Jurnal Elektro Luceat [November] [2021]

KOMBINASI GNU *PRIVACY GUARD* DAN *HAMMING DISTANCE* UNTUK KEAMANAN *EMAIL* SERTA JALUR SERTIFIKASI

COMBINATION OF GNU PRIVACY GUARD AND HAMMING DISTANCE FOR EMAIL SECURITY AND CERTIFICATION PATHS

Matheus Supriyanto Rumetna[1]

[1]Universitas Victory Sorong

[1]matheus.rumetna@gmail.com

Abstrak

Email merupakan salah satu fitur canggih terkait surat menyurat secara elektronik dengan memanfaatkan teknologi internet. Salah satu alasan kenapa *email* dipakai banyak orang, karena memberikan cara yang mudah dan cepat dalam mengirimkan sebuah informasi. Tetapi *email* juga tidak terlepas dari masalah keamanan seperti disadap, dipalsukan, disusupi virus, *spamming*, *mailbomb*, *mail relay*. Tetapi kerahasiaan *email* terancam bukan oleh para peretas saja, melainkan para sistem administrator sendiri. Salah satu cara untuk mengatasi hal ini adalah dengan mengenkripsi *email* dengan memanfaatkan Gnu PG. Jadi, fokus penelitian ini adalah masalah keamanan *email* serta untuk membuat jalur sertifikasi yang terpercaya. Dalam penelitian ini, diusulkan sebuah protokol otentikasi yang membuat ukuran repositori sertifikat sebagai log2 N menggunakan konsep *Hamming Distance*, dengan meyakinkan untuk membuat jalur sertifikasi yang aman dari satu node ke yang lain. Disajikan pula mekanisme manajemen kunci publik untuk mengeluarkan, *update* dan mencabut sertifikat antara node berdasarkan *Hamming Distance*.

Kata kunci: *email,* Gnu PG, keamanan, kriptografi, *Hamming Distance*

Abstract

Email is one of the advanced features related to electronic correspondence by utilizing internet technology. One of the reasons why many people use email, because it provides an easy and fast way to send information. But email is also inseparable from security problems such as being intercepted, forged, infiltrated by viruses, spamming, mailbombing, mail relay. But email confidentiality is threatened not only by hackers, but by system administrators themselves. One way to overcome this is to encrypt the email using Gnu PG. So, the focus of this research is on email security issues as well as to create a trusted certification path. In this study, an authentication protocol is proposed that makes the certificate repository size as log2 N using the concept of Hamming Distance, convincingly to create a secure certification path from one node to another. It also provides a public key management mechanism for issuing, updating and revoking certificates between nodes based on Hamming Distance.

Keywords: email, Gnu PG, security, cryptography, Hamming Distance

1. PENDAHULUAN

Email sudah digunakan orang sejak awal terbentuknya internet pada sekitar tahun 1969 dan merupakan salah satu fasilitas yang ada pada saat itu. Sesuai dengan perkembangan internet, penggunaan *email* ini juga semakin membesar walaupun pada saat ini persentasinya sudah turun karena adanya sebuah fasilitas baru di internet yang dikenal sebagai *Web*. Salah satu alasan kenapa

email dipakai banyak orang, karena memberikan cara yang mudah dan cepat dalam mengirimkan sebuah informasi [1], [2]. Selain itu, *email* juga dapat mengirimkan informasi dalam bentuk *file* mulai dari ukuran kecil hingga *file* yang ukurannya besar. Namun sifat *email* yang memanfaatkan penghantar elektronik tak sepenuhnya dimaksudkan sebagai medium pribadi, karena menyimpan potensi bahaya penyalahgunaan yang bukan saja menjengkelkan tetapi juga dapat bersifat fatal [3].

Ketika mengirimkan suatu *email*, maka *email* tersebut disampaikan ke suatu sistem komputer yang administratornya tidak diketahui. Dari komputer tersebut disampaikan ke sistem komputer lain sampai kepada penerima yang dituju [4], [5], [6], [7], [8]. Pada beberapa *link* di rantai ini, *email* yang dikirimkan dapat dibaca oleh siapa saja yang diinginkan oleh sistem administrator, atau oleh suatu biro penyelidikan yang sedang mencurigai suatu aktivitas kejahatan, dan berbagai kemungkinan lainnya [9]. Tetapi secara ringkasnya adalah ketika mengirimkan suatu *email*, kita tidak mengetahui siapa yang membaca pesan itu, penerima yang diharapkan ataupun orang lain.

Beberapa masalah keamanan yang terkait dengan sistem *email* adalah disadap, dipalsukan, disusupi virus, *spamming*, *mailbomb*, *mail relay*. Tetapi kerahasiaan *email* terancam bukan oleh para peretas saja, melainkan para sistem administrator sendiri [1], [2], [10]. Para sistem administrator terkadang bosan tidak tahu apa yang harus dikerjakan selain membaca-baca *email* orang lain. Mereka dapat melakukannya tanpa sedikit pun meninggalkan jejak. Salah satu cara untuk mengatasi hal ini adalah dengan mengenkripsi *email* [11]. GNU *Privacy Guard* (Gnu PG, atau GPG) adalah sistem enkripsi *key public*, program ini di *install* pada semua mesin DICE Linux. Gnu PG adalah suatu re-implementasi GNU dari program PGP (*Pretty Good Privacy*), memenuhi spesifikasi *OpenPGP*, yang pertama kali ditulis dan didistribusikan oleh Zimmerman [1], [11], [12].

Jadi fokus penelitian ini adalah masalah keamanan *email* serta untuk membuat jalur sertifikasi yang terpercaya. Dalam penelitian ini, diusulkan sebuah protokol otentikasi yang membuat ukuran repositori sertifikat sebagai *log2* N menggunakan konsep *Hamming Distance*, dengan meyakinkan untuk membuat jalur sertifikasi yang aman dari satu node ke yang lain. Disajikan pula mekanisme manajemen kunci publik untuk mengeluarkan, *update* dan mencabut sertifikat antara node berdasarkan *Hamming Distance* [12], [5].

2. DASAR TEORI /MATERIAL DAN METODOLOGI/PERANCANGAN

2.1 *Email (Electronic Mail)*

Email adalah layanan yang dapat digunakan saat terhubung dengan internet. Apabila kita mempunyai program *client email* seperti Eudora dan memiliki akses ke layanan *email*, maka dapat mengirim *email* ke setiap orang yang alamat emailnya kita ketahui [2], [11].

Alamat *email* merupakan gabungan dari nama *user* dan *domain name: user@domainname*. Misalnya matheus@rumetna.com. Untuk mengirim *email* kepada seseorang, maka harus membuat pesan terlebih dahulu. Pesan *email* biasanya terdiri atas teks, namun dapat juga berisi *file* biner seperti gambar grafis dan program. Pesan tersebut meliputi: nama dan alamat yang dituju, teks berisi pesan. Pesan tersebut akan disampaikan melalui satu *host* ke *host* yang lain hingga mencapai tujuan.

Tidak mudah untuk menyadap sebuah pesan *email*, tetapi itu hal yang mungkin, untuk alasan inilah beberapa orang mengenkripsi pesan mereka agar tidak seorangpun kecuali penerima yang dapat membacanya.

2.2 Kriptografi (*Cryptographygraphy*)

Kriptografi merupakan ilmu dan seni untuk menjaga pesan agar aman. Para pelaku atau praktisi kriptografi disebut *cryptographygraphers*. Sebuah algoritma kriptografi (*cryptographygraphic algorithm*), disebut *cipher*. *Cipher* merupakan persamaan matematik yang digunakan untuk proses

enkripsi dan dekripsi. Biasanya kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat [1], [3], [13].

Proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah enkripsi (*encryption*) [14]. Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi data akan disandikan (*encrypted*) dengan menggunakan sebuah kunci (*key*). Untuk membuka (*decrypt*) data tersebut digunakan juga sebuah kunci yang sama dengan kunci untuk mengenkripsi (untuk kasus *private key cryptographygraphy*) atau dengan kunci yang berbeda (untuk kasus *public key cryptographygraphy*).

Ciphertext adalah pesan yang sudah tidak dapat dibaca dengan mudah. Menurut ISO 7498-2, terminologi yang lebih tepat digunakan adalah "*encipher*". Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*, disebut Dekripsi (*decryption*). Menurut ISO 7498-2, terminologi yang lebih tepat untuk proses ini adalah "*decipher*". *Cryptanalysis* adalah seni dan ilmu untuk memecahkan *ciphertext* tanpa bantuan kunci. *Cryptanalyst* adalah pelaku atau praktisi yang menjalankan *cryptanalysis*. *Cryptographylogy* merupakan gabungan dari *cryptographygraphy* dan *cryptanalysis*.

Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data yang dikirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Banyak layanan di internet yang masih menggunakan "*plaintext*" untuk *authentication*, seperti penggunaan pasangan *userID* dan *password*. Informasi ini dapat dilihat dengan mudah oleh program penyadap atau pengendus (*sniffer*) [2], [3], [11]. Contoh layanan yang menggunakan *plaintext* antara lain:

1) Akses jarak jauh dengan menggunakan telnet dan rlogin.
2) Transfer *file* dengan menggunakan FTP.
3) Akses *email* melalui POP3 dan IMAP4.
4) Pengiriman *email* melalui SMTP.
5) Akses *web* melalui HTTP.

2.3 *Hamming Distance*

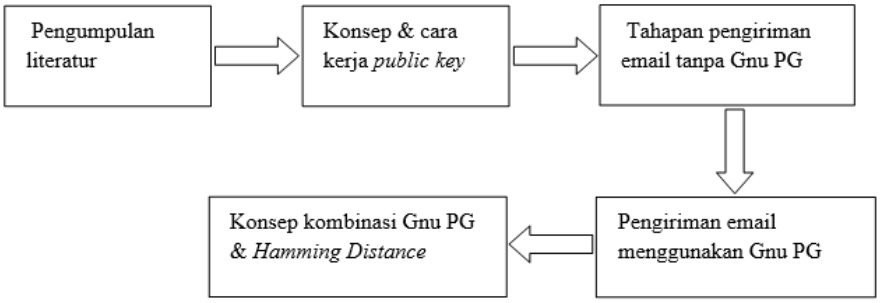
Hamming Distance dinamai oleh Richard Hamming, yang memperkenalkan konsep dalam makalah mendasar pada *Hamming* kode kesalahan mendeteksi dan mengoreksi kesalahan kode pada tahun 1950. Analisis berat *Hamming* bit digunakan dalam beberapa disiplin ilmu termasuk teori informasi, teori *coding*, dan kriptografi [12], [5].

Hal ini digunakan dalam telekomunikasi untuk menghitung jumlah bit membalik dalam kata biner panjang tetap sebagai perkiraan kesalahan, dan karena itu kadang-kadang disebut jarak sinyal. Untuk *string q-ary* lebih dari satu alfabet ukuran $q \geq 2$ *Hamming Distance* diterapkan dalam kasus saluran simetris *q-ary*. Jarak *Hamming* juga digunakan dalam sistematika sebagai ukuran jarak genetik.

2.4 Metode Penelitian

Metode yang digunakan adalah studi literatur [15], [16], [17], [18], [19], [20], dimana pengumpulan data dilakukan dengan cara mencari dan mempelajari data-data dari buku, jurnal ataupun referensi lain yang berhubungan dengan penelitian ini, serta menciptakan suatu konsep keamanan *email* dengan melakukan kombinasi antara Gnu PG dan algoritma *Hamming Distance* untuk membuat jalur sertifikasi yang terpercaya.

Pendekatan metode ini diharapkan dapat memberikan wawasan kepada para pembaca agar dapat mengetahui tentang masalah keamanan yang terjadi pada *email* serta meningkatkan keamanan *email*. Kerangka penelitian dapat dilihat pada Gambar 1.



Gambar 1. Kerangka Penelitian

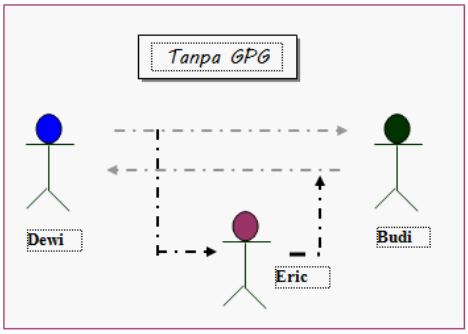
Keterangan:

1) Pengumpulan literatur, dilakukan untuk mendapatkan informasi terkait dengan penelitian yang akan dilakukan.
2) Konsep & cara kerja *public key*, dipaparkan secara sederhana agar dapat mengetahui konsep serta cara kerja *public key*.
3) Tahapan pengiriman *email* tanpa Gnu PG, diberikan suatu contoh untuk mengetahui tahapan pengiriman *email* yang sering dilakukan dan juga untuk menunjukkan celah keamanan dari tahapan ini.
4) Pengiriman *email* menggunakan Gnu PG, diberikan suatu contoh sebagai pembanding antara pengiriman *email* biasa dan pengiriman *email* yang menggunakan Gnu PG, untuk mengetahui proses keamanan yang dilakukan Gnu PG.
5) Konsep kombinasi Gnu PG & *Hamming Distance*, dipaparkan suatu konsep keamanan email yang akan bekerja untuk membuat jalur sertifikasi terpercaya dengan menggunakan *Hamming Distance*.

3. PEMBAHASAN

Kriptografi *Public Key* cara kerjanya berkenan dengan penerjemahan. Pada tahun 1976 Whitfield Diffie Dan Martin Hellman mengumumkan pada dunia cara baru melakukan enkripsi data yang dilakukan dengan sistem kunci publik. Untuk lebih mudah memahami cata kerja sistem kunci public berikut ini adalah contohnya:

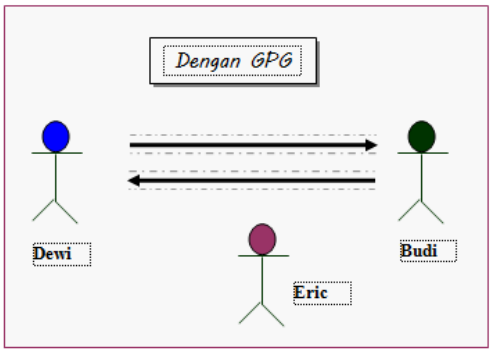
Dewi dan Budi melakukan suatu percakapan, Dewi mengirimkan Budi suatu pesan sederhana, dan Budi menjawabnya dengan pesan sederhana pula. Tetapi Dewi dan Budi tidak mengetahui bahwa Eric tengah menginterupsi pesan ini, membaca, dan menyampaikannya kembali. Ia mengubah sebagian dari pesan balasan yang dikirim ke Dewi dari Budi (lihat Gambar 2).



Gambar 2. Ilustrasi Tanpa GPG

Gambar 3 memperlihatkan Dewi dan Budi yang memanfaatkan kriptografi *Public Key* (GPG), sehingga semua mis-komunikasi dapat diketahui. Dewi dan Budi dapat melakukan enkripsi pesan sebelum dikirimkan, bahkan pesan itu tidak dapat dibaca oleh Eric. Juga tidak perlu

menyembunyikan pesan mereka, tetapi harus memperhatikan dengan menguji identitas penulis pesan tersebut bahwa mereka dapat menandatangani pesan sebelum dikirim.



Gambar 3. Ilustrasi Menggunakan GPG

Secara keseluruhan proses kriptografi *Public Key* adalah Dewi mempuyai dua kunci yaitu *Public Key* dan *Private Key*, begitu juga Budi. Dewi dan Budi kemudian saling bertukar *Public Key*. Budi menulis suatu pesan ke Dewi, dan menggunakan *Publik Key* Dewi untuk mengenkrip pesan tersebut, setelah menerima pesan itu, Dewi kemudian dapat mendekripsikan pesan menggunakan *Private Key* miliknya.

Dewi kemudian membalas pesan Budi agar dia tahu pesannya telah diterima. Setelah menulis balasannya Dewi kemudian menanandatangani pesan tersebut dengan *Private Key* Budi, kemudian Budi dapat memeriksa tanda tangan Dewi dengan menggunakan *Public Key* Dewi. Jika semua sesuai Budi yakin bahwa pesan ini memang dari Dewi.

Private Key merupakan sesuatu yang harus dirahasiakan, karena *Private Key* adalah satu-satunya kunci yang dapat mendekripsikan pesan yang telah dienkripsi dengan *Public Key*. Juga karena kita merupakan satu-satunya yang mempunyai akses ke *Private Key*, kemudian digunakan untuk memverifikasi pesan yang kita kirim.

Public Key Cryptography berbeda dari *Private Key* atau *Symmetric Key*. Sebelum adanya *Public Key Cryptography* orang-orang yang ingin melakukan percakapan yang aman harus bertemu terlebih dahulu, dan saling bertukar *key*. Tetapi sekarang dengan *Public Key Cryptography*, dapat terjamin keamanan percakapan, tetapi tidak berjumpa sebelumnya. Sistem ini mempunyai implikasi mengagumkan untuk suatu jaringan walaupun penggunanya berjauhan secara geografis.

3.1 Pengiriman *Email* Menggunakan Gnu PG

Pengamanan *email* dapat menggunakan Gnu PG, agar *email* terenkripsi sebelum melakukan pengiriman. Terbukti dengan menggunakan Gnu PG masalah keamanan pada *email* dapat ditekan [5], [2], [3], [11], [13]. Berikut langkah-langkah untuk mengamankan *email* menggunakan Gnu PG:

3.1.1 Membuat Sepasangan Kunci (*Public & Private*)

Langkah awal adalah membuat *public key* dan *private key* agar dapat menggunakan Gnu PG dalam penyandian. Ukuran kunci *default* adalah 1024 bit. Ini telah memadai untuk hampir semua keperluan. Ukuran kunci tidak dapat diubah lagi setelah dipilih. Kemudian menentukan berapa lama kunci ini berlaku.

Gnu PG membutuhkan kata sandi (atau kalimat sandi) untuk melindungi kunci pribadi dan kunci publik. Anda harus mengisikan kata sandi untuk melindungi *private key*, dan panjang kata sandi tidak terbatas. Kata sandi haruslah dipilih secara seksama, karena dari sudut pandang keamanan, bagian paling lemah dari Gnu PG (dan sistem penyandian lainnya) adalah kata sandi (yang digunakan untuk membuka *private key*). Idealnya, kata sandi tidak boleh menggunakan kata-kata yang terdapat dalam kamus, serta mengandung campuran huruf kapital, huruf kecil, angka dan karakter *non*-alfabet lainnya. Kata sandi yang baik sangat krusial dalam keamanan penggunaan Gnu PG.

3.1.2 Membuat *Revocation Certificate*

Setelah sepasang kunci dibuat, sebaiknya dibuat pula sertifikat penarikan kembali (*revocation certificate*) untuk *public key primer* menggunakan *option --gen-revoke*. Jika Anda lupa kata sandi yang digunakan atau *private key* Anda hilang dan jatuh ke tangan orang lain, sertifikat penarikan kembali ini dapat dipublikasikan untuk memberitahukan kepada pihak-pihak lain bahwa *public key* Anda yang mereka punyai sebaiknya tidak lagi digunakan.

Kunci dapat berupa *IDkey* dari pasangan kunci *primer* atau bagian lain dari *UserID* yang mengidentifikasikan pasangan kunci Anda. Sertifikat akan dibuat pada *file* "*sertifikat-darurat.asc*". Sebaiknya sertifikat tidak disimpan pada direktori dimana orang lain dapat mengakses, karena jika demikian dapat terjadi seseorang mempublikasikan sertifikat penarikan kembali dan mengakibatkan kunci publik menjadi tidak berguna.

3.1.3 Melihat Daftar Kunci Publik

Untuk melihat daftar kunci publik yang anda miliki, gunakan *option --list-keys*

```
[root@tasproject /]# gpg --list-keys
/root/.Gnu PG/pubring.gpg
--------------------------------
pub  1024D/5920142A 2017-02-22 Matheus Rumetna (tesproject)
< matheus@rumetna.com >
sub  1024g/3A9EEFCE 2017-02-22 [expires: 2021-12-22]
```

3.1.4 Mengekspor Kunci Publik

Anda dapat mempublikasikan *public key* yang Anda miliki pada personal *website*, melalui berbagai *key server* di internet, atau beragam cara lain. Untuk mengirimkan *public key* Anda pada orang lain, Anda harus mengekspor *public key* tersebut dengan menggunakan *option --export*. argumen tambahan diperlukan untuk menentukan *public key* yang akan diekspor. Untuk mengekspor *public key* Anda dalam format binari.

3.1.5 Mengimpor Kunci Publik

Setelah pasangan kunci selesai dibuat, Anda harus memasukkan pasangan kunci tersebut kedalam *database* pasangan kunci (yang berisi koleksi pasangan kunci dari pihak lain yang dapat digunakan untuk penyandian/penerjemahan pesan tersandi dalam komunikasi antar personal). Untuk memasukkan pasangan kunci Anda (atau pasangan kunci pihak lain) gunakan *option –import*.

3.1.6 Memvalidasi Kunci

Setelah *public key* di impor ke dalam *database*, kunci tersebut harus divalidasi dengan memverifikasi "sidik jari kunci" (*key fingerprint*), dan kemudian menandatangani kunci tersebut untuk mengesahkannya. Sidik jari dari kunci dapat dilihat dengan *option –fingerprint*. Hal ini dapat dilakukan secara langsung, melalui telepon, *email* atau sarana lain, sejauh dapat menjamin bahwa kita benar-benar berhubungan dengan pemilik kunci sebenarnya.

3.1.7 Menandatangani Kunci

Setelah mengimpor dan memverifikasi *public key* yang kita masukkan pada *database*, kini kita dapat menandatangani kunci tersebut. Dengan menandatangani kunci, kita menyatakan bahwa kita mengetahui pemilik kunci tersebut. Sebaiknya kita menandatangani kunci publik hanya jika kita 100% yakin akan keaslian kunci tersebut.

3.1.8 Memeriksa Tanda Tangan

Setelah kunci publik kita tandatangani, kita dapat memeriksa kunci tersebut untuk melihat daftar tanda tangan yang ada pada kunci tersebut, serta tanda tangan yang kita

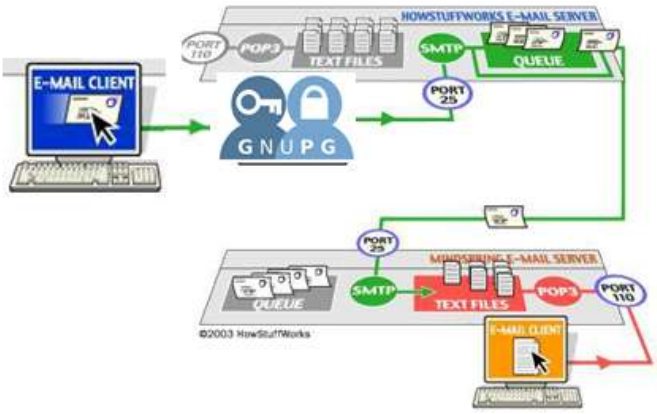
tambahkan. Setiap *UserID* di kunci akan mempunyai satu atau lebih tanda tangan. Kita dapat memeriksa tanda tangan dari suatu kunci dengan menggunakan *option --check-sigs*.

3.1.9 Penyandian dan Penerjemahan Data Tersandi

Cara menyandikan dan menerjemahkan data tersandi sangat mudah. Jika kita ingin mengirimkan data untuk RedHat, maka sandikan data tersebut dengan menggunakan *public key* dari RedHat, hingga hanya RedHat Inc saja yang dapat menerjemahkan data tersandi tersebut dengan menggunakan *private key* miliknya. Jika Mandrake ingin mengirim pesan pada kita, Mandrake akan menyandikan pesan dengan menggunakan *public key* milik kita, dan kita akan menerjemahkan data tersandi tersebut menggunakan *private key* milik kita. Anda harus mempunyai *public key* pengirim pesan pada *database* agar dapat menerjemahkan pesan tersandi dari pengirim tersebut.

3.1.10 Memeriksa Kembali Tanda Tangan

Setelah kita selesai membuat pasangan kunci dan mempublikasikannya, dengan menggunakan *option --verify* dari Gnu PG agar pihak lain dapat memeriksa apakah data tersandi yang kita kirimkan, kita tandatangani (lihat Gambar 4).



Gambar 4. Tahapan Pengiriman *Email* Menggunakan Gnu PG

3.2 Mengkombinasikan Gnu PG Dan *Hamming Distance*

Pengguna saling bertukar pesan atau saling mengirim pesan, proses yang dilakukan oleh Gnu PG adalah untuk mengamankan *email* mulai dari membuat sepasangan kunci hingga memeriksa tanda tangan telah dilakukan. Selanjutnya, algoritma *Hamming Distance* akan diterapkan disini untuk membuat jalur sertifikasi terpercaya dan juga untuk mempersingkat rantai *link*.

Dalam sistem ini, pengguna (atau node) protokol otentikasi adalah untuk memverifikasi jalan otentikasi dari pengguna utama (*Tn*) ke pengguna lain/*client* (*Vn*) dengan cara sebagai berikut [12]:

1) Pengguna memperoleh jalur sertifikasi dari *Tn* untuk *Vn* menggunakan repositori sertifikatnya dan repositori sertifikat node lain melalui jaringan dan dipasang pada Gnu PG, proses ini disebut dengan konstruksi jalur sertifikasi.
2) Pengguna *Tn* memeriksa bahwa semua sertifikat harus valid (atau tidak dicabut) dan benar, proses ini disebut dengan validasi jalur sertifikasi. Difokuskan pada pembangunan jalur sertifikasi karena kita dapat menggunakan algoritma jalur validasi RFC3280 untuk validasi jalur sertifikasi.

Disini, akan dijelaskan mengenai karakteristik dasar *Hamming Distance* antara dua bilangan bulat dan konsep *Hamming Distance* untuk meningkatkan ukuran repositori setiap node dan memungkinkan pembangunan jalur sertifikasi. Menggunakan teori:

For $a \in Z_n$, *define* $R_a = \{ x \in Z_n \mid HD(a, x) = 1 ,\}$,
then $|R_a| = \log_2 N$, *where* $Z_n = \{0, 1, 2,..., N-1, 2^m , m > 0\}$ (1)

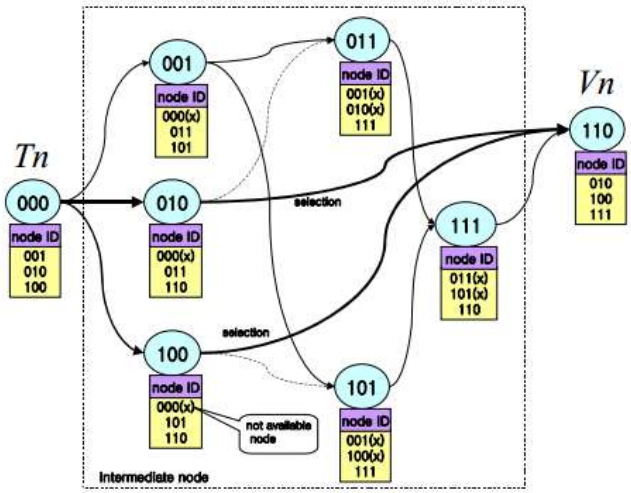
Definisi 1: Sertifikat ID (*Identification Number*) dalam jaringan yaitu unsur Z_n, {0, 1, 2, ..., N -1, 2^m, m> 0}, dan ukuran maksimum jaringan didefinisikan sebagai N. Namun, karena node dalam jaringan yang berubah, jumlah node yang terlibat dalam jaringan yang sebenarnya didefinisikan sebagai *Nr*.

Definisi 2: ID dari dua node, *a* dan b, didefinisikan sebagai a_{ID} ($\in Z_n$) dan b_{ID} ($\in Z_n$) dan jarak *Hamming* antara ID ini didefinisikan sebagai HD (a, b) atau (HD).

Definisi 3: Sebuah node *a* dalam *store* jaringan dan mengelola beberapa sertifikat *public key* dalam jaringan di repositori Gnu PG dalam rangka untuk membangun jalur sertifikasi. Pada saat ini, node *a* didefinisikan sebagai orangtua simpul (*PN*) dan set node yang disimpan kemudian dikelola dalam repositori dari *PN* didefinisikan sebagai node anak (*CN*). Selain itu, salah satu *CN* didefinisikan sebagai CN_i. Setiap node *ID* memenuhi kondisi berikut: *HD* (*PN*, CN_i) = 1.

Definisi 4: Ketika sebuah node *a* mencoba untuk mengotentikasi node *b*, sebuah jalur sertifikasi terpercaya dari node *a* ke node *b* didefinisikan sebagai $Auth_p\ (a \rightarrow b)$. Pada titik ini, mari kita mendefinisikan node *a* sebagai *Tn* dan node *b* sebagai *Vn*.

Gambar 5. Tahapan Pengiriman *Email* Menggunakan Gnu PG Dan *Hamming Distance*



Gambar 6. Konsep Jalur Sertifikasi Konstruksi *Hamming Distance*

Hasil dari konsep ini diharapkan bahwa dengan menggunakan Gnu PG, kita dapat mengamankan *email* dari masalah keamanan karena Gnu PG dapat mengirim *email* dengan penyandian. Menyandikan data dan dokumen serta mengirimkan data atau dokumen secara terenkripsi melalui jaringan, dimana hal ini lebih baik dibandingkan apabila kita secara langsung mengirimkan *email* tanpa Gnu PG, karena *email* yang kita kirimkan tanpa melakukan enkripsi terlebih dahulu sangat rentan terhadap masalah keamanan serta kerahasiaannya. Kemudian dikombinasikan dengan algoritma *Hamming Distance* untuk membuat jalur sertifikasi terpercaya dan juga untuk mempersingkat rantai *link*, hal ini sangat membantu prinsip kerja Gnu PG menjadi lebih cepat dan stabil (lihat Gambar 5 dan 6).

4. KESIMPULAN

Beberapa masalah keamanan yang terkait dengan sistem *email* adalah disadap, dipalsukan, disusupi virus, *spamming*, *mailbomb*, *mail relay*. Tetapi kerahasiaan *email* terancam bukan oleh para peretas saja, melainkan para sistem administrator sendiri. Hal ini dapat diatasi dengan menggunakan Gnu PG untuk mengamankan *email* dari ancaman orang lain. Hal ini sangat membantu, terutama ketika berhadapan dengan informasi sensitif, karena cara komunikasi yang terenkripsi. Enkripsi Gnu PG hanya berguna ketika kedua belah pihak menggunakan praktik keamanan yang baik dan waspada tentang praktik keamanan yang lain.

Program ini dapat digunakan untuk menyandikan pesan *email*, data atau dokumen rahasia juga dapat digunakan untuk mengirimkan data tersandi via jaringan secara aman. Dari uraian di atas beberapa kegunaan Gnu PG:

1) Mengirimkan email tersandi.
2) Menyandikan data dan dokumen.
3) Mengirimkan data/dokumen tersandi melalui jaringan.

Algoritma *Hamming Distance* dalam konsep ini digunakan untuk membuat jalur sertifikasi terpercaya dan juga untuk mempersingkat rantai *link*, hal ini sangat membantu prinsip kerja Gnu PG menjadi lebih cepat dan stabil.

Agar lebih meningkatkan keamanan email, ke depannya mungkin dapat menggabungkan atau mengkolaborasikan 2 program untuk kemanan agar celah yang ada pada Gnu PG yaitu untuk penyandian dapat ter-*cover* oleh program lainnya tetapi dengan tidak mengesampingkan perihal kecepatan komputasi.

DAFTAR PUSTAKA

[1] M. Tariq Banday, "Effectiveness and Limitations of E-Mail Security Protocols," *Int. J. Distrib. Parallel Syst.*, vol. 2, no. 3, pp. 38–49, 2011, doi: 10.5121/ijdps.2011.2304.

[2] S. Gavankar and S. Vidhani, "Email Security System," vol. 8, no. 3, pp. 347–351, 2017.

[3] E. Ismaredah, "Keamanan E-Mail Menggunakan Metode Enkripsi Gnupg Dengan Squirellmail Dan Thunderbird," *Jupiter*, vol. 7, no. 2, pp. 13–22, 2015, [Online]. Available: https://media.neliti.com/media/publications/289148-keamanan-e-mail-menggunakan-metode-enkri-2fb119a3.pdf.

[4] T. N. Lina, D. Manongga, and A. Iriani, "PENERAPAN FRAMEWORK KNOWLEDGE MANAGEMENT PADA UKM KULIT PARI YOGYAKARTA," in *Seminar Nasional GEOTIK*, 2017, pp. 139–145.

[5] M. S. Rumetna, M. Pieter, and M. Manurung, "APLIKASI PENGENALAN KARAKTER ALFANUMERIK MENGGUNAKAN ALGORITMA HAMMING DISTANCE," *Pros. SNATIF*, no. 4, pp. 77–84, 2017, [Online]. Available: https://media.neliti.com/media/publications/173678-ID-aplikasi-pengenalan-karakter-alfanumerik.pdf.

[6] T. N. Lina and Sem, "PENERAPAN METODE DECISION TREE UNTUK PENENTUAN NILAI PRINSIP-PRINSIP E-PROCUREMENT," in *Seminar Nasional GEOTIK*, 2017, pp.

10–19.

[7] M. S. Rumetna and I. Sembiring, "PEMANFAATAN CLOUD COMPUTING BAGI USAHA KECIL MENENGAH (UKM)," in *Prosiding Seminar Nasional Geotik*, 2017, no. ISSN:2580-8796, pp. 1–9.

[8] M. S. Rumetna, "Pemanfaatan Cloud Computing Pada Dunia Bisnis: Studi Literatur," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 3, pp. 305–314, 2018, doi: 10.25126/jtiik.201853595.

[9] H. Hamid, "Analisis Keamanan Aplikasi Email Bawaan Android Dan Gmail Pada Jaringan Nirkabel," *Teknoin*, vol. 23, no. 2, pp. 125–136, 2017, doi: 10.20885/teknoin.vol23.iss2.art5.

[10] B. Sutedjo and D. Oetomo, "Efektivitas Email Untuk Pemasaran," *J. Eksplor. Karya Sist. Inf. dan Sains*, vol. 2, no. 2, 2015, [Online]. Available: https://ti.ukdw.ac.id/ojs/index.php/eksis/article/view/390.

[11] K. Sivaraman and P. Arumugam, "The security related to electronic mail," *Int. J. Pure Appl. Math.*, vol. 119, no. 12, pp. 9665–9671, 2018, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85048791552&partnerID=40&md5=8b1073b9a96c3ce8760e28dc91e79840.

[12] S. Lee and J. Song, "Public-Key Management System using Hamming Distance for Mobile Ad Hoc Network," vol. 6, no. 8, pp. 172–181, 2006.

[13] D. Riyadi, "STUDI ANALISIS PENGGUNAAN GNU PRIVACY GUARD (GPG) SEBAGAI ENKRIPSI KEAMANAN EMAIL BERBASIS WINDOWS," Indonusa Eda Unggul, 2010.

[14] M. El-Dairi and R. J. House, "Optic nerve hypoplasia," *Handbook of Pediatric Retinal OCT and the Eye-Brain Connection*. pp. 285–287, 2019, doi: 10.1016/B978-0-323-60984-5.00062-7.

[15] M. S. Rumetna, T. N. Lina, L. Simarmata, L. Parabang, A. Joseph, and Y. Batfin, "Pemanfaatan POM-QM Untuk Menghitung Keuntungan Maksimum UKM Aneka Cipta Rasa (ACR) Menggunakan Metode Simpleks," in *GEOTIK*, 2019, pp. 12–22.

[16] T. N. Lina *et al.*, "PENERAPAN METODE SIMPLEKS DALAM OPTIMALISASI KEUNTUNGAN HASIL PRODUKSI LEMON CINA DAN DAUN JERUK PURUT," *Elektro Luceat*, vol. 6, no. 1, 2020.

[17] M. S. Rumetna *et al.*, "BERBASIS WEBSITE PADA PERUSAHAN CENDRAWASIH WIPUTRA MANDIRI KOTA SORONG DESIGN OF A WEBSITE-BASED DEMAND INFORMATION SYSTEM IN CENDRAWASIH WIPUTRA MANDIRI COMPANY," *Elektro Luceat*, vol. 7, no. 1, pp. 10–19, 2021.

[18] M. S. Rumetna *et al.*, "PENDAMPINGAN DAN PELATIHAN PENERAPAN METODE SIMPLEKS PADA USAHA DAGANG BINTANG TIURMA," *J. Abdimas Bina Bangsa*, vol. 01, no. 02, pp. 205–214, 2020.

[19] M. S. Rumetna, T. N. Lina, T. P. Sari, P. Mugu, A. Assem, and R. Sianturi, "Optimasi Jumlah Produksi Roti Menggunakan Program Linear Dan Software POM-QM," *Comput. Based Inf. Syst. J.*, vol. 09, no. 01, pp. 42–49, 2021.

[20] S. Rumalutur, Alimuddin, and E. P. Sianipar, "SISTEM KONTROL OTOMATIS PENGISIAN TANGKI BBM DAN MONITORING SUHU MENGGUNAKAN PLC," *J. Elektro Luceat*, vol. 6, no. 1, 2020.