# IMPLEMENTASI KRIPTOGRAFI PADA EMAIL MENGGUNAKAN ALGORITMA RIVEST CODE 4 (RC4) DAN DATA ENCRYPTION STANDART (DES) BERBASIS JAVA DESKTOP PADA PT VEPRO NUSA PERSADA

**Arief Rilo Pambudi[1)], Windarto[2)]**
[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : ariefrilopambudi@gmail.com [1)], windarto@budiluhur.ac.id [2)]

**ABSTRAK**

*Bertukar informasi menjadi hal penting dalam kehidupan bermasyarakat untuk berkomunikasi, email adalah salah satu media komunikasi untuk bertukar informasi. Karena kemudahan dalam mengakses, menjadikan media komunikasi tersebut sangat berdampak bagi keamanan untuk mengakses media tersebut. Banyak orang berusaha menemukan cara untuk mengamankan informasi yang melalui media pertukaran informasi. Salah satu caranya adalah dengan menggunakan kriptografi dalam mengamankan data dalam pertukaran informasi Dalam kriptografi, terdapat fungsi enkripsi dan dekripsi yang menjadi kunci keamanan media tersebut. PT Vepro Nusa Persada adalah perusahaan penyedia dan kontraktor elektrik pompa yang banyak komunikasi yang dilakukan melalui email dalam proses kerja samanya. Didalam dokumen yang dikirim melalui email yang merupakan dokumen penting. Pada tugas akhir ini dirancang suatu aplikasi kriptografi yang digabungkan dengan email, dimana penulis mengharapkan aplikasi ini kriptografi yang dapat membantu segala kegiatan pada PT Vepro Nusa Persada. Dalam perancangan aplikasi ini menggunakan metode pengembangan sistem dengan model waterfall. Aplikasi menggunakan algoritma Rivest Code 4 (RC4) dan Data Encryption Standart (DES) dengan bahasa pemrograman java, dimana kunci enkripsi dan dekripsi diatur oleh pengguna, hal ini dilakukan untuk meminimalisir kesalahan dari sistem. Algoritma Rivest Code 4 (RC4) dan Data Encryption Standart (DES) diharapkan mampu memproses enkripsi dan dekripsi data dengan waktu yang lebih cepat dan pengamanan yang lebih aman. Adapaun file yang dapat diproses oleh aplikasi hanya file berekstensi .docx, .xlxs, .pptx, dan .pdf.*

**Kata Kunci:** Algoritma Rivest Code 4(RC4), Algoritma Data Encryption Standart (DES), Enkripsi

## 1. PENDAHULUAN

Dunia teknologi informasi yang berkembang cepat, membuat banyak perubahan dalam berkomunikasi. Dalam kehidupan di era globalisasi ini, banyak hal yang menggunakan teknologi informasi untuk menjalankan aktivitasnya, salah satu perkembangan dalam dunia teknologi informasi adalah perkembangan dari aplikasi perangkat lunak, saat ini banyak aplikasi yang bisa menulis dan mengirimkan *file*, namun kurang dalam segi keamanannya, ketika informasi dituliskan dalam sebuah file dan dikirimkan melalui *email* atau *file* itu hanya sekedar disimpan untuk konsumsi pribadi, *file* tersebut tidak memiliki keamanan apapun, maka diperlukan suatu pengamanan dari isi informasi yang ditulis dengan begitu pertukaran data akan aman biarpun disadap atau dicuri pada saat mengirim dengan email dan informasi aman untuk digunakan secara pribadi.

Tidak sedikit pengguna atau user seperti instansi atau bahkan individu – individu tidak ingin informasi atau data yang dikirimkan diketahui oleh pihak atau orang lain yang tidak mempunyai hak. Begitu pula PT Vepro Nusa Persada yang bergerak di bidang penyedia dan kontraktor elektrik pompa, agar lebih efisien, file – file penting seperti surat penawaran antara *client* dan kantor, faktur pemesanan antara *client* dan kantor, slip gaji karyawan, surat Keputusan kantor yang dikirim kepada karyawan dan surat surat lainnya yang dikirimkan melalui *email* dan itu tidak memiliki keamanan apapun, sehingga diperlukan pengamanan isi pesan *email* dan isi file yang dikirimkan melalui *email*. Untuk menjaga isi pesan *email* dan *file* email dokumen supaya tidak dapat digunakan oleh orang yang tidak berhak.

Maka dari itu, dikembangkan cabang ilmu untuk mempelajari cara mengamankan data atau informasi yaitu kriptografi. Mengamankan informasi dapat dilakukan dengan menggunakan teknik enkripsi terhadap data atau informasi sehingga sulit untuk dibaca atau diterjemahkan

yang dapat disebut juga dengan sebutan kriptografi. Kriptografi bertujuan agar pesan atau informasi yang dikirim tidak dibaca oleh orang yang tidak berhak dan pemalsuan pesan serta dokumen juga dapat dibuktikan, sehingga orang yang mengirim pesan tidak dapat mengelak dari tanggung jawab telah mengirim pesan tersebut. Salah satu caranya adalah dengan menerapkan teknik kriptografi dengan mengenkripsi isi dari file yang akan dikirimkan menggunakan algoritma yaitu RC4 dan DES, teknik enkripsi merupakan seni menyembunyikan pesan dengan merubahnya menjadi tulisan yang tidak bisa dibaca dan memanfaatkan kunci untuk mengembalikan isi informasi file kedalam informasi aslinya dengan menggunakan dua algoritma yaitu RC4 dan DES, algoritma DES yang memiliki kelebihan lebih cepat dalam proses enkrip dan ditambah dengan algoritma RC4 sebagai pengamanan ganda dalam pertukaran data.

## 2. LANDASAN TEORI

### 2.1. Email

*Email* adalah salah satu media untuk bertukar informasi dan hanya bisa digunakan dalam jaringan internet. Diibaratkan *email* adalah sebuah kantor pos yang digunakan untuk mengirimkan surat, namun email digunakan dengan media elektronik.

Selain dapat mengirim pesan dalam bentuk teks, e*mail* dapat mengirim berbagai jenis *file* sepert gambar, video, audio dari suatu perangkat elektronik lainnya. Saat ini pengirim *email* tidak hanya bisa dilakukan dengan menggunakan komputer melainkan banyak perangkat elektornik yang telah memiliki aplikasi pengiriman *email* seperti *tablet, mobile phone, laptop* dan lain sebagainya.[1]

### 2.2. Kriptografi

Kriptografi adalah ilmu yang digunakan untuk mengamankan pesan agar tidak dapat dibaca oleh orang yang tidak berhak. Kriptografi mempunyai sejarah yang sangat panjang, dimulai saat jaman Romawi kuno dan masih dikembangkan hingga saat ini. Dalam kriptografi, terdapat teknik enkripsi dan dekripsi. Teknik enkripsi digunakan untuk mengubah kalimat asli menjadi kalimat yang acak dengan menggunakan kunci sebagai parameternya. Sedangkan teknik dekripsi digunakan untuk mengubah kalimat yang telah terenkripsi menjadi kalimat asli saat sebelum proses enkripsi.

Jadi, pada umumnya kriptografi digunakan untuk menyembunyikan dan mejaga pesan dengan cara diubah menjadi suatu kalimat acak yang tidak bisa dipahami oleh yang tidak berhak. [2]

### 2.3. Algoritma RC4 (*Rivest Code 4*)

Algoritma kriptografi *Rivest Code* 4 (RC4) merupakan salah satu kunci simetris dibuat oleh RSA *Data Security Inc* (RSADSI) yang berbentuk *stream chiper*. Algoritma ini ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu sebagai berikut: *Rivest Shamir Adleman*). RC4 menggunakan panjang kunci dari 1 sampai 256 *byte* yang digunakan untuk menginisialisasikan tabel sepanjang 256 *byte*. Tabel ini digunakan untuk generasi yang berikut dari *pseudo random* yang menggunakan *XOR* dengan *plaintext* untuk menghasilkan *ciphertext*. Masing-masing elemen dalam tabel saling ditukarkan minimal sekali. [2]

Secara garis besar algoritma dari metode RC4 *stream chipper* ini terbagi menjadi dua bagian, yaitu *key setup* atau *key schedulling Algorithm* (PRGA) dan proses XOR dengan *stream* data.[2]

Algoritma RC4 Stream Chiper untuk melakukan enkripsi dekripsi adalah sebagai berikut:

1) Proses *Inisialisasi S-Box* (Array S)

   For I = 0 to 255, S[i] = i
2) Proses *Inisialisasi S-Box* (Array K)
   For I = 0 to 255, S[i] = i
3) Pengacakan S-Box
   I=0; j=0
   For I = 0 to 255 {
   J=(j+S[i]+[K] mod 256)
   Swap S [i] dan S[j]
   }
4) Membuat *Pseudorandom Byte*
   I = (i+1) mod 256
   J = (j+S[i]) mod 256
   Swap S[i] dan S[j]
   T=(S[i] + S[j]) mod 256
   K=S[t]

.

### 2.4. Algoritma DES ( *Data Encryption Standart*)

Algoritma kriptografi *Data Encryption Standart* (DES) merupakan algoritma enkripsi yang paling banyak digunakan di dunia yang diadopsi oleh NIST (*National Institue of Standards and Technology*) sebagai standar pengolah informasi Federal AS dan semua kontraktor dan penyedia jasa untuk pemerintahan Amerika Serikat. DES dirancang oleh IBM yang dipimpin oleh Horst Feitsel dengan bantuan dari NSA (*National Security Agency*). Data *plaintext* dienkripsi dalam blok-blok 64 bit menjadi 64 bit data ciphertext menggunakan kunci 56 bit kunci internal (*internal key*). DES mentransformasikan input 64 bit dalam

beberapa tahap enkripsi ke dalam output 64 bit. Dengan demikian, DES termasuk block cipher. Dengan tahapan dan kunci yang sama, DES digunakan untuk membalik enkripsi. Kunci internal pada algoritma DES dibangkitkan dari kunci eksternal (*external key*) 64 bit [3]

## .ANALISA DAN PERANCANGAN PROGRAM

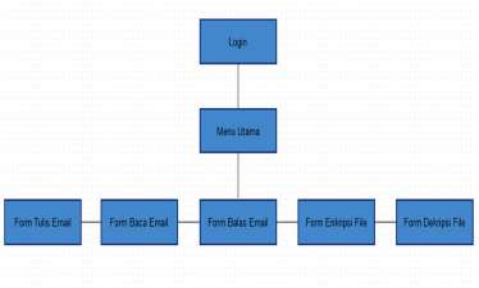
### 3.1. Analisa Masalah

Dalam perkembangan teknologi yang pesat ini dan diimbangi dengan tingkat kriminal dunia maya atau *cybercrime* yang merajalela, hal tersebut membuat akun *email* PT Vepro Nusa Persada rentan terhadap ancaman serangan *hacker* yang melakukan *cybercrime*. Segala data yang memungkinkan bahwa semua isi yang ada di dalam akun *email* tersebut akan terbaca oleh *hacker*, apalagi dalam pesan itu terdapat *file* dan pesan yang bersifat rahasia seperti data perusahaan.

### 3.2. Penyelesaian Masalah

Dari uraian permasalahan yang telah diuraikan diatas, maka dibutuhkannya pengamanan data melalui *email* dengan menerapkan ilmu kriptografi, yakni melakukan enkripsi dan dekripsi dengan suatu metode pada isi pesan *email* dan *file* yang dikirim dengan menggunakan metode algoritma RC4 dan DES yang di implementasikan dalam sebuah aplikasi. Pesan *email* yang akan dirahasiakan adalah isi pesan dan *file email* sehingga apabila akun *email* karyawan PT Vepro Nusa Persada menjadi korban *hacker*, maka sang *hacker* tidak dapat membaca isi dari emailtersebut.

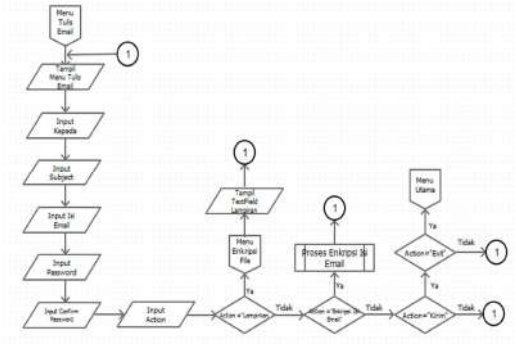
### 3.3. Rancangan Menu




Gambar 1 Rancangan Menu

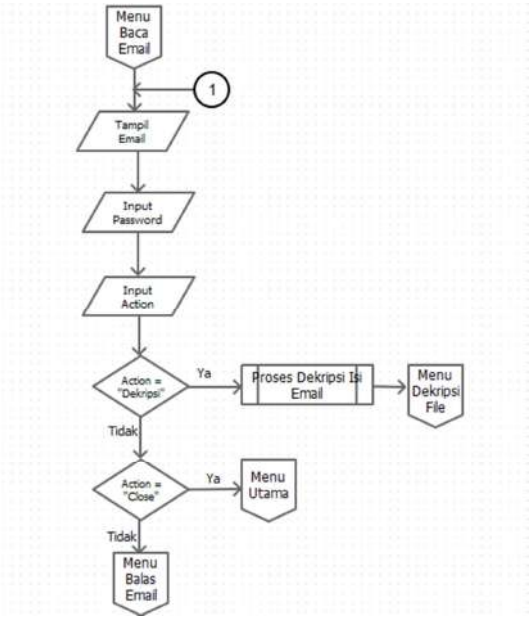
### 3.4. *Flowchart* Program

**a. *Flowchart* Tulis *Email***



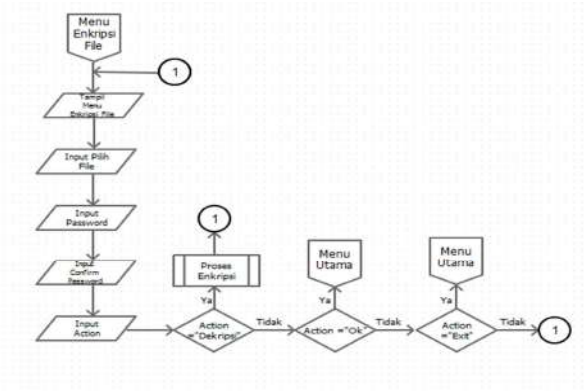

Gambar 2 *Flowchart* Tulis *Email*

**b. *Flowchart* Baca *Email***



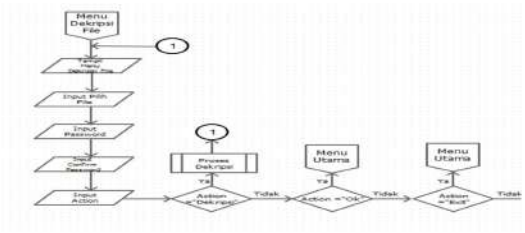

Gambar 3*Flowchart* Baca *Email*

**c. *Flowchart* Enkripsi *File***



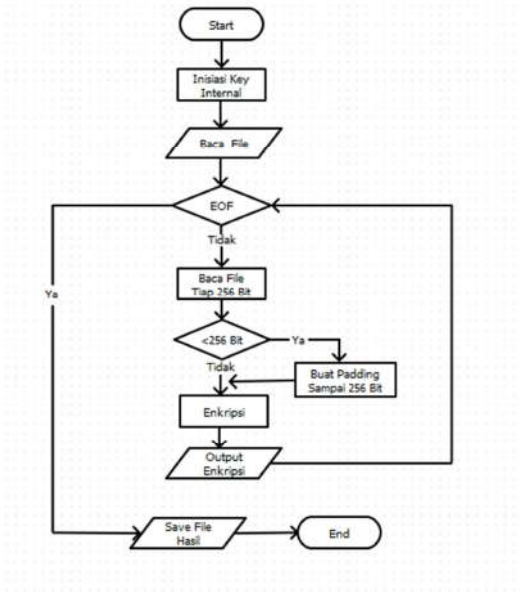

Gambar 4 *Flowchart* Enkripsi *File*

**d. *Flowchart* Dekripsi *File***



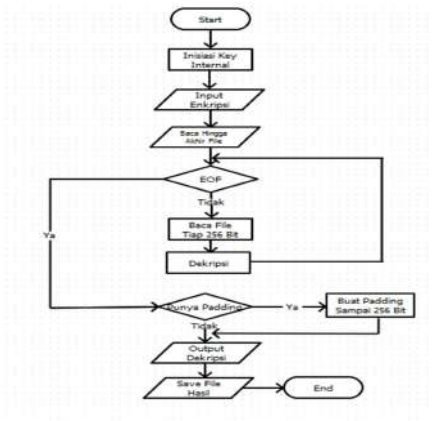
Gambar *5 Flowchart Dekripsi File*

**e. *Flowchart* Proses Enkripsi RC4**



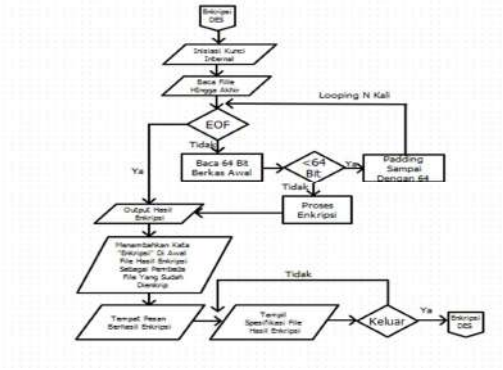

Gambar 6 *Flowchart* Proses Enkripsi RC4

**f. *Flowchart* Proses Dekripsi RC4**



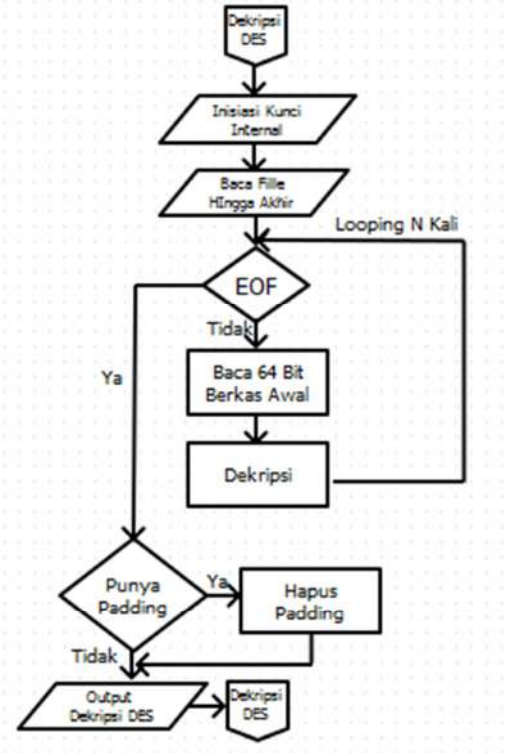
Gambar 7 *Flowchart* Proses Dekripsi RC4

**g. *Flowchart* Proses Enkripsi DES**




Gambar 8 *Flowchart* Proses Enkripsi DES

**h. *Flowchart* Proses Dekripsi DES**




Gambar 9*Flowchart* Proses Dekripsi DES

## 4. IMPLEMENTASI DAN UJI COBA PROGRAM

### 4.1. Pengujian Program

Pengujian program merupakan suatu uji coba yang dilakukan untuk bertujuan menentukan apakah aplikasi berjalan dengan baik atau tidak. Langkah dalam pengujian aplikasi kriptografi email sebagai berikut :

a. FormTulis Email
*Form* ini tampil ketika pengguna klik tombol "Tulis Email" yang terdapat pada menu utama. *Form* ini digunakan untuk mengirim pesan baru kepada pengguna *email* lainnya. Dengan mengisi *email* penerima, *subject*. Seperti gambar dibawah ini.

Gambar 10 *Form* Tulis *Email*

b. Form Baca Email
Pada tampilan ini berfungsi untuk membaca *email* masuk. *Form* baca *email* masuk dan *email* keluar akan tampil bila pengguna "klik" salah satu pesan *email* yang terdapat pada *list email* masuk atau *list email* terkirim. Pada *form* ini pengguna juga dapat membalas *email.* Terlihat seperti gambar berikut.

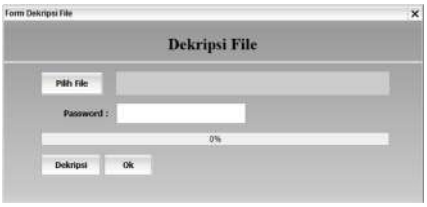
Gambar 11 *Form* Baca *Email*

c. Form Enkripsi *Email*

*Form* enkripsi *file email* ini akan tampil ketika pengguna klik pada menu enkripsi dan *submenu* enkripsi *file email*. Fungsi pada *form* ini adalah untuk mengenkripsi isi *file email*. Seperti gambar dibawah ini.


Gambar 12 *Form* Dekripsi *File*

d. Form Dekripsi File
Form ini tampil ketika pengguna membaca *email* masuk, dan terdapat lampiran yang terenkripsi. Untuk membaca nya harus di dekripsi terlebih dahulu. Seperti gambar dibawah ini.




Gambar 13 *Form* Dekripsi *File*

**4.2. Tabel Pengujian**

Pengujian program merupakan salah satu hal yang perlu dilakukan dalam pembuatan perangkat lunak (*software*) untuk mengetahui hasil yang telah dicapai oleh aplikasi yang telah dibuat dalam penelitian. Pada penelitian ini penulis melakukan pengujian enkripsi dekripsi *file* document yang berekstensi *docx*, *xlsx*, *pptx*, dan *pdf*. Pengujian tersebut akan mendapatkan hasil perbandingan *file* asli yang telah dienkripsi. Berikut adalah tabel uji coba proses enkripsi dan dekripsi file document *docx*, *xlsx*, *pptx*, dan *pdf* dengan menggunakan metode algoritma RC4 (*Rivest Code* 4) dan DES (Data Encryption Standart).

Tabel 1Hasil Pengujian .docx

| No. | Nama | Ukuran File (KB) | Waktu Proses (MiliSecond) | | Ukuran File Setelah (KB) | |
|---|---|---|---|---|---|---|
| | | | Enkripsi | Dekripsi | Enkripsi | Dekripsi |
| 1 | Document_1 | 234 | 1.179881 | 0.878217 | 467 | 234 |
| 2 | Document_2 | 21.926 | 6.456108 | 2.864384 | 43.850 | 21.926 |
| 3 | Document_3 | 64 | 0.796765 | 0.728176 | 127 | 64 |
| 4 | Document_4 | 16 | 0.245256 | 0.183629 | 31 | 16 |

Tabel 2 Hasil Pengujian .xlsx

| No | Nama | Ukuran File (KB) | Waktu Proses (MiliSecond) | | Ukuran File Setelah (KB) | |
|---|---|---|---|---|---|---|
| | | | Enkripsi | Dekripsi | Enkripsi | Dekripsi |
| 1 | Book_1 | 15 | 0.253366 | 0.134355 | 24 | 15 |
| 2 | Book_2 | 24 | 1.35902 | 1.18590 | 53 | 24 |
| 3 | Book_3 | 21 | 1.136790 | 0.629163 | 35 | 21 |
| 4 | Book_4 | 126 | 2.083610 | 2.381630 | 135 | 126 |

Tabel 3 Hasil Pengujian .pptx

| No | Nama | Ukuran File (KB) | Waktu Proses (MiliSecond) | | Ukuran File Setelah (KB) | |
|---|---|---|---|---|---|---|
| | | | Enkripsi | Dekripsi | Enkripsi | Dekripsi |
| 1 | Presentation_1 | 80 | 0.784505 | 1.143532 | 97 | 80 |
| 2 | Presentation_2 | 268 | 0.84698 | 1.373649 | 312 | 268 |
| 3 | Presentation_3 | 817 | 0.982639 | 1.561038 | 1190 | 817 |
| 4 | Presentation_4 | 1188 | 2.382520 | 2.962961 | 2389 | 1188 |

Tabel 4 Hasil Pengujian .pdf

| No | Nama | Ukuran File (KB) | Waktu Proses (MiliSecond) | | Ukuran File Setelah (KB) | |
|---|---|---|---|---|---|---|
| | | | Enkripsi | Dekripsi | Enkripsi | Dekripsi |
| 1 | PDF_1 | 105 | 1.234382 | 1.424829 | 127 | 105 |
| 2 | PDF_2 | 275 | 1.289461 | 1.489204 | 299 | 275 |
| 3 | PDF_3 | 510 | 1.483026 | 1.527493 | 523 | 510 |
| 4 | PDF_4 | 238 | 1.143729 | 1.386347 | 265 | 238 |

**4.3. Evaluasi Program**

Setelah dilakukan pengujian program, maka dapat dianalisa dan ditentukan kelebihan dan kekurangan program, yaitu sebagai berikut :

**Kelebihan Aplikasi:**

a. Adanya fitur simpan mode offline, sebuah fitur bahwa aplikasi dapat digunakan dengan baik tanpa harus menggunakan koneksi *internet* pada saat membaca email yang sudah masuk, dan melakukan proses enkripsi serta dekripsi pada file sisipan di email tersebut.
b. Pengguna dapat mengenkripsi isi *file email* isi konten pesan *email* sebelum dikirim
c. *File* yang sudah dienkripsi tidak bisa dibaca atau dibuka sebelum dilakukan dekripsi
d. Isi *file* dari hasil dekripsi tidak mengalami perubahan.
e. Sisipan file yang ada dipesan bisa langsung disimpan dan bisa langsung didekripsi.

**Kekurangan Aplikasi:**

a. Semakin besar ukuran *file* yang akan dienkripsi dan didekripsi, maka semakin lama waktu proses yang dibutuhkan.
b. Aplikasi hanya dapat mengenkripsi *file* yang berekstensi *.docx, .xlsx, .pptx*, dan *.pdf* saja.
c. Aplikasi hanya bisa melampirkan *file* berekstensi *.docx, .xlsx, .pptx,* dan *.pdf*.
d. *File* hasil enkripsi berubah ukurannya menjadi lebih besar dibandingkan *file* aslinya.
e. Tidak adanya fitur teruskan *email*.
f. Tidak bisa mengirim *email* ke banyak penerima.

## 5. PENUTUP

Berdasarkan penelitian yang telah dilakukan terhadap permasalahan dari aplikasi yang telah dibuat,bisa di tarik kesimpulan dan saran yang dapat dijadikan panutan untuk pengembangan aplikasi.

**5.1. Kesimpulan**

Adapun kesimpulan yang dapat diperoleh dari perancangan, pembuatan, uji coba dan analisa aplikasi ini, maka dapat dibuat beberapa kesimpulan sebagai berikut:

a. Dengan adanya aplikasi ini, informasi atau data penting yang dimiliki oleh karyawan perusahaan dapat terjamin keamanan dan kerahasiaannya.
b. Karyawan perusahaan yang menggunakan aplikasi kriptografi ini dapat mengenkripsi dan mendekripsi *file* berekstensi *.docx, .xlsx, .pptx,* dan *.pdf.*
c. Ukuran *file* pada saat sebelum dienkripsi atau *plaintext* dengan *file* setelah dienkripsi atau *ciphertext* mengalami perubahan.
d. Ukuran *file* sangat mempengaruhi waktu pengenkripsian.

**5.2. Saran**

Beberapa saran yang diberikan untuk pengembangan aplikasi lebih lanjut dengan beberapa perkembangan lagi yang harus dilakukan, diantaranya sebagai berikut:

a. Menambahkan metode kompresi sehingga ukuran *file* yang dienkripsi dapat diminimalisir
b. Agar dapat mengenkripsi *file* selain tipe *.docx, .xlsx, .pptx, dan .pdf.*
c. Menambahkan beberapa fitur seperti *draft* dan proses dalam mengekripsi.
d. Menambahkan fitur teruskan *email*
e. Menambah fitur agar bisa mengirim *email* ke banyak penerima.

## DAFTAR PUSTAKA


[1] Nurcahyo Budi Nugroho, Z. A. (2016). Aplikasi Keamanan Email Menggunakan Algoritma RC4. SAINTIKOM Vol 15, No 3, 81-88.

[2] Ariyus, Donny 2008, Kriptografi Keamanan Data Dan Komunikasi, Yogyakarta: Graha Ilmu.

[3] Primartha, Rifkie. (2011) .Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma DES. Jurnal Sistem Informasi (JSI) Vol 3, No 2, 371-387.

[4] Hendrawati, Hamdani, Awang Harsa K. (2014). Keamanan Data Dengan Menggunakan Algoritma Rivest Code 4 Dan Steganografi Pada Citra Digital. Informatika Mulawarman Vol 9, No 1, 6-12.

[5] Nurcahyo Budi Nugroho, Z. A. (2016). Aplikasi Keamanan Email Menggunakan Algoritma RC4. SAINTIKOM Vol 15, No 3, 81-88.

[6] Hasugian, A. H. (2017). Implementasi Algoritma Hill Cipher, Pelita Informatika Budi Darma, Volume :IV

[7] Budiawan, I.G.A. (2008) .Aplikasi Pengamanan Data Menggunakan Algoritma RC4,Jurnal Telematika Vol 1, No 2.


.