KEAMANAN EMAIL MENGGUNAKAN METODE PRETTY GOOD PRIVACY DENGAN ALGORITMA RSA

[1]Ridwan Ighfirlana Ananda, [2]Fauziah, [3]Nur Hayati
[1,3]Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional
Jl. Sawo Manila No. 61, Pasar Minggu 12520, Jakarta
[1]ridwan404.ri@gmail.com, [2]fauziah@civitas.unas.ac.id, [3]nurhayati@civitas.unas.ac.id

Abstrak

Seiring dengan perkembangan teknologi di era sekarang, semua orang dapat dengan mudah berkomunikasi dengan menggunakan layanan surat menyurat elektronik yang dinamakan email. Email mampu berkomunikasi antar pengguna ke pengguna lainnya melalui internet. Saat berkomunikasi tidak jarang memasukan data yang bersifat rahasia dan dapat dengan mudah diambil oleh orang lain jika tidak memiliki keamanan yang cukup pada email. Maka dibutuhkan proses enkripsi (penyandian pesan) untuk menjaga data saat proses pengirimannya. Penelitian ini menggunakan metode PGP (Pretty Good Privacy) dengan menggunakan algoritma RSA (asimetris) yaitu sebuah algoritma yang mampu menghasilkan sepasang kunci (public dan private) untuk proses enkripsi dan dekripsi. Pada pengujian dengan menggunakan 8 data yang di enkripsi dan dikirim secara acak ke beberapa user, menunjukan hasil informasi data yang telah berubah dari segi size file dan hash yang dilakukan dengan menggunakan MD5. Dari hasil pengujian data yang telah di enkripsi menggunakan algoritma RSA dengan Pretty Good Privacy, dengan format .TXT menunjukan perbedaan size file. Dengan size file data asli 7,402 Bytes dan size file yang di enkripsi menjadi 7,777 Bytes.

***Kata Kunci**: Enkripsi, Email, Metode Pretty Good Privacy, RSA*

Abstract

Along with technological developments in the present era, everyone can easily communicate using an electronic correspondence service called email. Email is able to communicate between users to other users via the internet. When communicating, it is not uncommon to enter data that is confidential and can be easily retrieved by other people if they do not have sufficient security in email. Then an encryption process (message encoding) is needed to protect the data during the transmission process. This study uses the PGP (Pretty Good Privacy) method using the RSA (asymmetric) algorithm, which is an algorithm capable of generating a pair of keys (public and private) for the encryption and decryption process. In testing using 8 data that is encrypted and sent randomly to several users, it shows the results of data information that have changed in terms of file size and hash which is done using MD5. From the results of testing the data that has been encrypted using the RSA algorithm with Pretty Good Privacy, with the .TXT format showing the difference in file size. With the original data file size of 7,402 Bytes and the encrypted file size to 7,777 Bytes.

***Keywords**: Encrypt, Email, Pretty Good Privacy Method, RSA*

PENDAHULUAN

Seiring dengan perkembangan teknologi yang semakin maju, proses untuk melakukan surat menyurat menjadi lebih mudah, karena di era sekarang ini sudah ada teknologi "email". Email adalah suatu layanan kirim surat menyurat berbasis online, yang mana ini

akan memudahkan setiap pengguna karena waktu yang dibutuhkan menjadi cepat dan lebih efisien. Tidak hanya berkirim surat menyurat seperti teks dan file, email mampu mengirimkan ke beberapa orang yang dituju dalam sekali pengiriman.

Terkadang saat melakukan pengiriman email, tidak jarang pihak pengirim mengirimkan informasi teks maupun file yang bersifat rahasia atau hanya boleh diketahui oleh pihak penerima. Jika saat proses pengiriman berlangsung dan penerima menerima email dari pengirim, itu aman. Tetapi jika saat proses pengiriman berlangsung dan penerima tidak menerima email dikarenakan dalam proses pengi-rimannya email diambil oleh orang lain ataupun salah dalam menuju ke alamat penerima itu akan jadi merepotkan kepada pihak pengirim, karena informasi tidak sampai kepada penerima yang dituju.

Enkripsi dan dekripsi menggunakan metode *Pretty Good Privacy* untuk mengatasi permasalahan seperti email yang diambil oleh orang lain ataupun salah dalam alamat pengiriman. Algoritma yang dihasilkan pada saat menggunakan *Pretty Good Privacy* adalah algoritma RSA. merupakan algoritma kriptografi kunci *public* (asimetris), sebagai algoritma kunci *public*, RSA mempunyai dua kunci, yaitu kunci *public* dan *private* [1]. Saat melakukan proses mengirim maupun menerima email dengan metode PGP, pengguna dapat melakukan *signing document* sebagai verifikasi bahwa email tersebut dikirimkan oleh pengirim (asli). Proses email yang akan dikirimkan maupun diterima akan lebih aman dan terjaga dikarenakan memiliki proses enkripsi dan dekripsi yang hanya bisa diakses oleh orang yang memiliki *public key* penerima.

Penelitian terdahulu telah dilakukan uji coba terhadap algoritma RSA untuk pengamanan file yang menghasilkan suatu proses enkripsi dan dekripsi dengan menggunakan program visual basic dengan cara kerja program membuat kunci yang akan digunakan saat enkripsi dan dekripsi dengan menerapkan algoritma RSA [2]. Penelitian berbasis *mail* server zimbra yang menghasilkan sebuah proses pengiriman file dengan membandingkan file saat pengiriman tanpa PGP dan pengiriman dengan PGP untuk ukuran file tersebut dengan menggunakan metode *Pretty Good Privacy* [3]. Penelitian berbasis data digital yang menghasilkan sebuah proses enkripsi dan dekripsi isi file, dengan cara saat file telah di enkripsi isi nya tidak dapat dibaca dan berbeda dengan isi file asli untuk melihatnya menggunakan Hex Editor dengan menerapkan algoritma RSA dan fungsi hash SHA-512 [4].

Penelitian ini dilakukan dengan menggunakan sistem *mail* server yaitu Zimbra *mail* dengan mengirim data email secara acak. Zimbra merupakan aplikasi email server berlisensi bebas dimana memiliki fitur-fitur yang lengkap dan juga kemudahan untuk *installasi* maupun

management mail server, meskipun masalah keamanan *mail* server menjadi faktor utama. Pada *mail* server zimbra dengan metode enkripsi untuk keamanan data email, sehingga dapat memberikan kontribusi terhadap kerahasiaan dalam pengiriman data atau penyimpanan data dengan menyem-bunyikan informasi melalui metode enkripsi dan sebagai bahan pembelajaran. Pentingnya sebuah keamanan data pada suatu jarinagn internet dalam upaya perbaikan sistem keamanan [5]. Peneliti juga melakukan pengujian terhadap metode *Pretty Good Privacy* dengan algoritma RSA (kunci *public* dan *private*) untuk mengetahui sebarapa cukup baik teknik enkripsi dan dekripsi yang dimiliki metode tersebut dan uji coba terhadap hasil data yang telah di enkripsi. Dengan tujuan penelitian untuk menganalisa seberapa cukup baik teknik enkripsi yang dimiliki sistem PGP terhadap data email [6].

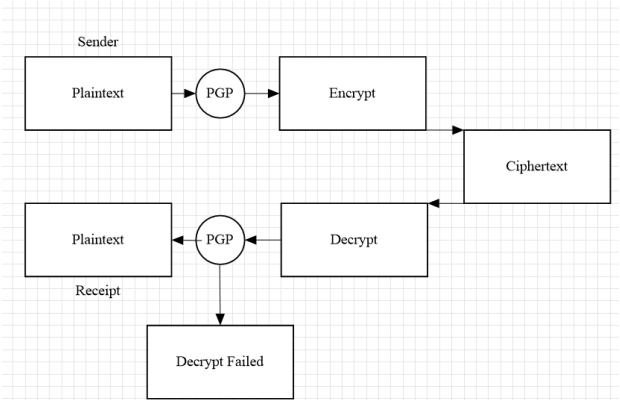
METODE PENELITIAN

Metode penelitian terdiri dari beberapa tahapan. Tahapan pertama adalah keamanan email, proses akan berjalan saat plaintext dikirim dan di enkripsi menjadi ciphertext. Tahapan kedua adalah pembuatan kunci *public* dan *private* yang berada pada algoritma RSA, pembuatan kunci ini berfungsi untuk proses enkripsi dan dekripsi. Tahapan ketiga adalah dengan menggunakan tanda tangan digital yang dibuat oleh sistem, proses yang dilakukan melibatkan kedua belah pihak yang akan berkomunikasi, dimana kedua belah pihak ini harus menyiapkan sepasang kunci, yaitu kunci *private* dan kunci *public*. Kunci *private* hanya dipegang oleh pemiliknya secara personal, sedangkan kunci *public* dapat diberikan kepada siapapun yang memer-lukannya, dan terakhir adalah rancangan sistem yang dipakai untuk melakukan pengujian.

A. Pretty Good Privacy

Keamanan *Pretty Good* P*rivacy* (PGP) menggunakan sistem kunci *private* dan kunci *public*. Proses pengiriman plaintext, isi email akan di enkripsi dan diubah menjadi ciphertext dan untuk melakukan dekripsi ciphertext, proses yang dibutuhkan yaitu pihak pengirim harus mempunyai *public key* penerima. Jika tidak memiliki nya maka, dekripsi akan gagal dan ciphertext tidak dapat di dekripsi.

Gambar 1 menjelaskan alur dari metode PGP yang bekerja dengan cara, dari pihak *sender* mengirimkan email berupa file (plaintext) yang akan di proses oleh PGP untuk menghasilkan enkripsi berupa file (ciphertext). Kemudian file (ciphertext) di proses kembali untuk melakukan dekripsi oleh PGP, yang nantinya menghasilkan file (plaintext) saat proses berhasil. Jika proses dekripsi gagal maka file (ciphertext) tidak dapat diubah menjadi file (plaintext).



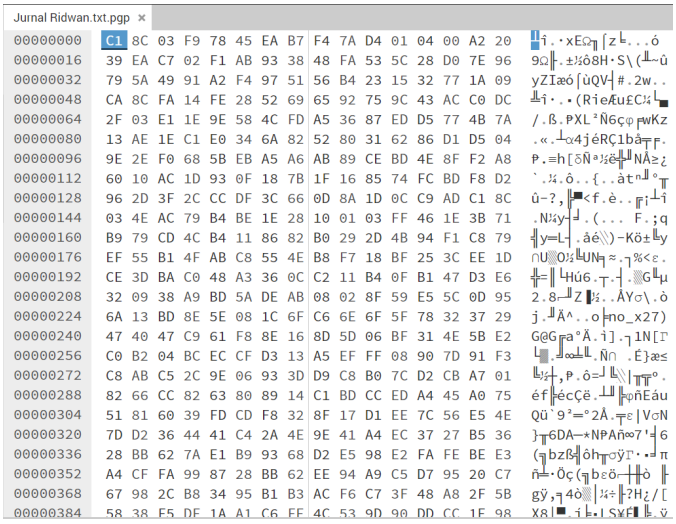
Gambar 1. Alur Diagram PGP

Jurnal Ridwan.txt

```
00000000  4A 75 64 75 6C 3A 20 53 69 73 74 65 6D 20 45 6E  Judul: Sistem En
00000010  6B 72 69 70 73 69 20 4B 65 61 6D 61 6E 61 6E 20  kripsi Keamanan
00000020  45 6D 61 69 6C 20 44 65 6E 67 61 6E 20 4D 65 74  Email Dengan Met
00000030  6F 64 65 20 50 72 65 74 74 79 20 47 6F 6F 64 20  ode Pretty Good
00000040  50 72 69 76 61 63 79 20 4D 65 6E 67 67 75 6E 61  Privacy Mengguna
00000050  6B 61 6E 20 41 6C 67 6F 72 69 74 6D 61 20 52 73  kan Algoritma Rs
00000060  61 0D 0A 50 65 6E 75 6C 69 73 3A 20 52 69 64 77  a..Penulis: Ridw
00000070  61 6E 20 49 67 68 66 69 72 6C 61 6E 61 20 41 6E  an Ighfirlana An
00000080  61 6E 64 61 2C 20 46 61 75 7A 69 61 68 2C 20 4E  anda, Fauziah, N
00000090  75 72 20 48 61 79 61 74 69 0D 0A 0D 0A 50 61 64  ur Hayati....Pad
000000A0  61 20 6A 75 64 75 6C 20 73 69 73 74 65 6D 20 65  a judul sistem e
000000B0  6E 6B 72 69 70 73 69 20 6B 65 61 6D 61 6E 61 6E  nkripsi keamanan
000000C0  20 65 6D 61 69 6C 20 73 65 62 61 69 6B 6E 79 61   email sebaiknya
000000D0  20 63 75 6B 75 70 20 64 69 62 75 61 74 20 6B 65   cukup dibuat ke
000000E0  61 6D 61 6E 61 6E 20 65 6D 61 69 6C 20 6D 65 6E  amanan email men
000000F0  67 67 75 6E 61 6B 61 6E 20 6D 65 74 6F 64 65 20  ggunakan metode
00000100  70 72 65 74 74 79 20 67 6F 6F 64 20 70 72 69 76  pretty good priv
00000110  61 63 79 20 64 65 6E 67 61 6E 20 61 6C 6F 67 6F  acy dengan alogo
00000120  72 69 74 6D 61 20 52 53 41 0D 0A 0D 0A 41 42 53  ritma RSA....ABS
00000130  54 52 41 4B 0D 0A 4B 61 74 61 20 22 64 69 20 61  TRAK..Kata "di a
00000140  6D 62 69 6C 22 20 64 69 73 61 6D 62 75 6E 67 0D  mbil" disambung.
00000150  0A 4B 61 6C 69 6D 61 74 20 22 4D 61 6B 61 20 64  .Kalimat "Maka d
00000160  69 20 70 65 72 67 75 6E 61 6B 61 6E 20 6D 65 74  i pergunakan met
00000170  6F 64 65 20 50 47 50 20 2E 2E 22 20 73 65 62 61  ode PGP .." seba
00000180  69 6B 6E 79 61 20 50 65 6E 65 6C 69 74 69 61 6E  iknya Penelitian
```

Gambar 2. File Plaintext

Enkripsi berfungsi untuk merubah isi file asli yaitu plaintext dan merubahnya ke dalam format yang tidak bisa dibaca. Dengan melakukan perbandingan file asli dan file cipher, dengan begitu peneliti dapat mengetahui tingkat keamanan enkripsi *Pretty Good Privacy*. Gambar 2 menampilkan file (plaintext) sebelum dilakukannya proses enkripsi oleh PGP, dapat dilihat isi file dari (plaintext) masih dapat terbaca dengan jelas. Seperti contoh kata *Judul* memiliki kode (4A 75 64 75 6C). Gambar 3 menampilkan file (plaintext) yang telah di enkripsi dan dapat terlihat isi dari file (ciphertext) telah berubah, yang tadinya memiliki kode (4A 75 64 75 6C) dengan contoh *Judul*, menjadi format yang tidak bisa dibaca dengan kode awal berubah menjadi (C1 8C 03 F9 78).



Gambar 3. File Ciphertext

B. Algoritma RSA

Algoritma RSA merupakan salah satu algoritma kunci asimetris. RSA (Rivest-Shamir-Adleman) adalah sebuah kriptografi kunci *public* yang berdasarkan pada eksponensial terbatas bilangan bulat (Z_N) di mana N adalah sebuah bilangan bulat gabungan dari dua faktor besar yaitu (semi-prime). RSA memiliki keamanan yang tinggi dikarenakan penggunaan dua kunci yang berbeda pada proses enkripsi dan dekripsinya dan sulitnya memfaktorkan bilangan menjadi factor prima dengan tujuan mendapat kunci untuk proses dekripsi [7]. Algoritma ini digunakan untuk kepentingan autentikasi, yakni dengan kata lain data dan informasi benar-benar berasal dari sumber yang benar [8]. Oleh karena itulah kunci pada algoritma ini berbeda saat enkripsi dan dekripsi. Algoritma ini terletak pada proses eksponensial dan pemfaktoran bilangan menjadi 2 bilangan prima yang hingga kini perlu untuk waktu yang lama untuk melakukan pemfaktorannya.

Tahapan kunci enkripsi dan dekripsi:

1. Pilih dua bilangan prima, p (19) dan q (17) yang bersifat rahasia
2. Hitung n = (p x q) = (19 x 17 = 323)
3. Hitung m = (p-1) x (q-1) = (18 x 16 = 288)
4. Menentukan nilai "e" dengan syarat nilai yang relatif lebih prima untuk menghasilkan public key. gcd(e,m) = 1 maka menghasilkan gcd(13, 288) = 1. Dimana "13" adalah nilai yang memenuhi syarat untuk nilai "e", nilai e bersifat tidak rahasia, untuk memastikan apakah gcd(13,288) = 1:

   288 mod 13 = 2

   13 mod 2 = 1

   13 mod 1 = 0
5. Menentukan nilai "d" untuk menghasilkan private key dengan syarat (d*e) mod m = 1 menghasilkan (421*13)

mod 288 = 1. Dimana "421" adalah nilai yang memenuhi syarat untuk nilai "d", nilai d bersifat rahasia. Untuk memastikan apakah (421*13) mod 288 = 1:

5473 mod 288 = 1

6. Dapat disimpulkan public key (e,n) = (13, 323) dan private key (d,n) = (421, 323)

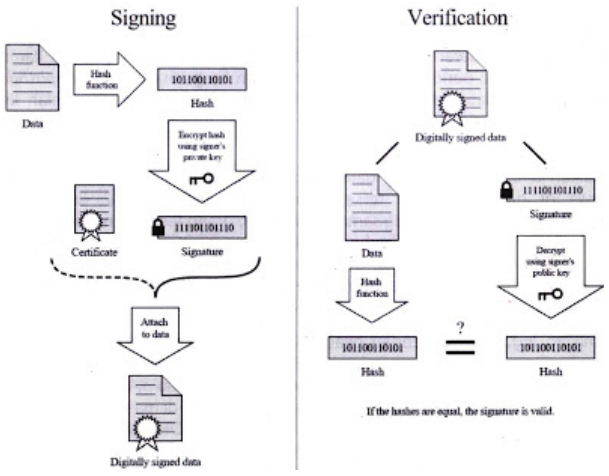
C. Digital Signature

Digital signature adalah sebuah tanda tangan yang dibuat secara elektronik oleh sistem. Tanda tangan ini tidak dapat dipalsukan oleh orang lain dikarenakan menggunakan *public key* dan *private key* yang diterbitkan oleh *Certification Authority*. Saat melakukan enkripsi isi email, file, dan *text* [9]. Tanda tangan ini menggunakan algoritma SHA256 sebagai proses hash.

Gambar 4 menunjukan proses bagaimana tanda tangan digital ini bekerja, pertama melakukan *signing* dengan data yang telah di hash dan di enkripsi menggunakan *private key*. Di dalam data yang telah di *signing* terdapat *certificate* yang berisi tanda tangan pengirim yang dibuat otomatis oleh sistem. Saat melakukan *verification*, data yang sebelumnya sudah di tanda tangan akan di dekripsi dengan menggunakan *public key* untuk proses hash. Jika hasil menunjukan hash yang sama, maka tanda tangan telah valid dan jika hasil hash nya berbeda maka tanda tangan tidak valid.

D. Rancangan Sistem

Rancangan sistem ini meliputi beberapa *hardware* dan *software* pendukung untuk menunjang keberhasilan pengujian sistem yang telah dibuat dapat dilihat pada Tabel 1 dan Tabel 2.



Gambar 4. Alur Digital Signature

Tabel 1. Hardware

No	Nama Perangkat	Spesifikasi	Jumlah
1	Laptop	i7-1065G7 RAM 8 GB SSD 500 GB	1
2	Wifi	Indihome 20 Mbps	1

Tabel 2. Software

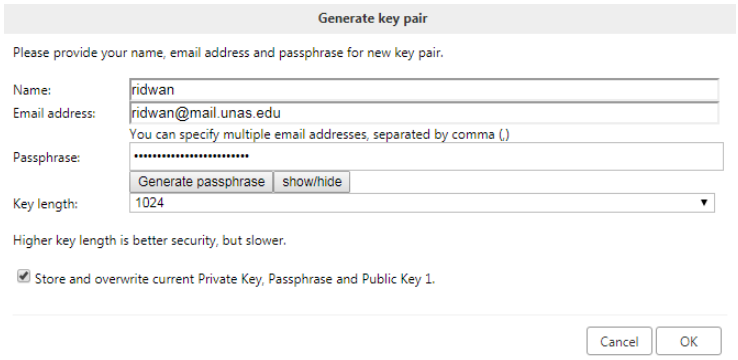
No	Nama Perangkat	Spesifikasi	Jumlah
1	Linux Virtualbox	SSD 29 GB RAM 2,9 GB	1
2	Windows 7 Virtualbox	SSD 36 GB RAM 2,2 GB	1

HASIL DAN PEMBAHASAN

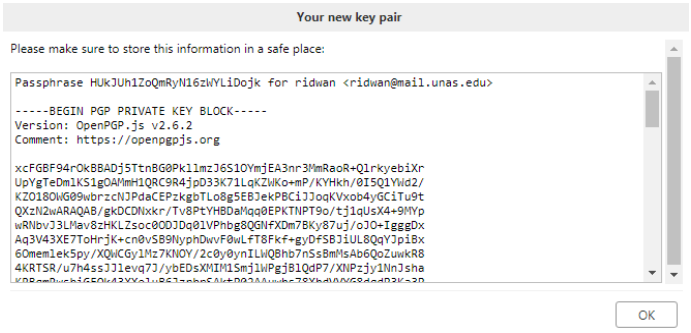
Uji coba dilakukan dengan melakukan implementasi pada sistem email untuk mengetahui seberapa baik sistem enkripsi yang dimiliki *Pretty Good Privacy*.

A. Penerapan Pretty Good Privacy

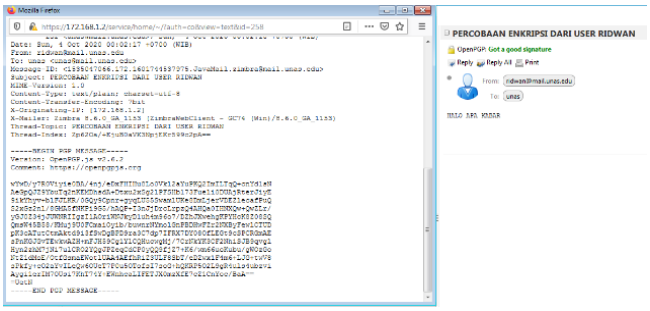
Peneliti melakukan implementasi pada sistem dengan membuat *public key* dan *private key* dengan panjang *key* 1024 bit. Panjang kunci menentukan seberapa kuat algoritma yang dipakai atau dengan kata lain tingkat keamanan bergantung dengan panjangnya kunci yang dipakai untuk pembuatan algoritma RSA. Dalam hal ini keamanan yang dipakai menggunakan dengan panjang kunci 1024 bit sudah cukup baik dari segi keamanan, karena kunci kriptografi ini memakai bilangan prima yang saat ini belum dipecahkan [10]. Gambar 5 menunjukan proses pembuatan kunci algoritma RSA yang meliputi informasi personal seperti ; nama, email, *passphrase* dan panjang kunci 1024 bit. Gambar 6 menunjukan hasil dari pembuatan kunci algoritma RSA dengan informasi personal yang ditampilkan berupa ; *passphrase*, nama, email, serta *private key* dan *public key*.



Gambar 5. Generate Key

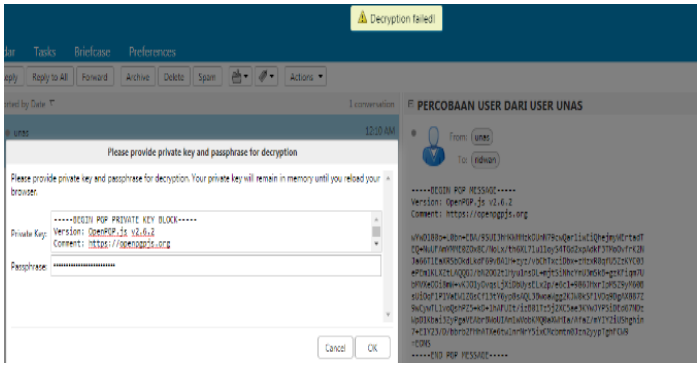


Gambar 6. Key Pair User Ridwan

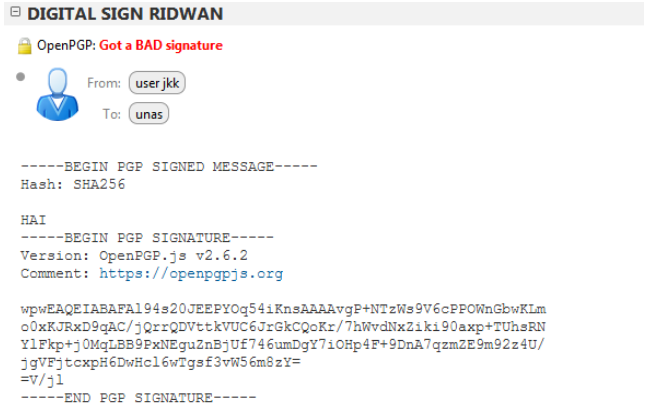


Gambar 7. Proses Dekripsi Berhasil

Gambar 7 menunjukan bahwa proses pengiriman email enkripsi yang berasal dari user ridwan kepada user unas telah berhasil di dekripsi. Proses ini dapat berhasil dikarenakan pihak pengirim memiliki kunci *public* penerima. Gambar 8 menunjukan proses telah gagal karena pengirim tidak memiliki *public key* penerima, sehingga email yang dikirim tidak dapat di dekripsi oleh penerima.



Gambar 8. Proses Dekripsi Gagal



Gambar 9. Signature Palsu

B. Tampilan Digital Signature

Tampilan ini merupakan tanda tangan digital yang dikirim oleh pengirim kepada penerima. Apabila "*Got a good signature*" maka email dikirim oleh pengirim yang sebenarnya dan apabila "*Got a bad signature*" bisa dipastikan bahwa email dikirim oleh orang lain yang mencoba memasulkan isi email. Gambar 9 menunjukan tanda tangan digital yang berusaha dipalsukan oleh pihak lain.

Seperti yang bisa dilihat pada status tanda tangan dengan informasi "*Got a bad signature*". Walaupun alamat email berisikan identitas yang sama akan tetapi tanda tangan ini tidak dapat dipalsukan.

Gambar 10. Signature Asli

Gambar 10 menunjukan tanda tangan digital yang asli. Seperti yang bisa dilihat pada status tanda tangan dengan informasi "*Got a good signature*".

C. Pengujian Pretty Good Privacy

Pada tahap ini dilakukan uji coba enkripsi dengan menggunakan 8 data yang akan dikirim ke beberapa user secara acak. Isi dari data yang telah di enkripsi akan di cek menggunakan hash MD5 dengan membandingkan size dari data, dengan tujuan untuk mengetahui apakah keamanan data yang telah di enkripsi sama seperti data asli atau tidak.

Tabel 3 menunjukan hasil yang diperoleh setelah dilakukan pengujian terkait data yang dikirim ke beberapa user dengan format yang berbeda. Pada hasil pengujian menunjukan hasil yang cukup baik. karena informasi data telah berubah dengan metode *Pretty Good Privacy*.

Tabel 3. Hasil Pengujian

			Data Asli / Pengirim				Data Dengan PGP / Penerima	
No	**User**	**Data**	**MD5**	**Size Bytes**	**User**	**Data**	**MD5**	Size Bytes
1	user1	unas.txt	3c51fdb37711f947b03a80282a2ca33c	7,402	user8	unas.txt.pgp	8f3569765d3b71c8fd067a0299d8ec72	7,777
2	user2	coba.topo	72890258293abbb082b43fad975dc703	3,719	user22	coba.topo.pgp	33dfee727ae04af921c094cd4852466b	4,236
3	user3	macan.jpg	ff9be549db73e64ac47ad4e56673aef4	130,633	user15	macan.jpg.pgp	1863f3fb6c2601c71fe306ac7ca78987	131,156
4	user4	jurnal ridwan.txt	44f2f528ba1d59d3d923c4fd31aca1b5	2,945	user11	jurnal ridwan.txt.pgp	1c33050fcd2aa3d3f0f692529999f6b1	3,320
5	user5	putty.exe	dcf21ca46349ce36f7866c24f1f60f0f	1,179,024	user22	putty.exe.pgp	27dc54493dcf1e38a75514ddf1e63fb1	1,179,405
6	user6	subnetting.xlsx	90c32a972f6d99bcea9654309687b910	10,972	user8	subnetting.xlsx.pgp	9d4a91d5e21c67ef7e825a7bfc81b222	11,353
7	user7	tutor.txt	9bcac9e9d9d91055bd556a9fd80d4aae	2,884	user8	tutor.txt.pgp	e10aadb8e1441c8453aeefe33236afbf	3,401
8	user8	format jurnal.docx	f38aa6e768db706aa6bd70ff6db8fc70	56,137	user17	format jurnal.docx.pgp	88b09aecdaed0700a8fcfa1b44d811c3	56,518

KESIMPULAN

Berdasarkan hasil pengujian yang telah dilakukan dengan menggunakan 8 data email yang dikirim ke beberapa user menunjukan bahwa sistem PGP cukup baik untuk teknik enkripsi. Seperti dari hasil pengujian metode ini, menunjukan hasil data yang telah di enkripsi dengan PGP, menghasilkan size file yang berbeda dari file asli jika di bandingkan. Misalnya pada data dengan format .TXT menunjukan dari size file asli 7,402 *Bytes* dan size file yang telah di enkripsi menjadi 7,777 *Bytes*. Untuk hash data email menggu-nakan MD5 juga menunjukan bahwa informasi data yang asli dan data hasil enkripsi telah berubah.

DAFTAR PUSTAKA

[1] A. P. Wahyadyatmika, R. R. Isnanto, and M. Somantri, "Implementasi Algoritma Kriptografi Rsa Pada Surat Elektronik (E-Mail)," *Transient*, vol. 3, no. 4, Des., pp. 443-450, 2014.

[2] J. Manurung, K. Sirait, and J. F. Panggabean, "Penerapan Algoritma RSA untuk Pengamanan File," *Jurnal Mantik Penusa*, vol. 2, no. 2, Des., pp. 112-116, 2018.

[3] D. P. Hostiadi, and I. B. Suradarma, "Implementasi Pengamanan PGP pada Platform Zimbra Mail Server," *Lontar Komputer*, vol. 8, no. 1, Apr., pp. 41-52, 2017.

[4] A. A. J. SinlaE, E. Ngaga, and S. D. B. Mau, "Rancang Bangun Kriptosistem untuk Pengamanan Data-data Digital," *Jurnal Maklumatika*, vol. 5, no. 1, Jul., pp. 64-75, 2018.

[5] A. Setiawan, "Implementasi Teknik Pretty Good Privacy (PGP) Pada Mail Server Zimbra Dengan Metode Enkripsi Untuk Keamanan Data Email Pada Data Center IAIN Syekh Nurjati Kota Cirebon," *Jurnal ICT: Information Communication & Technolog*y, vol. 17, no. 2, Des., pp. 60-64, 2018.

[6] A. Ginting, R. R. Isnanto, and I. P. Windasari, "Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email," *Jurnal Teknologi dan Sistem Komputer*, vol. 3, no. 2, Apr., pp. 253-258, 2015.

[7] M. I. Zulfikar, G. Abdillah, and A. Komarudin, "Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA)," In Proc. Seminar Nasional Aplikasi Teknologi Informasi '03, 2019, pp. 19-26.

[8] Pahrizal, and D. Pratama, "Implementasi AlgoritmA RSA untuk Pengamanan Data Berbentuk Teks," *Jurnal Pseudocode*, vol. 3, no. 1, Feb., pp. 44-49, 2016.

[9] M. Ihwani, "Model Keamanan Informasi Berbasis Digital Signature dengan Algoritma RSA," *Journal Of*

Computer Engineering System And Science, vol. 1, no. 1, Jan., pp. 15-20, 2016.

[10] N. Iriadi, "Analisis Keamanan E-Mail Menggunakan Pretty Good Privacy," *Paradigma*, vol. 13, no. 1, Mar., pp. 30-43, 2011.