APLIKASI PENGAMANAN *FILE EMAIL* DENGAN METODE KRIPTOGRAFI *RIVEST CODE* 4 (RC4) DAN STEGANOGRAFI *END OF FILE* (EOF) PADA PT. PRATAMA INDOMITRA KONSULTAN

Faris Nur Abdurrahman[1)], Purwanto[2)]
[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260
E-mail : afarisnur16@gmail.com[1)], purwanto@budiluhur.ac.id[2)]

Abstrak

Pertukaran informasi dan komunikasi dibutuhkan oleh setiap orang, salah satu medianya adalah media elektronik email. Email mampu memberi kemudahan dan kecepatan dalam mengakses. Oleh karena itu, media elektronik ini membawa dampak keamanan. Salah satu dampak nya adalah banyak pihak yang akan mencari cara untuk membobol email untuk mendapatkan dan mencuri informasi yang ada pada email tersebut. Informasi yang didapat oleh pihak yang tidak bertanggung jawab dapat dimanipulasi dan disalahgunakan. Dibutuhkanlah aplikasi untuk pengamanan isi pesan email dan file email. Salah satu caranya dengan menggunakan kriptografi dan steganografi algoritma Rivest Code 4 (RC4) dan End Of File (EoF). PT Pratama Indomitra Konsultan merupakan perusahaan dibidang konsultasi perpajakan dan pelatihan umum. Banyak pertukaran komunikasi dan informasi yang dilakukan melalui email dengan client, salah satunya dokumen TP-Doc dan dokumen pajak. Dokumen tersebut merupakan file rahasia yang harus dijaga keamanannya. Pada penelitian ini, penulis merancang aplikasi pengamanan file email yang digabungkan dengan pengamanan isi pesan email. Aplikasi ini dibangun dengan menggunakan kriptografi dan steganografi algoritma RC4 dan EoF, serta menggunakan bahasa pemprograman Java. Dengan menggunakan algoritma tersebut diharapkan proses enkripsi dan dekripsi dapat dilakukan dengan lebih cepat dan lebih aman. Melalui aplikasi ini, file email dan isi pesan email dapat lebih terjamin keamanannya.

Kata kunci : Kriptografi, Steganografi, Algoritma *Rivest Code 4*, *End Of File*, Java, *Email*

1. PENDAHULUAN

Saat ini keamanan menjadi hal yang penting dalam sebuah sistem informasi dan komunikasi. Terlebih jika data atau informasi yang dimiliki oleh sebuah instansi perusahaan bersifat penting dan rahasia. Banyak pihak yang akan mencari cara bagaimana mendapatkan dan mengakses data atau informasi tersebut. Hal tersebut dapat menjadi masalah karena data atau informasi tersebut dapat disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. PT Pratama Indomitra Konsultan salah satu instansi perusahaan yang memiliki banyak data, dokumen dan informasi *client* serta data, dokumen dan informasi perusahaan yang bersifat rahasia dan pribadi. Salah satu contohnya isi pesan pada *email*, isi dokumen TP-Doc, data *training client*, dokumen pajak *client*, dokumen keuangan, data *cash in cash out*, surat keputusan dan surat lainnya. Dokumen atau data tersebut adalah dokumen rahasia karena berhubungan dengan data pribadi perusahaan dan data *client.* Oleh karena itu diperlukanlah pengamanan untuk menjaga isi dokumen yang dikirim melalui email agar tidak diakses oleh orang yang tidak bertanggung jawab. Aplikasi *email* sebenarnya sudah dapat dikatakan aman untuk menjaga isi dokumen namun jika password pengguna dapat diretas oleh orang yang tidak bertanggung jawab maka ia bisa masuk ke akun *email* tersebut. Untuk itu diperlukan aplikasi pengamanan *file* atau dokumen dan isi pesan di *email*. Sehingga, *email* memiliki dua pengamanan yaitu pengamanan *username* dengan *password* dan pengamanan dokumen atau *file email* yang telah dienkripsi. Metode kriptografi dapat menjadi salah satu cara untuk menjamin keamanan data. Algorima kriptografi dan steganografi yang akan digunakan pada tugas akhir ini adalah algoritma Rivest Code 4 (RC4) dan End Of File (EoF). Teknik kriptografi dan steganografi dengan algoritma tersebut dipilih karena diharapkan dengan menggunakan algoritma RC4 dan EoF dapat membuat proses enkripsi dan dekripsi data dilakukan dengan waktu yang lebih singkat dan lebih aman. Terdapat 3 masalah yang melatarbelakangi pengamanan email ini, yaitu pertama bagaimana membuat aplikasi enkripsi dan dekripsi *email* untuk mengirimkan dan menerima pesan yang bersifat rahasia sehingga terjaga keamanan dan kerahasiaan. Kedua bagaimana mengimplementasikan algoritma RC4 dan EoF ke dalam aplikasi ini serta masalah yang terakhir adalah kurang terjaminnya keamanan isi pesan *email* dan isi *file* atau dokumen data *client* yang disimpan. Tujuan dari penelitian ini adalah untuk menemukan cara mengimplementasikan menggunakan algoritma RC4 dan EoF untuk aplikasi

pengamanan isi pesan *email* dan *file* atau dokumen di *email*. Selain itu termasuk juga untuk Mengamankan isi *file* atau dokumen di *email* dan pesan *email* yang dikirim atau diterima melalui *email* pada PT Pratama Indomitra Konsultan agar tidak dapat diketahui oleh orang yang tidak berwenang dan mendekripsikan kembali isi *file* dan pesan tersebut kembali ke isi aslinya. Dan tujuan terakhir adalah menghasilkan aplikasi enkripsi *email* yang dimengerti dan digunakan oleh pengguna. Dalam penulisan penelitian ini, terdapat 4 metode yang digunakan oleh penulis dalam perancangan aplikasi keamanan isi pesan *email* yaitu studi literatur, analisa data, perancangan sistem dan pengujian sistem.

2. METODE PENELITIAN

2.1 Analisa Masalah

Setiap instansi perusahaan pastinya memiliki informasi, data dan dokumen rahasia dan penting yang tidak boleh diketahui oleh semua orang. Kerahasiaan sebuah informasi selalu menjadi masalah tersendiri untuk setiap instansi perusahaan dimana informasi, data dan dokumen yang dimiliki oleh perusahaan harus bisa diamankan. Tanpa pengamanan yang maksimal, timbul resiko kerugian yang akan dialami perusahaan tersebut apabila terdapat data penting ataupun rahasia yang hilang diambil oleh orang yang tidak bertanggung jawab. Pertukaran informasi saat ini telah berkembang pesat dan dapat membuat informasi semakin rawan untuk dicuri oleh orang yang tidak bertanggung jawab.

Kemajuan teknologi pada saat ini juga berdampak pada banyaknya orang yang dapat mengakses segala bentuk informasi, data dan dokumen serta mudahnya bertukar informasi dan mengirim pesan melalui *Email*, baik yang bersifat umum maupun pribadi. Hal ini dapat menimbulkan masalah baru, terutama masalah pengamanan *file* yang sebagian informasi, data dan dokumen (*file*) adalah data rahasia milik *client*.

Email adalah salah satu bentuk teknologi komunikasi yang paling banyak digunakan orang saat ini. Dengan menggunakan *Email,* memungkinkan untuk tidak menggunakan jasa kantor pos atau jasa pengiriman lainnya untuk mengirim informasi, data dan dokumen. *Email* juga memberikan fasilitas yang memadai dalam mengirimkan informasi, data dan dokumen yang penting melalui internet dan juga tidak perlu bertemu dengan penerima. Dengan *email* kita juga bisa melakukan pertukaran informasi, data dan dokumen dengan sangat cepat, serta murahnya biaya yang dikeluarkan. Faktor-faktor tersebutlah yang menjadi alasan PT Pratama Indomitra Konsultan menggunakan *email* sebagai media pertukaran informasi, data dan dokumen.

Seiring dengan perkembangan teknologi informasi dan komunikasi, tingkat kriminalitas dalam dunia maya atau *cybercrime* meningkat. Salah satu bentuk kriminalitas di dunia maya adalah pembobolan akun *email*, baik itu melalui teknik *phising, keyloger, wifi shiniffing* dll untuk mendapatkan *password* dan segala data yang memungkinkan semua pesan yang ada di dalam akun *email* tersebut dapat diketahui oleh *hacker*, apalagi bila dalam pesan itu terdapat *file* dan pesan yang bersifat rahasia dan penting.

2.2 Penyelesaian Masalah

Dari uraian permasalahan yang telah dijelaskan sebelumnya, maka penulis akan membuat sebuah aplikasi yang dapat digunakan untuk pengamanan *file* melalui *Email* dengan menerapkan ilmu kriptografi dan steganografi. Dengan melakukan enkripsi dan dekripsi menggunakan beberapa metode pada isi pesan *email* dan *file Email*. Pesan *Email* yang akan dirahasiakan adalah isi pesan *Email* dan *file Email* sehingga apabila akun *Email* seseorang menjadi korban kejahatan *hacker*, maka sang *hacker* tidak dapat membaca isi dari pesan *Email* dan *file Email* yang ada. Dengan menggunakan aplikasi ini, diharapkan pengguna akan dapat melakukan pertukaran data atau informasi yang sifatnya rahasia dan penting tanpa takut akan ada pihak lain yang dapat membaca atau mengetahui isi pesan dan *file* tersebut.

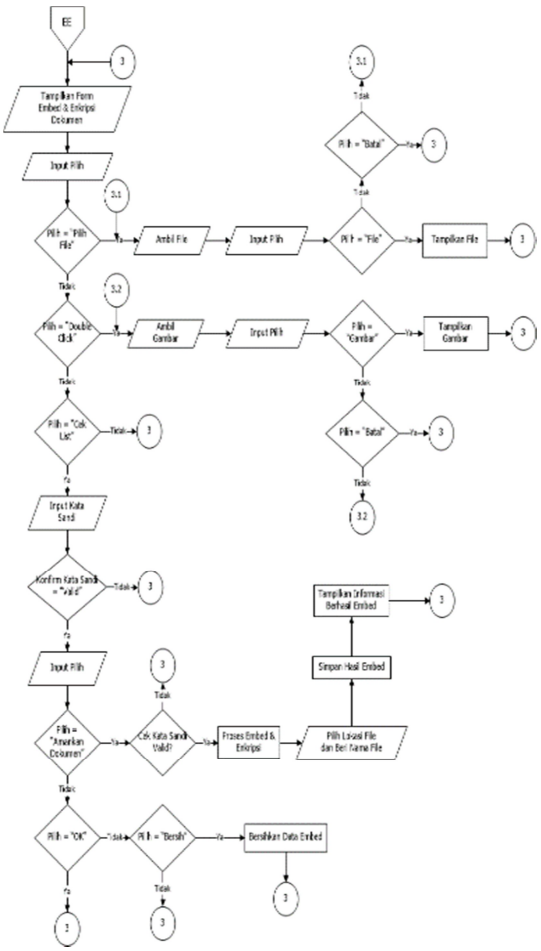
2.3 Perancangan Program

Program yang akan dibuat terdiri dari beberapa *form*, yaitu *form login*, *form* menu utama, *form* enkripsi text *email*, *form* enkripsi dan *embed file email*, *form* dekripsi teks *email*, *form* kotak masuk, *form* dekripsi dan *Retrieve email*, *form* baca *email*, *form* tulis pesan. Pada *form* menu utama terdapat beberapa menu dan sub-menu yang dapat digunakan sesuai kebutuhan pengguna, yaitu tombol hapus (untuk menghapus pesan), tombol tulis pesan (untuk menulis pesan), tombol perbarui/*refresh* (untuk memperbarui pesan) dan tombol keluar (untuk keluar dari program). Pada *form* enkripsi teks bertujuan untuk melakukan enkripsi teks, dengan cara pengguna harus meng-input isi teks dan *password* yang ingin dienkripsi. Pada *form enkripsi* dan *embed file email* digunakan untuk mengenkripsi *file* pesan *email* baru kemudian memasukkan *password* untuk melakukan enkripsi *file*, setelah itu baru pengguna memilih tombol enkripsi untuk mendapatkan hasil *file* yang isinya telah dienkripsi. *Form* dekripsi teks digunakan untuk mendekripsi teks hasil enkripsi dengan cara pengguna harus mempunyai teks hasil enkripsi dan *password*-nya, kemudian pada *form* dekripsi dan *Retrieve email* bertujuan untuk melakukan

pendekripsian isi *file* yang telah dienkripsi dengan cara pengguna terlebih dahulu memilih *file* yang telah dienkripsi tadi. Selanjutnya pengguna harus memasukkan *password* dekripsi yang sesuai dengan *password* enkripsi tadi. *Password* enkripsi yang digunakan sebagai bukti pencocokan, setelah itu barulah pengguna mengklik tombol dekripsi, jika *password* tidak cocok maka pengguna tidak dapat melakukan dekripsi *file* dan isi *file* tersebut.

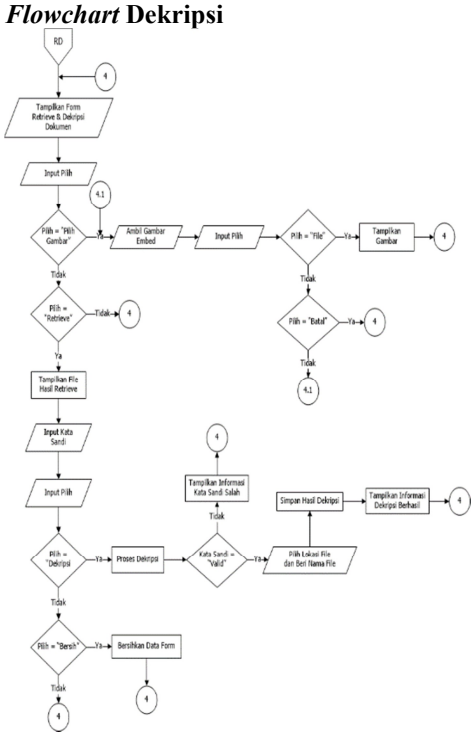
2.4 *Flowchart* Enkripsi.

Flowchart ini menjelaskan alur proses untuk mengekripsi *file*. Pengguna harus memilih *file* yang akan dienkripsi, memasukan kata sandi dan konfirmasi kata sandi. Kemudian klik tombol enkripsi. Proses enkripsi *file* akan berjalan seperti pada Gambar 1.



Gambar 1. Flowchart Enkripsi

2.5 *Flowchart* Dekripsi



Gambar 2. Flowchart Dekripsi

Flowchart ini menjelaskan alur proses untuk mendekripsi dan *Retrieve file*. Pengguna harus memasukan kata sandi yang sama dengan kata sandi enkripsi *file* tersebut dan pengguna selanjutnya klik tombol "Dekripsi" seperti pada Gambar 2.

3. HASIL DAN PEMBAHASAN

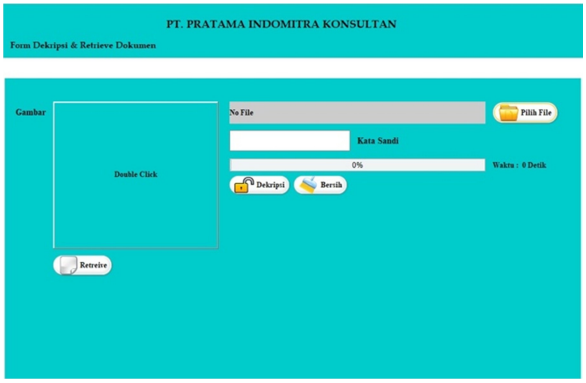
Setelah aplikasi selesai dirancang, tahap selanjutnya adalah implementasi program melalui pengkodean dan pengujian program. Agar aplikasi ini berjalan dengan baik, spesifikasi perangkat yang digunakan untuk mengimplementasi aplikasi ini juga harus didukung oleh perangkat keras dan lunak.

3.1 Tampilan Layar

Pada bagian ini, diuraikan beberapa tampilan layar aplikasi ini, tampilan layar aplikasi ini akan diuraikan pada saat memulai pertama kali aplikasi dijalankan sampai dengan selesai dijalankan. Berikut ini adalah tampilan layar aplikasi pengamanan *email* yang diikutin dengan penjelasannya.

Gambar 3. Tampilan Layar Enkripsi dan Embed Dokumen

Form enkripsi dan *embed file email* ini akan tampil ketika pengguna klik pada menu mengamankan dokumen dan submenu *embed* & enkripsi *file email*. Fungsi pada *form* ini adalah untuk mengenkripsi isi *file email*. Seperti pada Gambar 3.



Gambar 4. Tampilan Layar Dekripsi dan Retrieve Dokumen

Pada tampilan layar dekripsi *email* ini adalah untuk melakukan dekripsi teks *email*. Untuk menampilkan *form* ini, pengguna klik pada menu enkripsi dan submenu dekripsi teks *email*. Seperti pada Gambar 4.

3.2 Hasil Uji Coba Program

Pengujian program merupakan proses yang perlu dilakukan dalam pembuatan perangkat lunak *(software)* untuk mengetahui kinerja aplikasi yang dibuat dalam penelitian. Pengujian yang dilakukan pada enkripsi dekripsi *file* dokumen yang bereksistensi .docx, .xlxs,
.pptx, dan .pdf. Setelah dilakukan uji coba maka didapatkan hasil aplikasi ini berhasil digunakan. Hasil dari pengujian program yang berekstensi .docx, .xlxs, .pptx, dan .pdf dapat dilihat pada Tabel 1, Tabel 2, Tabel 3 dan Tabel 4.

Tabel 1. Hasil Proses Enkripsi dan Dekripsi .doc

No.	Nama	Ukuran (KB)	Waktu Proses		Ukuran setelah	
			Eknrip	Dekris	Enkri	Dekri
			si	pi	psi	psi
1	Document_1	20	0.342565	0.196639	40	20
2	Document_2	70	0.998578	0.758186	148	70
3	Document_3	134	1.297188	0.978327	332	134
4	Document_4	22	0.454276	0.283749	50	22

Tabel 2. Hasil Proses Enkripsi dan Dekripsi .xlxs

No.	Nama	Ukuran (KB)	Waktu Proses		Ukuran setelah	
			Eknripsi	Dekripsi	Enkripsi	Dekripsi
1	Book_1	24	1.459021	1.185902	53	24
2	Book_2	21	1.13789	0.629173	35	21
3	Book_3	126	2.09361	2.381633	135	126
4	Book_4	15	0.253398	0.134355	24	15

Tabel 3. Hasil Proses Enkripsi dan Dekripsi .pptx

No.	Nama	Ukuran (KB)	Waktu Proses		Ukuran setelah	
			Eknripsi	Dekripsi	Enkripsi	Dekripsi
1	Presentation 1	80	0.784605	1.143535	97	80
2	Presentation 2	278	0.846981	1.383659	312	278
3	Presentation 3	816	0.982649	1.571038	1190	816
4	Presentation 4	82	0.894715	1.156452	99	82

Tabel 4. Hasil Proses Enkripsi dan Dekripsi .pdf

No.	Nama	Ukuran (KB)	Waktu Proses		Ukuran setelah	
			Eknripsi	Dekripsi	Enkripsi	Dekripsi
1	PDF 1	105	1.234356	1.424829	127	105
2	PDF 2	275	1.289471	1.489204	299	275
3	PDF 3	510	1.483037	1.571038	523	510
4	PDF 4	238	1.14373	1.345847	265	238

3.3 Evaluasi Program

Setelah melakukan analisa dan uji coba program pada aplikasi, maka diperoleh beberapa kelebihan dan kekurangan pada aplikasi ini, sebagai berikut.

a. Kelebihan Program

1) *User* (pengguna) dapat melakukan enkripsi *file email* pada isi konten pesan *email* sebelum dikirim.

2) *File* atau data yang sudah di enkripsi tidak dapat dibaca atau dibuka sebelum pengguna melakukan proses dekripsi.
3) Tampilan aplikasi menarik dan mudah digunakan oleh pengguna.
4) Aplikasi dapat digunakan dengan baik dan lancar dengan menggunakan koneksi internet.
5) *Attatchment file* yang terdapat dipesan dapat disimpan dan di dekripsi.
6) Tidak ada perubahan pada isi *file* atau data yang telah di dekripsi.

b. Kekurangan Program

1) Aplikasi membutuhkan waktu yang *relative* lama apabila ukuran data atau *file* terlalu besar.
2) Aplikasi membutuhkan koneksi internet yang stabil.
3) Aplikasi tidak bisa mengirim kebanyak user seperti Cc dan Bcc
4) Dalam aplikasi ini tidak menyediakan fitur *email* terkirim, *draft,* dan lainnya, karena kelemahan dari pengaturan *server webmail* dengan domain yang tersedia dari perusahaan tidak mendukung untuk aplikasi ini, jadi hanya dapat membaca isi dari *email* masuk saja.

4. KESIMPULAN

Beberapa kesimpulan yang didapatkan dari perancangan, pembuatan, serangkaian uji coba program dan hasil analisa pada aplikasi ini, maka dapat diperoleh kesimpulan sebagai berikut.

a. Dengan adanya aplikasi pengamanan *email* ini, penulis berharap permasalahan pengamanan *email* di PT. Pratama Indomitra Konsultan dapat teratasi.
b. Dengan adanya aplikasi pengamanan *email* ini, pertukaran dokumen, data dan informasi yang dimiliki oleh perusahaan dapat terjaga dan terjamin kerahasiaan dan keamanannya.
c. Pengguna yang menggunakan aplikasi kriptografi ini dapat mengenkripsi dan mendekripsi file berekstensi .docx, .xlsx, .pptx, dan .pdf.
d. Ukuran *file* atau data sangat mempengaruhi waktu pada proses pengenkripsian.
e. Ukuran *file* pada saat sebelum di enkripsi atau *plaintext* dengan *file* setelah di enkripsi atau *ciphertext* mengalami perubahan.

Selain kesimpulan, terdapat pula saran untuk pengembangan aplikasi lebih lanjut yang dapat dilakukan, diantaranya sebagai berikut.

a. Dalam pengembangan selanjutnya, dapat menambahkan atau menggunakan metode lain.
b. Menambahkan beberapa fitur tambahan pada aplikasi selanjutnya seperti fitur *draft* dan *email* terkirim.
c. Dalam pengembangan selanjutnya, aplikasi tidak hanya dapat mengenkrip *file* .docx, .xlsx, .pptx, dan .pdf.
d. Dalam pengembangan selanjutnya, aplikasi ini dapat menggunakan metode kompresi lain sehingga ukuran fie yang dienkrip dapat diminimalisir.

5. DAFTAR PUSTAKA

[1] Ariyus, Dony, 2008, Kriptografi Keamanan Data Dan Komunikasi, Yogyakarta: Graha Ilmu.

[2] Anggraini, Y., Sakti, D.V.S.Y,. (2014).Penerapan steganografi metode *end of file* (eof) dan enkripsi metode *data encryption standard* (des) pada aplikasi pengamanan data gambar berbasis java *programming*, KNSI2014-346.

[3] Hendrawati, Hamdani, Awang Harsa K. (2014). Keamanan Data Dengan Menggunakan Algoritma Rivest Code 4 Dan Steganografi Pada Citra Digital. Informatika Mulawamah, 6-12. [4] Yuliansyah, Harry. 2016. Uji Kinerja Pengiriman Data Secara Wireless Menggunakan Modul ESP8266 Berbasis Rest Architecture. Lampung : Jurnal Rekayasa dan Teknologi Elektro Volume 10, No. 2.

[4] Nurcahyo Budi Nugroho, Z. A. (2016). Aplikasi Keamanan Email Menggunakan Algoritma RC4.Saintikom, 81-88.

[5] Widarma, A. (2016). Kombinasi Algoritma AES, RC4 Dan Elgamal Dalam Skema Hybrid Untuk Keamanan Data.

[6] Wasino,Setiawan,Tri uji Rahayu. (2012).Implementasi Steganografi Teknik *End Of File* dengan Enkripsi *Rijndael*, 1-6, SENTIKA 2012.

[7] Zain,R.H (2012). Perancangan Dan Implementasi Cryptography Dengan Metode Algoritma RC4 Pada Type File Document Menggunakan Bahasa Pemograman Visual Basic 6.0. Padang: Universitas Putra Indonesia "YPTK" Padang