RESOLUSI : Rekayasa Teknik Informatika dan Informasi
ISSN 2745-7966 (Media Online)
Vol 3, No 2, November 2022
Hal 49-54
https://djournals.com/resolusi

Pengimplementasian Algoritma RSA Untuk Mengamankan E-mail Menggunakan Outlook dan OpenPGP

Sri Ana Margareth Nababan, Resad Setyadi*

Fakultas Informatika, Sistem Infromasi, Institut Teknologi Telkom Purwokerto, Banyumas, Indonesia
Email: [1]19103066@ittelkom-pwt.ac.id, [2*]resad@ittelkom-pwt.ac.id
Email Penulis Korespondensi: resad@ittelkom-pwt.ac.id

Abstrak−Perkembangan teknologi cukup membantu manusia dalam menjalankan aktifitasnya sehari hari. Dengan adanya teknologi manusia bisa mengakses data dan informasi dimana pun dan kapanpun dengan mudah. Penggunaan teknologi yang paling sering digunakan orang orang adalah untuk berkomunikasi karena bisa terhubung dengan cepat dan mudah. Banyaknya kegiatan yang bisa dilakukan melalui teknologi membuat sebagian orang membutuhkan keamanan dan kerahasiaan dalam aktifitas serta dalam komunikasinya. Algoritma RSA memiliki 2 jenis key dalam keamanannya yaitu Public key dan Private key. Public key bisa diberikan kepada siapapun sedangkan untuk private key hanya bisa diketahui oleh orang orang yang berkepentingan saja. MsOutlook adalah software yang bisa digunakan bertukar pesan dengan orang lain dan OpenPGP adalah software yang dilengkapi dengan kemampuan kriptografi yaitu enkripsi dan dekripsi. Enkripsi digunakan untuk mengubah pesan yang awalnya Plaintext menjadi ciphertext dan dekripsi digunakan untuk menerjemahkan ciphertext menjadi plaintext. Tujuan dari penelitian ini adalah membantu menjelaskan bagaimana cara dari MsOutlook dan OpenPGP saling terintegrasi untuk membantu menjaga kerahasiaan pesan yang dikirimkan. Adapun untuk hasil yang diperoleh dari hasil penelitan ini adalah menampilkan keberhasilan enkripsi dan dekripsi dalam menjaga kerahasiaan pesan yang telah dikirimkan dengan menggunakan passphrase untuk akses pesan tersebut.

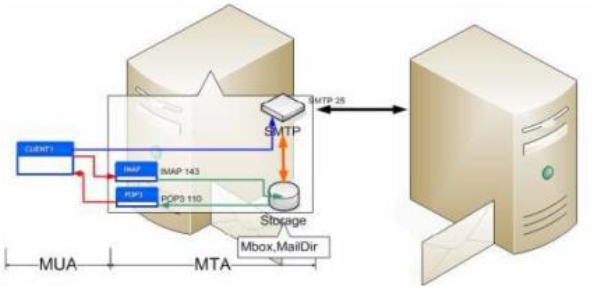
Kata Kunci: E-mail; Kriptografi; Ms.Outlook; Open PGP; RSA

Abstract−The development of technology is enough to help humans in carrying out their daily activities. With the existence of technology, humans can easily access data and information anywhere and anytime. The use of technology most often used by people is to communicate because it can connect quickly and easily. The many activities that can be carried out through technology make some people need security and confidentiality in their activities and in their communications. The RSA algorithm has 2 types of keys for security, namely the Public key and the Private key. The public key can be given to anyone while the private key can only be known by interested people. MsOutlook is software that can be used to exchange messages with other people and Open PGP is software that is equipped with cryptographic capabilities, namely encryption and decryption. Encryption is used to convert messages that were originally plaintext to ciphertext and decryption is used to translate ciphertext to plaintext. The purpose of this research is to help explain how MsOutlook and Open PGP are integrated with each other to help maintain the confidentiality of messages sent. As for the results obtained from the results of this research is to display encryption and decryption in maintaining the confidentiality of messages that have been sent by using a passphrase to access the message.

Keywords: E-mail; Cryptography; MsOutlook; Open PGP; RSA

1. PENDAHULUAN

Perkembangan teknologi di era sekarang sangat mengandalkan teknologi dikarenakan mempermudah aktivitas manusia dalam banyak aspek salah satunya mengakses data dan informasi. Penggunaan yang paling sering dilakukan adalah sebagai media perantara untuk melakukan komunikasi. Implementasinya yang sangat sering digunakan adalah e-mail. E-mail adalah singkatan dari Electronic Mail yang berfungsi untuk melakukan pengiriman surat atau pesan digital menggunakan jaringan internet [1]. Pada tahun 1960-an saat internet belum terbentuk dengan baik, e-mail mulai dipakai. E-mail sudah dinikmati oleh secara umum sejak mulai 1980-an yang mengakibatkan pengiriman surat dari perusahaan pos sudah mulai ditinggalkan [2]. Cara kerja e-mail dikirim ke penerima (end-user) dan surat dikumpulkan terlebih dahulu dalam server komputer (host) dan biasanya penyimppanannya lebih besar dibandingkan komputer biasa. Komputer yang melayani penerimaan e-mail secara terus-menerus tersebut biasa disebut dengan mailserver atau mailhost. Penjelasan cara kerja e-mail akan dijelaskan melalui Gambar 1 [3].



Gambar 1. Cara Kerja E-mail

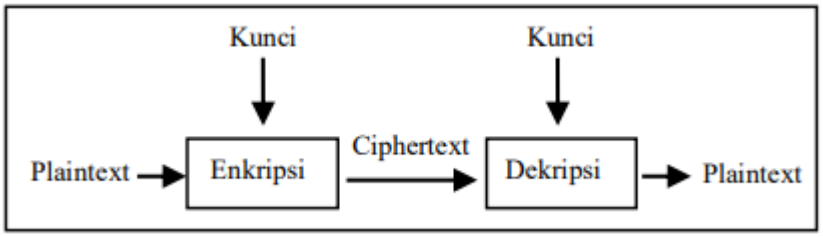
Dikarenakan maraknya data yang penting dalam penggunaan e-mail, beberapa oknum mulai melakukan kejahatan demi keuntungan diri sendiri seperti pemalsuan e-mail, peretasan, dan pembobolan. Oleh karena itu untuk pengiriman dan melakukan penerimaan e-mail diperlukan aspek dalam menjaga keamanan informasi[4].

ISSN 2745-7966 (Media Online)
Vol 3, No 2, November 2022
Hal 49-54
https://djournals.com/resolusi

Dari permasalahan yang ada maka diperlukan solusi / antisipasi untuk meningkatkan keamanan pada data dan informasi. Salah satunya solusi yang dapat diterapkan yaitu dengan menerapkan metode kriptografi dalam menjaga keamanan, kerahasian, dan keaslian informasi di email. Kriptografi merupakan suatu ilmu yang membahas aspek keamanan informasi, seperti kerahasian data, validnya data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi [5]. Secara umum kriptografi adalah teknik dalam mengamankan informasi yang telah diubah sedemikian rupa sehigga menjadi suatu informasi baru dan tidak dapat dipahami oleh orang yang tidak berkepentingan dan jika infromasi ingin diubah kembali ke dalam bentuk aslinya hanya dilakukan oleh orang yang memiliki kunci akses [6].

Kriptografi memiliki 2 proses yaitu enkripsi dan dekripsi . Enkripsi merupakan proses perubahan pesan/teks asli (plaintext) menjadi suatu pesan dalam bahasa sandi (ciphertext) [7]. Bahasa sandi yang dimaksud berupa set karakter, angka, simbol, dan kata yang telah ditentukan. Secara singkat proses enkripsi yaitu algoritma yang mengubah plaintext ke dalam bentuk ciphertext dengan menggunakan sebuah kunci. Proses dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi. Dekripsi adalah proses pembuatan kembali pesan dalam suatu bahasa sandi menjadi pesan asli. Pada dasarnya data yang sudah dienkripsi tidak bisa dibaca dan dimengerti tanpa menggunakan kunci . Secara singkat proses dekripsi yaitu algoritma yang mengubah ciphertext ke dalam plaintext dengan menggunakan sebuah kunci [8].

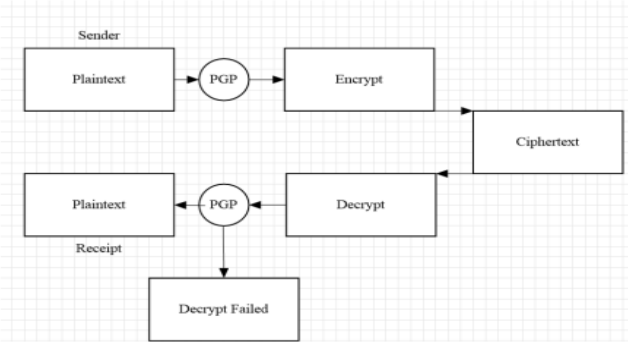
Keamanan data dapat diatasi dengan menggunakan kunci yang dirahasiakan. Kunci akan memiliki fungsi sebagai parameter utama untuk melakukan proses perubahan inputan. Dengan menggunakan kunci maka dapat digambarkan skema dari enkripsi dan dekripsi melalui Gambar 2 [9].



Gambar 2. Alur enkripsi dan dekripsi menggunakan kunci

Algoritma kriptografi dibagi menjadi 2 kelompok dalam hal penggunaan kunci yaitu Algoritma Kriptografi Simetris dan Algoritma Kriptografi Asimetris[10], [4] Pada penelitian sebelumnya menerpakan algoritma RSA. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (Massachusetts Institute of Technology) pada tahun 1976, yaitu: Ron (R)ivest, Adi(S)hamir, dan Leonard (A)dleman [11]. RSA merupakan algoritma kriptografi kunci publik (asimetris). Nama RSA merupakan singkatan dari nama tiga orang pembuatnya, yaitu Rivest, Shamir, dan Adleman [12]. Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. RSA mendasarkan proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmetika modulo. Baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan bulat [10]. Algoritma RSA adalah sebuah block cipher algoritm (algoritma yang bekerja per blok data) yang mengelompokkan plaintext menjadi blok-blok terlebih dahulu sebelum dilakukan enkripsi hingga menjadi ciphertext [13].

Penelitian lainnya menerapkan PGP dalam mengamankan e-mail. Pretty Good Privacy (PGP) adalah program komputer yang dikembangkan Phil Zimmermann pada tahun 1991. Program ini mampu untuk mengirimkan pesan, e-mail, ataupun file dengan menambahkan fitur kerahasiaan dan authentifikasi pengguna dengan menggunakan tanda tangan digital [14]. Keamanan PGP menggunakan private key dan public key sehingga menggunakan algoritma kriptografi asimetris. Cara kerja PGP yaitu pengirim akan mengirimkan e-mail berupa plaintext kemudian akan diproses oleh PGP untuk menghasilkan sebuah ciphertext. Nantinya ciphertext akan diproses kembali untuk dilakukan dekripsi oleh PGP, sehingga menghasilkan plaintext jika proses berhasil (menggunakan private key). Gambar 5 akan menjelaskan alur dari metode PGP.



Gambar 3. Alur Diagram PGP

RESOLUSI : Rekayasa Teknik Informatika dan Informasi
ISSN 2745-7966 (Media Online)
Vol 3, No 2, November 2022
Hal 49-54
https://djournals.com/resolusi

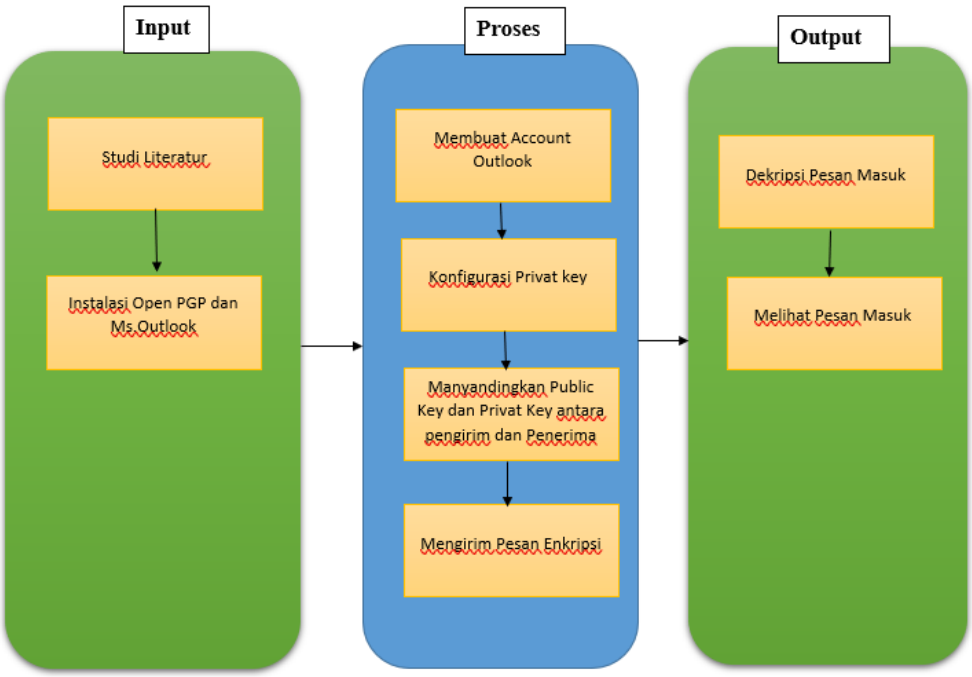
Pada penelitian alat yang digunakan untuk melakukan pengiriman dan penerimaan e-mail adalah Outlook. Outlook adalah perangkat lunak uang memiliki fungsi utama membantu mengolah waktu dan informasi baik sebagai klien e-mail maupun manajemen kalender, pengelolaan tugas, pengelolaan kontak, pencatatan, pencatatan jurnal, dan melakukan penjelajahan web. Outlook adalah produk dari perusahaan Microsoft yang dirilis pada tahun 1997. Outlook juga dapat diakses melalui versi web, sehingga membuat Oulook menjadi software yang kompatibel [15].

Penelitian ini bertujuan mengetahui bagaimana proses pengamanan pesan melalui proses enkripsi dan dekripsi menggunakan Outlook. Proses pengamanan dilakukan dengan dua tahap yaitu melakukan enkripsi pada e-mail yang akan dikirim menggunakan alat bantu enkripsi OpenPGP. Kedua mengenkripsi kunci asimetris menggunkaan algoritma RSA. Dengan kombinasi tersebut maka akan menjadi jalan keluar untuk menjadikan pengamanan pada informasi yang lebih kuat.

2. METODOLOGI PENELITIAN

2.1 Alur Penelitian

Pada bagian ini akan dipaparkan mengenai tahapan penelitian yang akan dimulai dari input, proses dan output seperti berikut:



Gambar 4. Alur Penelitian

a. Studi Literatur

Dalam mendukung kelancaran proses penelitian, terlebih dahulu melakukann studi literatur melalui jurnal, serta penelitian terdahulu mengenai alur bagaimana penelitian terlaksana serta mempelajari hal hal yang berkaitan dengan penelitian[16].

b. Instalasi Open PGP dan Ms. Outlook

Setelah melakukan studi literatur dan melihat beberapa acuan maka akan dilanjutkan dengan penginstalan software untuk melakukan penelitian ini. Ada 2 jenis software yang harus diinstal yakni: Open PGP dan Ms. Outlook. Ms.Outlook menjadi sarana dalam melakukan tukar pesan seperti email pada umumnya , dan Open PGP adalah alat tambahan yang akan otomatis terhubung dengan Ms.Outlook setelah kita lakukan instalasi.

c. Membuat Account Outlook

Membuat account atau login dalam Ms.outlook untuk bisa bertukukar pesan dengan orang lain sesuai dengan kebutuhan dari user.

d. Konfigurasi Privat Key

Setelah kita login ke dalam Ms.Outlook maka akan otomatis muncul beberapa fitur yang bisa digunakan untuk proses pengaturan privat key, enkripsi, dekripsi, pengaturan, dan beberapa fitur lainnya. Selanjutnya adalah ketahap konfigurasi atau pembuatan privat key yang akan kita gunakan untuk membuka pesan yang telah dikirimkan orang lain kepada penerima.

e. Menyandingkan Publik Key dan Privat Key

Untuk bisa melakukan enkripsi dan dekripsi pesan, maka antara penerima dan pengirim harus bertukar privat key dan publik key serta melakukan konfiurasi di accountnya masing masing.

ISSN 2745-7966 (Media Online)
Vol 3, No 2, November 2022
Hal 49-54
https://djournals.com/resolusi

f. Mengirim Pesan Enkripsi

Setelah melakukan penyandingan antara pengirim dan penerima, maka tahap selanjutnya adalah melakukan kirim pesan dengan melakukan enkripsi pada pesan yang dikirim. Pesan yang awalnya berupa kalimat atau kata (Plaintext) akan diubah menjadi bentuk yang tidak bisa dibaca dan lebih aman (Ciphertext).

g. Dekripsi Pesan

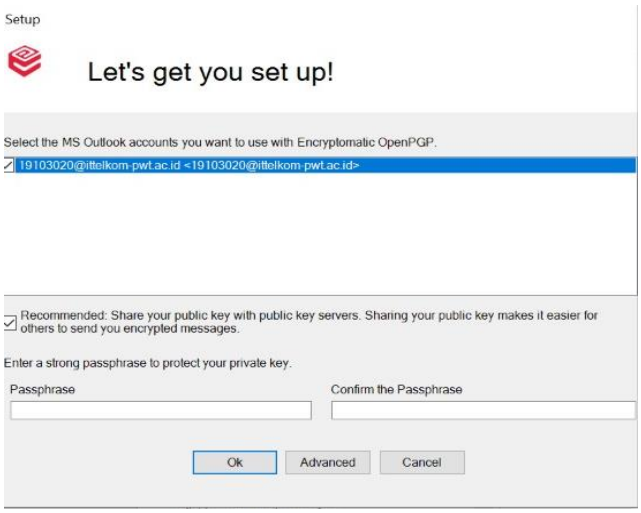
Setelah menerima pesan dari pengirim, maka format yang diterima adalah pgp serta apabila filenya dibuka maka akan mencul ciphertext yang tidak bisa dibaca tanpa melakukan dekripsi. Untuk melakukan dekripsi pada pesan, maka perlu memasukkan Privat key dari penerima. Apabila sender ingin membuka kembali pesan yang telah dikirim, maka sender memerlukan privat key dari penerima karena pesan tersebut telah diatur untuk bisa dibuka hanya dengan privat key dari penerima.

h. Pesan Terbaca

Menampilkan pesan yang telah didekripsi sebelumnya, maka yang awalnya jenis filenya pgp (Ciphertext) akan muncul menjadi plaintext sesuai yang dikirim oleh sender.

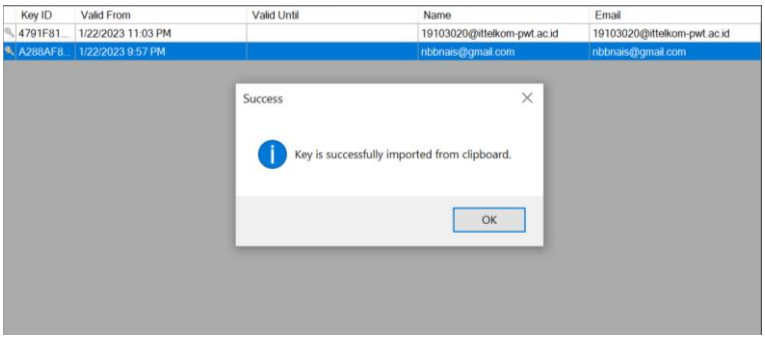
3. HASIL DAN PEMBAHASAN

Dalam penelitia ini menggunakan software yang sudah dirancang utuk memiliki kemampuan dalam melakukan enkripsi dan dekripsi pada pesan. Penelitian ini bertujuan mengetahui bagaimana proses pengamanan pesan melalui enkripsi dan dekripsi menggunakan Outlook dan OpenPGP. Adapun tahapan awal yan dilakukan setelah melakukan penginstalan dan login account e-mail adalah perlu dilakukan konfigurasi privat key (pada OpenPGP disebut passphrase). Tampilan konfigurasi privat key dapat dilihat pada Gambar 5.



Gambar 5. Konfigurasi private key (passphrase)

Tahapan selanjutnya yaitu melakukan penyandingan public key dan private key antara si pengirim dan penerima pesan. Hal ini dilakukan dikarena penerapan Algoritma RSA kedua belah pihak harus memiliki kedua kunci agar dapat melakukan proses enkripsi dan dekripsi. Jika kedua pihak hanya membagikan salah satu kunci saja, maka nantinya akan ada proses yang tidak bisa dijalankan baik enkripsi atau dekripsi. Berikut pada Gambar 8 ditampilkan bahwa kedua pihak berhasil menyandingkan kedua kunci.

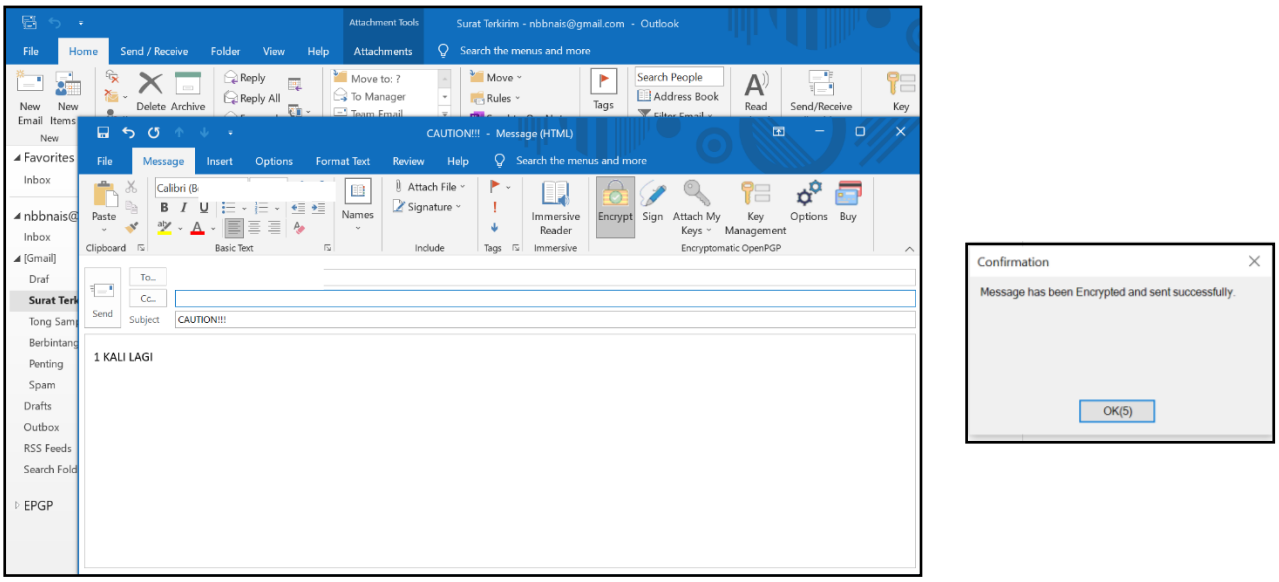


Gambar 6. Proses penyandingan kedua kunci

Setelah konfigurasi berhasil maka kedua pihak akan saling terhubung dan dapat melakukan proses enkripsi dan dekripsi pesan. Maka langkah ini dapat dilakukan pengiriman pesan dengan cara pilih New Mail => isi kelengkapan pesan (penerima, subject, body pesan atau dapat melampirkan file) => kemudian pilih fitur encrypt => masukkan private key

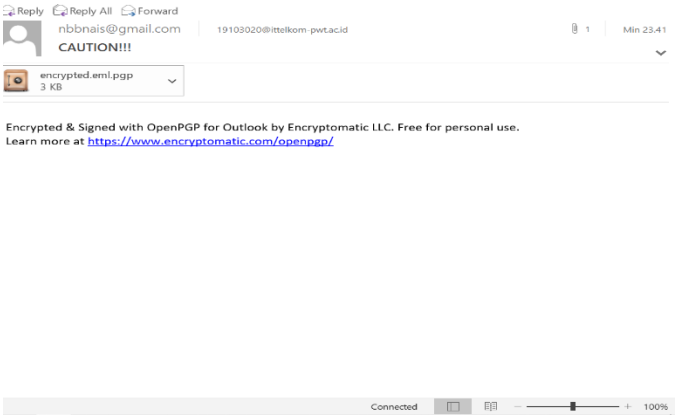
ISSN 2745-7966 (Media Online)
Vol 3, No 2, November 2022
Hal 49-54
https://djournals.com/resolusi

=> setelah selesai kirim pesan. Gambar 7 adalah tampilan dari proses pengiriman pesan yang dienkripsi. Jika berhasil maka akan muncul pop up berhasil .



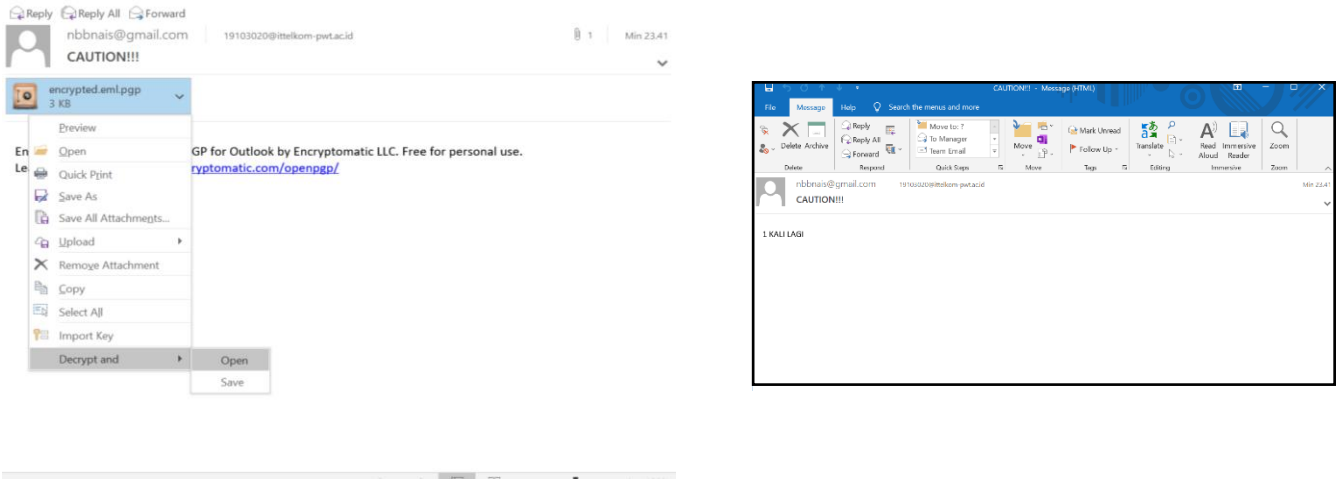
Gambar 7. Proses pengiriman email

Jika sudah maka selanjutnya si penerima perlu melakukan pengecekan email terhadap email masuk. Ketika pesan sudha masuk maka akan muncul isi pesan seperti Gambar 8.



Gambar 8. Tampilan e-mail yang sudah di enkripsi

Pesan akan berbentuk seperti file terlampir. Saat ingin membuka file pesan akan ada pilihan decrypt => pilih open atau save yang akan tampil pada Gambar 9. kemudian masukkan privat key milik si penerima pesan, maka akan tampil pesan yang sudah menjadi plaintext.



Gambar 9. Proses dekripsi pesan

4. KESIMPULAN

Electronic Mail (e-mail) menjadi sebuah alat yang digunakan setiap orang dalam berkomunikasi atau bertukar pesan, baik berupa file dokumen, gambar, audio,teks dan berbagai jenis lainnya. Ada beberapa pesan yang cukup ingin dijaga kerahasiaan dan integritasnya serta hanya orang orang tertentu saja yang bisa mengakses pesan yang dikirimkan. Dengan Ms.Outlook dan Open PGP user bisa mendapatkan keamanan pengiriman dan penerimaan pesan berupa enkripsi dan dekripsi. Dalam proses keamanannya menggunakan RSA yang memiliki public key dan private key untuk menjaga keamanannya. Antara account pengirim dan account penerima harus tersanding terlebih dahulu (bertukar public key dan private key) agar bisa terhubung satu sama lain. Pesan yang awalnya berupa plaintext dari pengirim, akan diubah menjadi Ciphertext saat proses pengirimannya serta tampilan dipenerima akan berupa file pgp yang membutuhkan passphrase (Privat key) untuk bisa melihat pesan yang telah dikirimkan. Hal yang perlu diketahui saat pengirim mengirimkan pesan yang terenkripsi kepada orang lain, apabila pengirim ingin membaca pesan kembali tersebut maka memerlukan private key dari pada penerima pesan. Hal ini cukup tinggi keamanannya karena apabila orang lain ingin mengakses pesan dari account pengirim, maka tidak bisa diakses dengan gampang karena hanya orang orang tertentu yang memiliki akses untuk private key satu sama lainnya.

REFERENCES

[1] A. Mawarsih, “PENGARUH ELECTRONIC MAIL SEBAGAI MEDIA KOMUNIKASI TERKADAP MENGERJAKAN TUGAS KULIAH MAHASISWA,” Ejurnal Ilmu Komunikasi, vol. 2, no. 1, pp. 334–348, 2014.

[2] B. Hozairi et al., “Implementasi Kriptografi Pada File Attachment Email IMPLEMENTASI KRIPTOGRAFI PADA FILE ATTACHMENT EMAIL,” no. c, pp. 75–81, 2018.

[3] R. Saleh and I. Imelda, “Kriptografi Email menggunakan Algoritma Rivest Code 6 (Rc6) berbasis Java Pada PT. XYZ,” Proceeding Seminar Nasional …, vol. 6, 2018.

[4] Suhardi, “Aplikasi Kriptografi Data Sederhana Dengan Metode Exlusive-or (Xor),” Jurnal Teknovasi, vol. 03, no. 2, pp. 23–31, 2016.

[5] M. M. Amin, “Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks,” Pseudocode, vol. 3, no. 2, pp. 129–136, 2017, doi: 10.33369/pseudocode.3.2.129-136.

[6] A. Cahya Putra, M. Simanjuntak, and Nurhayati, “Penerapan Algoritma Rivest Shamir Adleman (Rsa) Untuk Mengamankan Database Program Keluarga Harapan (PKH),” Jurnal Teknik Informatika Kaputama (JTIK), vol. 5, no. 1, pp. 76–84, 2021.

[7] M. I. Zulfikar, G. Abdillah, and A. Komarudin, “Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA),” Seminar Nasional Aplikasi Teknologi Informasi (SNATi), pp. 19–26, 2019.

[8] A. Rosyadi, “Implementasi Algoritma Kriptografi AES Untuk Enkripsi Dan Dekripsi Email,” Transient, vol. 1, no. 3, pp. 2–6, 2012.

[9] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, “Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard,” Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer, vol. 10, no. 1, p. 20, 2016, doi: 10.30872/jim.v10i1.23.

[10] 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, p. 253, 2015, doi: 10.14710/jtsiskom.3.2.2015.253-258.

[11] D. Apdilah and H. Swanda, “Penerapan Kriptografi RSA Dalam Mengamankan File Teks Berbasis PHP,” Jurnal Teknologi Informasi, vol. 2, no. 1, p. 45, 2018, doi: 10.36294/jurti.v2i1.407.

[12] M. Rizki and P. Farida Ariyani, “Penerapan Kriptografi Dengan Menggunakan Algoritma Rsa Untuk Pengamanan Data Berbasis Desktop Pada Pt Trias Mitra Jaya Manunggal,” Skanika, vol. 4, no. 2, pp. 1–6, 2021, doi: 10.36080/skanika.v4i2.1991.

[13] D. P. Pahrizal, “Implementasi Algoritma Rsa Untuk Pengamanan Data Berbentuk Teks,” Jurnal Pseudocode, vol. III, no. 1, p. ISSN : 2355 – 5920, 2013.

[14] R. I. Ananda, Fauziah, and N. Hayati, “Keamanan Email Menggunakan Metode Pretty Good Privacy Dengan Algoritma Rsa,” Jurnal Ilmiah Informatika Komputer, vol. 25, no. 3, pp. 213–224, 2020, doi: 10.35760/ik.2020.v25i3.3118.

[15] P. I, “Microsoft Outlook Bagi Pemula,” JIKEM: Jurnal Ilmu Komputer, Ekonomi dan Manajemen, vol. 2, no. 2, pp. 2871–2879, 2022.

[16] R. Setyadi, A. Fattah, and B. Waseso, “Trust Effect on Business-IT Governance Alignment in Society Culture (A Case Study in Indonesia),” 2019 7th International Conference on Cyber and IT Service Management, CITSM 2019, no. January 2020, pp. 2–7, 2019, doi: 10.1109/CITSM47753.2019.8965411.