP:

Gambar 1. Cara Kerja Enkripsi PGP

Proses deskripsi bekerja sebaliknya, Penerima menerima pesan lalu membuka pesan tersebut dengan kunci privatnya, namun pesan tersebut masih terenkripsi dengan session key. Dengan Menggunakan PGP, penerima mendekrip chipertext yang terenkripsi secara konvensional.

2.2 Ilustrasi Pemakaian PGP

Public-key sangat lambat bila dibandingkan dengan konvensional, jadi PGP akan mengkombinasikan dua algoritma, yaitu *RSA and IDEA*, untuk melakukan enkripsi *plaintext*a. Sebagai contoh, Badrun (pemilik

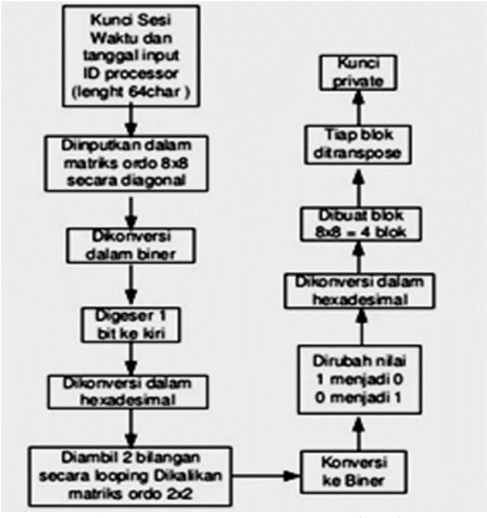
PGP) ingin mengenkripsi suatu file yang diberi nama plain.txt sedemikian sehingga hanya si Matangin yang dapat mendekripsi-nya. Maka Badrun mengirimkan PGP perintah (*command line*) untuk melakukan enkripsi: pgp -e plain.txt Matangin pada *command line* ini, pgp adalah *file executable*, -e berarti memberitahukan PGP untuk meng-encrypt file, plain.txt adalah nama *plaintext*, dan dul merepresentasikan public key suatu tujuan (Matangin) yang diinginkan Badrun untuk mengenkripsi message-nya. PGP menggunakan suatu *random number generator*, dalam file randseed.bin untuk menghasilkan suatu kunci (*session key*) temporary IDEA. *Session key* itu sendiri dienkripsi dengan kunci RSA *public* yang direpresentasikan oleh Matangin yang disematkan pada plaintext.

Kemudian, PGP menggunakan *session key* untuk mengenkripsi *message*, *ASCII-armors* dan menyimpan seluruhnya sebagai cipher.asc. Bila Matangin ingin membaca pesannya, ia mengetikkan command.

2.3 Perancangan Sistem Teknik PGP

a. Pemrosesan Kunci Private

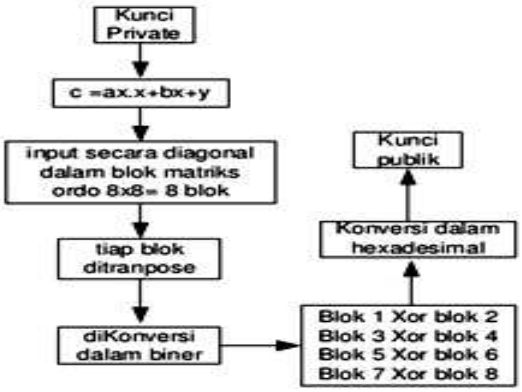
Untuk dapat memproleh kunci private maka dilakukan proses algoritma enkripsi kunci sesi yang diinputkan oleh user. Kunci sesi tersebut secara otomatis digabungkan dengan waktu input. Tanggal input, dan ID processor. Algoritma pembangkitan kunci private dapat dilihat pada gambar.



Gambar 2. Pemrosesan Kunci Private

b. Pemrosesan Kunci Publik

Untuk dapat memproleh kunci publik maka akan dilakukan enkripsi kunci private, untuk algoritma enkripsi kunci private dapat diketahui dalam proses dibawah ini urutan pemrosesan kunci public dapat dilihat pada gambar dibawah ini.



Gambar 3. Pemrosesan Kunci Publik

3. PEMBAHASAN

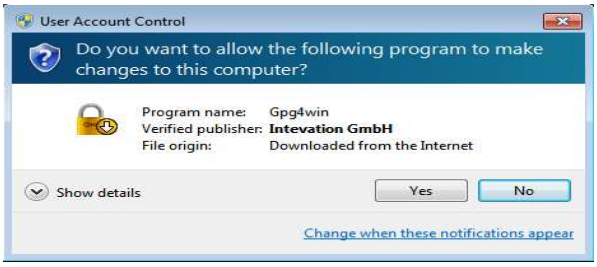
3.1 Hasil

Hasil dari konfigurasi teknik PGP yang dilakukan oleh penulis adalah seperti gambar dibawah ini.

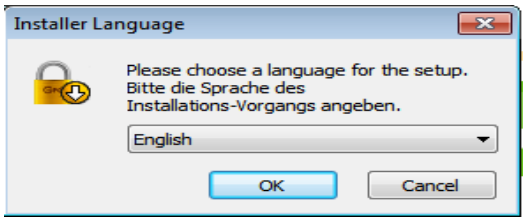
1. Alamat https://gpg4win.org/download.html.

Gambar 4. Langkah ke-1

2. Lalu akan menyimpannya, dan membukanya bila dilakukan mendowload. Jika anda memiliki UAC diaktifkan, klik "yes" pada jendela yang muncul, setelah itu pilih bahasa klik OK.



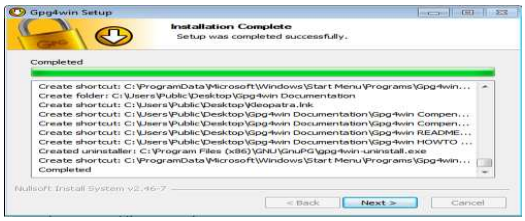
Gambar 5. Langkah ke-2



Gambar 6. Langkah ke-3

3. Kemudian 'Next' terus pilih 'kleopatra', 'GpgEX', 'Gpg4win compendiun', kemudian klik 'Next' dan akan mengintal.

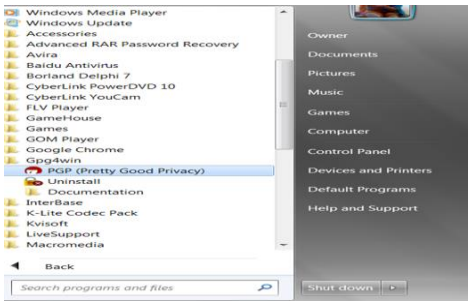
Gambar 7. Langkah ke-4



Gambar 8. Langkah ke-5

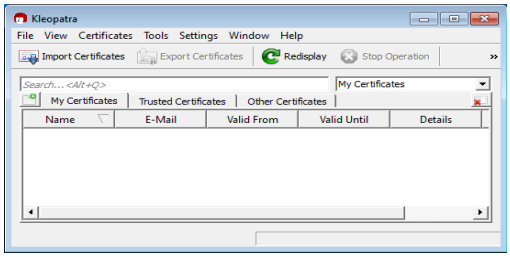
3.2 Pembahasan

1. Buka Aplikasi PGP (Pretty Good Privacy)



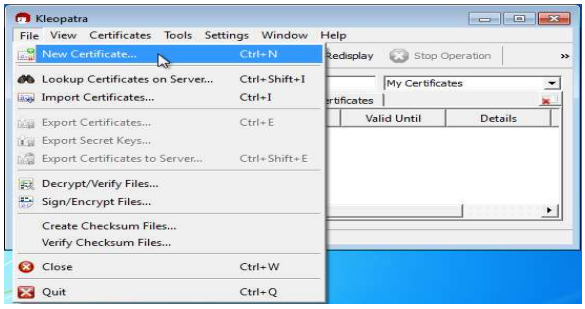
Gambar 9. Tampilan Start Menu

2. Kemudian akan tampil seperti gambar berikut tekan CTRL+N



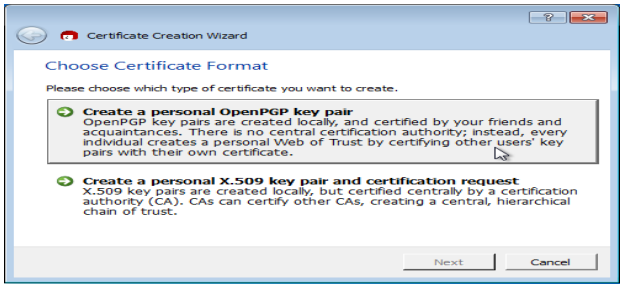
Gambar 10. Tampilan PGP (*Pretty Good Privacy*)

3. Kemudian akan tampil seperti gambar berikut.



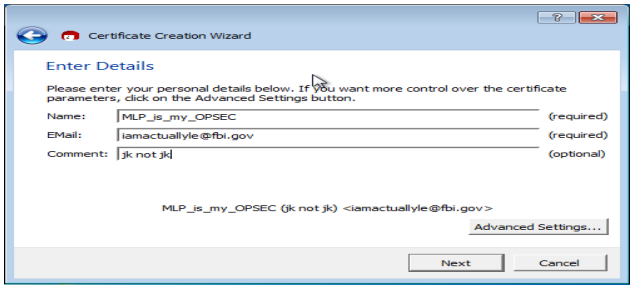
Gambar 11. Tampilan PGP Membuat Email

4. Lalu klik *create a personal* OpenPGP key pair



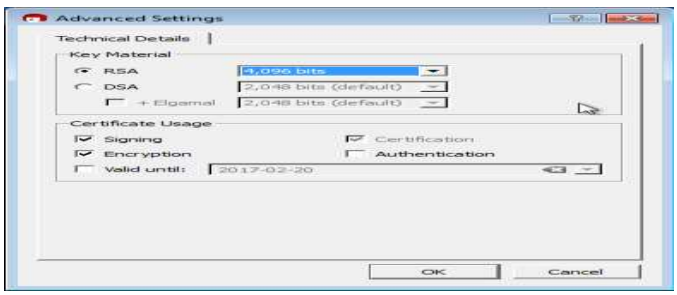
Gambar 12 Tampilan Membuat Email

5. Kemudian buat nama lengkap, Email, dan komentar. Kemudian *klik advanced setting*.



Gambar 13. Tampilan Mengisi Nama Lengkap

6. Kemudian tampil ukuran material dan ceklis pada RSA.

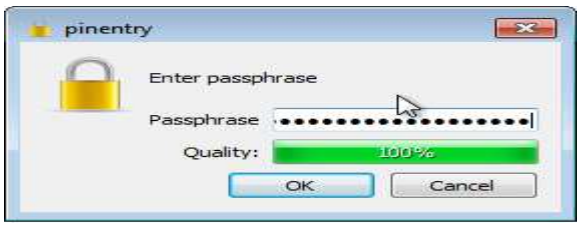


Gambar 14 Tampilan Mengubah Material bit

7. Maka akan tampil Email yang telah dibuat, lalu klik *create key*.

Gambar 15. Tampilan Nama & Email

8. Set Master password lalu OK



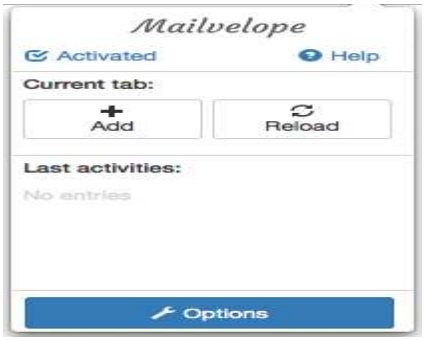
Gambar 16. Tampilan Membuat password

9. Finish

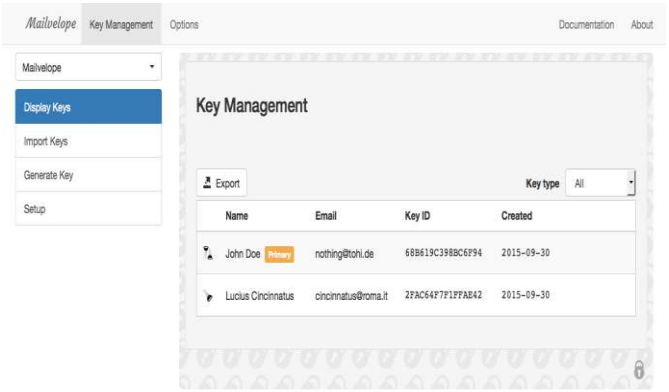
Gambar 17. Tampilan Email yang telah selesai

Langkah selanjutnya adalah;

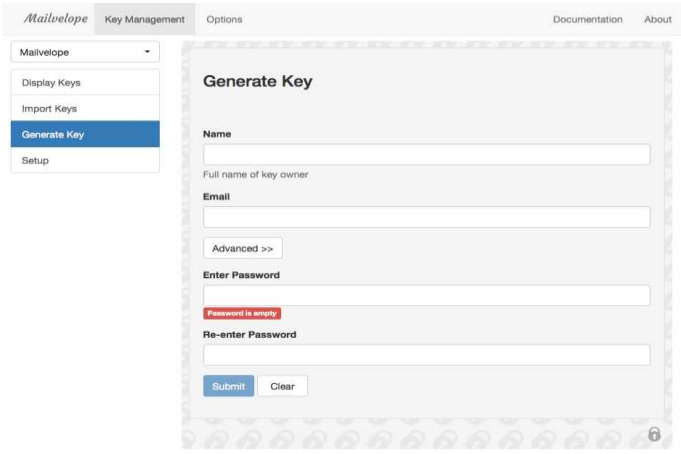
1. Klik di sini untuk membuka open Mailvelope in the Chrome app store. Kemudian klik Install. Ketika konfirmasi muncul, klik Install. Setelah instalasi, ikon kunci ditampilkan di utama toolbar Google Chrome (di sebelah kanan address bar). Klik untuk membuka menu utama Mailvelope.



2. Penanganan Kunci (Key Handling)
   Klik pada ikon kunci Mailvelope di toolbar untuk membuka menu utama. Klik Opsi untuk menavigasi ke Key Ring, di mana semua tombol disimpan:

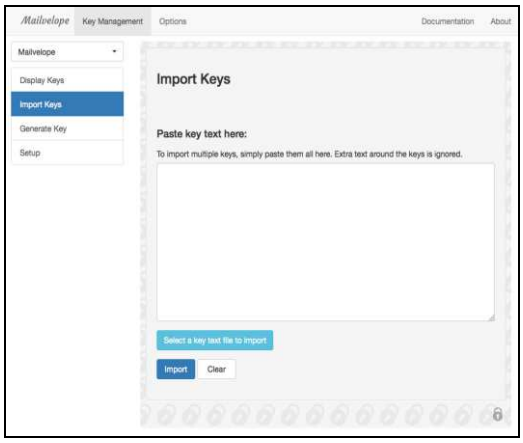


3. Membangkitkan Keys (generating keys)
   Untuk menggunakan Mailvelope, setidaknya satu pasangan kunci (yang terdiri dari kunci publik dan swasta) harus tersedia. Anda dapat menghasilkan pasangan kunci baru seperti yang dijelaskan dalam bagian ini, atau mengimpor pasangan kunci yang ada seperti yang dijelaskan di bawah ini. Klik Generate Key untuk membuka dialog pembangkitan kunci. Isilah kotak dan menetapkan sandi kunci. Pastikan Anda tidak pernah kehilangan password ini. Jika hilang, password tidak dapat dipulihkan dan kunci tidak bisa lagi digunakan.

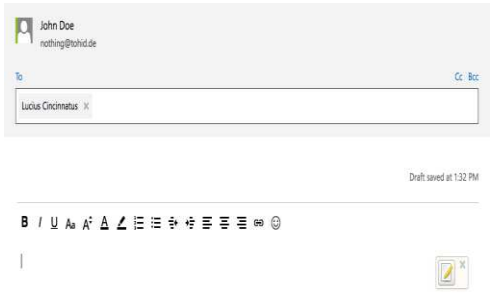


Masukkan semua informasi yang diperlukan. Klik Kirim untuk mulai menghasilkan kunci. Setelah itu, Anda dapat melihat hasilnya dalam daftar kunci dengan memilih Tampilan Keys.

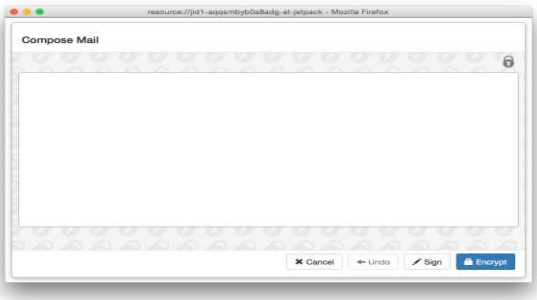
4. Mengimpor Keys
   Kunci yang ada dapat diimpor dari aplikasi lain. alam menu pilihan, klik Gantungan Kunci dan kemudian Impor kunci.



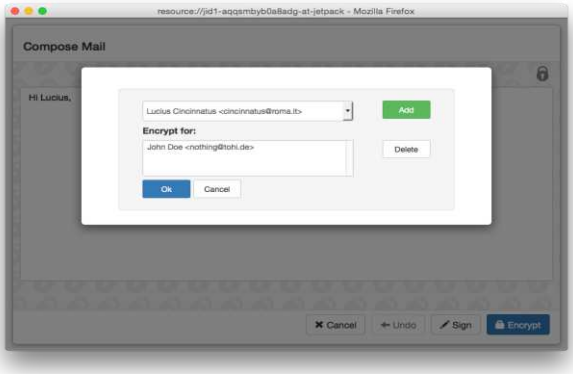
5. The Compose (ikon) tombol ditampilkan di semua bidang e-mail menyusun penyedia webmail dan akan meluncurkan editor eksternal Mailvelope ini.



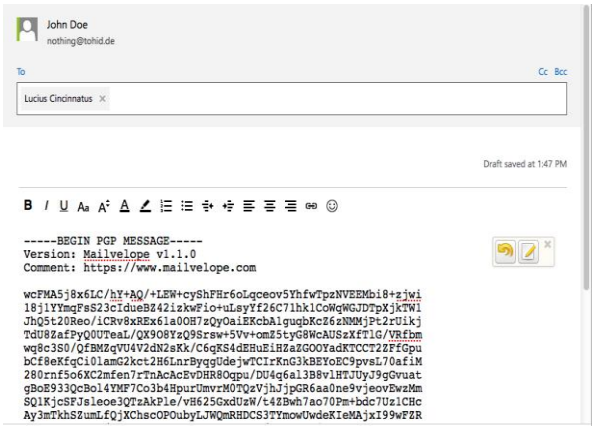
6. Mengklik tombol Compose akan membuka popup baru dengan editor terpisah. Hal ini memastikan bahwa penciptaan e-mail dan proses enkripsi benar-benar terisolasi dari penyedia webmail.



7. E-mail sekarang dapat terdiri. Selanjutnya, klik tombol Encrypt untuk menampilkan dialog enkripsi. Di sini, Anda dapat memilih penerima, atau lebih khusus orang-orang yang harus diizinkan untuk mendekripsi pesan. Anda dapat menambahkan orang-orang ini ke dalam daftar. kunci publik mereka harus sudah diimpor seperti yang dijelaskan dalam Mengimpor kunci.

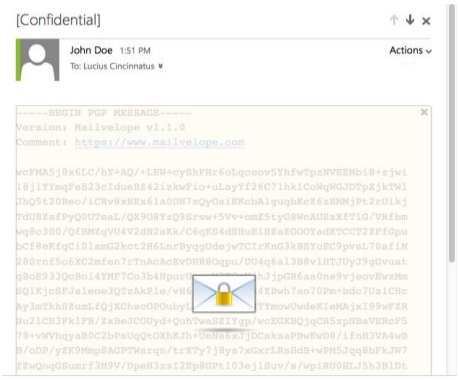


8. Klik OK untuk mendekripsi e-mail. Teks e-mail akan diganti dengan pesan terenkripsi Tombol Undo akan mengkonversi konten kembali ke teks terenkripsi dan Anda dapat memulai kembali proses tersebut. Langkah terakhir adalah untuk menyalin pesan terenkripsi kembali ke penyedia e-mail. Mengklik transfer akan melakukan ini dan tutup editor eksternal.

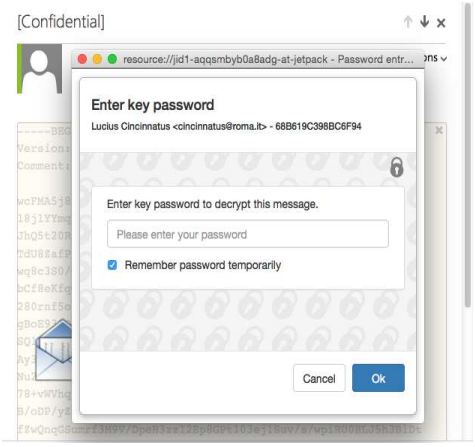


9. Enkripsi dalam editor webmail
   Mailvelope juga menawarkan modus kedua dimana pesan dienkripsi langsung pada halaman penyedia webmail ini. Lihat bagian Security untuk petunjuk tentang mengaktifkan mode ini dan rincian tentang apa implikasi keamanan modus ini.

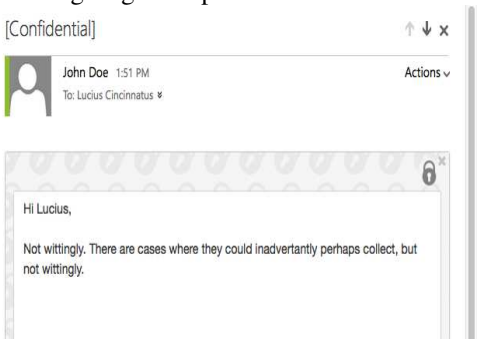
10. Pesan Dekripsi
    Setiap kali Mailvelope mendeteksi pesan terenkripsi dalam sebuah e-mail, menandai dengan ikon (amplop tertutup). Klik ikon ini untuk memulai dekripsi.



11. Masukkan password kunci Anda dan konfirmasikan dengan mengklik OK. Pesan ini kemudian didekripsi dan ditampilkan secara langsung.



12. Mailvelope mencoba untuk menemukan kunci pribadi yang diperlukan untuk mendekripsi pesan. Jika tombol yang benar ditemukan di gantungan kunci, yang sesuai Pengguna dan Key ID akan ditampilkan. Setelah kunci dibuka dengan password, pesan dienkripsi dan langsung ditampilkan di daerah ditandai.



Perbandingan dari software public key encryption dan teknik PGP dapat dilihat dari tabel berikut :

Tabel 1. Perbandingan public key encryption dan teknik PGP

No.	Fitur	Public Key Encryption	PGP
1.	Mengunci dan meproteksi data.	✓	✓
2.	Password yang diperkuat teknologi enkripsi.	✓	✓
3.	Ringan dan tidak aman untuk mengamankan email dan password.	✓	✓
4.	Pengoperasian yang mudah dan menarik untuk mengamankan email dan password.	✓	✓
5.	Menggunakan sandi meteran (contoh dccokebgt1)	x	✓
6.	Menggunakan dua kunci private key dan public key.	✓	x

Gambar 18. Tampilan perbandingan software

4. KESIMPULAN

Kesimpulan dalam penelitian ini adalah sebagai berikut:

1. Dalam sistem pertukaran informasi, antara pengirim dan penerima masing – masing memiliki 2 kunci yaitu kunci publik (public) dan kunci pribadi (private). Kedua kunci tersebut digunakan untuk membuat sistem keamanan data. Data yang dikirimkan terlebih dahulu akan dienkrip dengan menggunakan kunci publik si penerima dan akan dibuka atau didekrip oleh kunci pribadi si penerima itu sendiri.
2. PGP merupakan aplikasi pengamanan komunikasi data yang dapat mengizinkan pengirim utnuk menandai pesan – pesan mereka dengan di buktikan pada pesan yang belum ada perubahan selama perjalanan. PGP memberikan pengamanan yang berlapis dalam beberapa tingkat. Saat ini PGP merupakan suatu aplikasi yang baik untuk keamanan e-mail juga file – file. Orang – orang banyak menggunakan aplikasi ini selain keamanan yang baik juga fleksibel yang dapat berjalan pada semua sistem operasi dan mudah didapatkan dengan gratis di internet.

PUSTAKA

Ariyus, dony, kriptografi, keamanan data, dan komunikasi, Public Key Encryption Dan Pretty Goog PrivacyGraham ilmu, Yogyakarta, 2006.

Doni ariyus.. Computer Security. Andi Yogyakarta. 2006

Mico pardosi. Membuat Dan Mengirim Email. 2006

Rudi siahaan. Membuat email yang efektif. 2005