# APLIKASI MENGAMANKAN EMAIL DENGAN MENGGUNAKAN METODE ALGORITMA KRIPTOGRAFI RC6 PADA PERCETAKAN LIBRADO

**Seh Anang Maulana[1)], Titin Fatimah[2)]**
[1,2]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : sehanangmaulana@gmail.com[1)], titin.fatimah@budiluhur.ac.id[2)]

## ABSTRAK

*Email merupakan salah satu sarana komunikasi yang digunakan saat ini. Dengan email orang bisa bertukar informasi dengan orang lain selama terhubung dengan jaringan internet. . Email tidak pernah menjamin kerahasiaan dari pesan yang dikirim oleh penggunanya. Karena teks pesan yang dikirim adalah pesan rahasia dan pribadi, sehingga kerahasiaan pesan menjadi sangat penting. Salah satu caranya adalah dengan menggabungkan sebuah aplikasi email dan juga menggunakan kriptografi yang menggunakan algoritma kunci simetris, dimana kunci enkripsi dan dekripsi tersebut sama namun jika kunci dekripsi dikirimkan secara terpisah hal ini memungkinkan kunci dapat diketahui oleh penyadap. Pada aplikasi ini menggunakan metode RC6 (Rivest Code 6) bagian dari algoritma simetris, dimana proses enkripsi dan dekripsinya memiliki kunci (key) yang sama.Penelitian ini menghasilkan Aplikasi mengamankan email dengan menggunakan metode Algoritma Kriptografi RC6 pada Percetakan Librano. Aplikasi ini dibuat dengan bahasa pemrograman Java. Aplikasi ini memiliki fitur melihat semua pesan masuk dan pesan keluar, aplikasi juga dapat membaca pesan masuk dan langsung membalas pesan tersebut. Dalam pesan masuk ataupun pesan keluar terdapat file yang dilampirkan, file tersebut dapat user simpan ke dalam direktori komputer yang user tentukan. Dengan menggunakan aplikasi ini, pengguna akan dapat mengirimkan pesan dan data yang sifatnya rahasia tanpa takut akan ada orang yang tidak berhak menerima email yang dapat membaca isi pesan dan data tersebut.*

**Kata Kunci :** *Email*, Kriptografi, Kunci Simetris, Enkripsi, Dekripsi, RC6,

## 1. PENDAHULUAN

### 1.1. Latar Belakang

Perkembangan teknologi informasi berkembang pesat saat ini, bukan hanya di negara maju, di negara berkembang. Hampir semua hal dapat disajikan dalam bentuk digital atau terkomputerisasi.

Dimana saat ini hampir semua perusahaan telah melakukan transaksi via *email* yang bersifat pribadi, namun hal ini tidak menutup kemungkinan terjadinya peretasan *email* transaksi terebut. Karena transaksi adalah sebuah alur bisnis yang sangat penting bagi sebuah prusahaan dimana kelancaran perkembangan perusahaan terletak di sana. Memang sebuah akun pribadi yang disuport oleh beberapa vendor yang memiliki keamanan tersendiri dalam *email* itu, namun ini tidak bisa menjadi patokan sendiri karena masih bisa dibobol dengan beberapa cara yang sudah banyak ditemukan celahnya. Maka lebih baik menggandakan keamanan tersebut dengan keamanan yang bisa kita tahu kemanaan *email* tersebut. Contohnya saja pada Percetakan Librado yang bergerak di bidang percetakan ini melakukan transaksi melalui *email*. Pada Percetakan Librado ini pernah terjadi sebuah kecerobohan saat melakukan pengiriman berkas transaksi dengan memasukan alamat *email* tujuan yang salah dan fatalnya *email* salah yang dikirim itu adalah *email* aktif seseorang, jika orang tersebut menyebarkan berkas hal yang menjadi alasan sebuah masalah pada percetakan tersebut. Inilah mengapa dibutuhkannya pengamanan dalam aktifitas bisnis melalui *email* tersebut yang hanya bisa diketahui oleh orang–orang yang terkait.

### 1.2. Permasalahan

Permasalahan yang akan dijelaskan yaitu sebagai berikut :

a. Bagaimana mengamankan data dan pesan yang akan dikirim dengan kriptografi RC6.
b. Bagaimana cara mengembalikan data dan pesan yang sudah dienkripsi menjadi data yang asli tanpa mengalami perubahan sedikitpun.
c. Bagaimana membuat aplikasi pengaman isi pesan *e-mail* dengan melampirkan *file* yang mudah digunakan oleh *user*.

### 1.3. Tujuan Penelitian

**a. Tujuan Penelitian**

Tujuan yang akan dibahas dalam penelitian ini adalah:

1. Dapat mengimplementasikan kriptografi untuk melindungi *file* dan pesan dengan menggunakan algoritma kriptografi RC6 pada Percetakan Librado.
2. Menghasilkan aplikasi pengamanan *email* berbasis *desktop* yang mudah digunakan oleh *user* pada Percetakan Librado.
3. Dapat mengembalikan *file* dan pesan seperti semula ketika dikirim dengan menggunakan algoritma kriptografi RC6.

### 1.4. Batasan Masalah

Agar penelitian ini lebih terarah dan tidak meluasnya pembahasan akan diberikan beberapa batasan masalah yaitu :

a. Algoritma yang akan digunakan untuk mengamankan data adalah algoritma RC6.
b. Bahasa pemrograman yang digunakan yaitu Java dan berbasis *desktop*.
c. Pada tipe *file* yang digunakan ini adalah *file* dengan ekstensi: **.doc, *.docx, *.pdf, *.xls,* dan **.xlsx.*

## 2. LANDASAN TEORI

### 2.1. Kriptografi

Kriptografi ini hanya bersangkutan dengan sebuah kepercayaan pesan. Dengan mengubah suatu pesan menjadi biasa yang dapat dimengerti dan menjadi pesan yang tidak dapat dimengerti, lalu mengubahnya kembali menjadi suatu pesan yang dapat dimengerti.[1] Ini bisa memungkinkan pesan menjadi lebih aman dari orang yang tidak dikenal untuk melihat pesan tersebut. Algoritma yang dipakai untuk mengenkripsi dan mendekripsi data menjadi sebuah *plaintext* dan melibatkan penggunaan menjadi suatu bentuk kunci. Pesan *plaintext* yang telah dienkripsi (atau dikodekan) dikenal sebagai *ciphertext* (teks sandi)**.[2]**

Dalam penulisan sebuah metode kriptografi ini, digunakan sebuah bahasa matematika. Pengertian umum enkripsi adalah merubah suatu pesan asli (plaintext) menjadi sebuah pesan tersandikan (ciphertext).

### 2.2. RC6

Metode RC6 dibangun untuk menitikutamakan agar memenuhi sebuah syarat AES yang akan digunakan adalah kemampuan yang akan untuk beroperasi pada sebuah metode blok 128 bit. Pada RC6 ini menggunakan 4 *register* dan 32 *bit*. Oleh karena itu maka akan mendapatkan 2 operasi rotasi pada setiap *half-round* yang digunakan dan juga akan memberikan lebih banyak *bit* yang akan digunakan dan ini akan mempengaruhi banyaknya suatu *bit* yang melakukan sebuah rotasi. Algoritma RC6 adalah versi yang telah dilengkapi dengan beberapa parameter yang ada, sehingga akan dituliskan sebagai RC6-w/r/b, yang dimana parameter w merupakan ukuran sebuah kata dalam satuan *bit*, r adalah suatu bilangan bulat dan bukan negatif yang akan menunjukan banyaknya sebuah iterasi yang selama proses enkripsi, dan b menunjukan ukuran kunci enkripsi dalam sebuah *byte* tertentu**.[3]**

## 3. PERANCANGAN SISTEM DAN APLIKASI

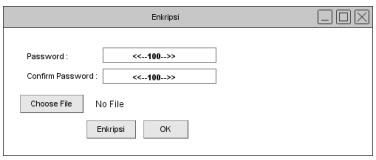
### 3.1. Rancangan Program

Program yang akan dibuat terdiri dari sepuluh buah *form*, yaitu terdiri dari *Form Login*, *Form ReadMe*, *Form* Utama, Baca *E-mail*, Balas *E-mail*, Enkripsi *File*, Dekripsi *File*, Enkrip *Text*, Dekrip *Text* dan *Compose*. Untuk melakukan enkripsi *file*, *user* dapat memilih Menu Enkripsi *file*. Pada menu tampilan ini, *user* harus memilih sebuah *file* dokumen terlebih dahulu lalu password diisi, baru kemudian sistem melakukan proses enkripsi. Selanjutnya akan tampil output berupa informasi hasil enkripsi *file* tersebut, informasi berupa nama file yang berubah dan waktu proses enkripsi. Sedangkan untuk mengembalikan *file* yang sudah dienkripsi menjadi *file* asli, *user* juga dapat memilih menu dekripsi *file*.

### 3.2. Rancangan Layar

**1. Rancangan Layar *Form* Enkripsi *File***

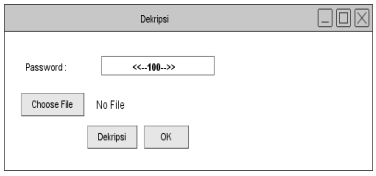
*Form* ini digunakan untuk mengenkripsi *file* sebelum dikirim. Dengan cara melampirkan *file* yang akan dienkripsi. Lalu masukkan *password*. Maka aplikasi akan melakukan proses pengacakan *file* dengan *password*. Seperti gambar 1 berikut ini:




*Gambar 1: Rancangan Layar From Enkripsi File*

**2. Rancangan Layar *Form* Dekripsi *File***

*Form* ini digunakan untuk mengdekripsi *file* yang sudah dienkripsi**.** Dengan cara memilih *file* hasil enkripsi dan memasukkan *password* yang sesuai pada saat mengenkripsinya. Lalu aplikasi akan menjalankan proses dekripsi *file*. Seperti gambar 2 berikut ini:




*Gambar 2: Rancangan Layar Form Dekripsi File*

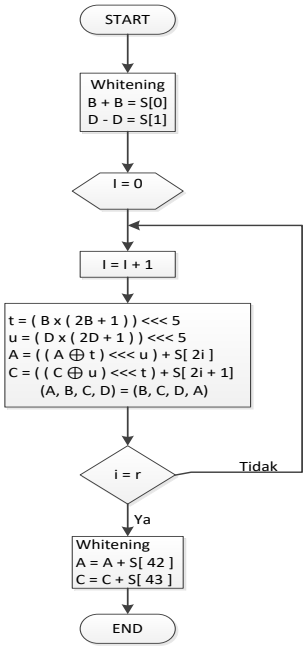
**3.3. Flowchart dan Algoritma Program**

Di dalam menggambarkan urutan proses pada aplikasi ini, memperjelas aliran proses *flowchart*, serta sebuah algoritma untuk mempermudah dalam suatu pembuatan perancangan pada program ini, *flowchart* dan algoritma di bawah ini akan menjabarkan sebuah cara kerja pada program untuk menjalankan sebuah proses dalam program. Di bawah ini akan digambarkan *flowchart* dan algoritma masing-masing prosesnya.

**a. *Flowchart* dan Algoritma enkripsi RC6**

**1) *Flowchart* Algoritma enkripsi RC6**

Berikut adalah flowchart dari algoritma enkripsi RC6:




*Gambar 3: Flowchart Algoritma Enkripsi*

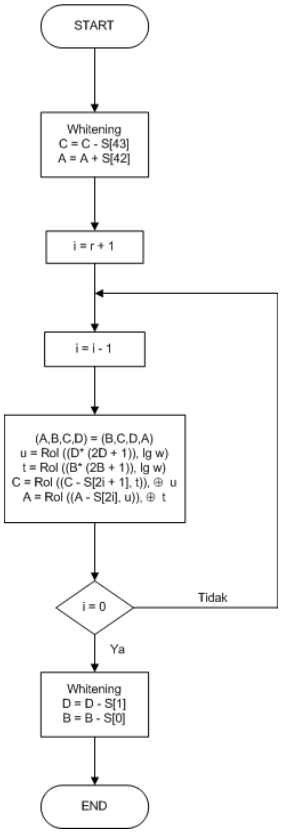
**2) RC6 Algoritma enkripsi RC6**

| | |
|---|---|
| 1. | Start |
| 2. | Input kunci |
| 3. | Inisialisasi kunci |
| 4. | S[0] = Pw |
| 5. | I = 1, 2r+3 |
| 6. | S[i] = S[i1] |
| 7. | Input berkas |
| 8. | Enkripsi |
| 9. | Whitening awal |
| 10. | B = B + S[0] |
| 11. | D = D + S[1] |
| 12. | Transformasi |
| 13. | t = (Bx(2B+1)) <<< 5 |
| 14. | u = (Dx(2D+1)) <<< 5 |
| 15. | Mixing |
| 16. | A = ((A XOR t) <<< u ) + S[2i] |
| 17. | C = ((C XOR u) <<< t ) + S[2i+1] |
| 18. | Swap register |
| 19. | (A,B,C,D) = (B,C,D,A) |
| 20. | Whitening akhir |
| 21. | A = A + S[2r+2] |
| 22. | C = C + S[2r+3] |
| 23. | Output berkas cipher RC6 |
| 24. | Return |

**b. *Flowchart* dan Algoritma Dekripsi RC6**

**1) *Flowchart* Algoritma dekripsi RC6**

Berikut adalah flowchart dari algoritma dekripsi RC6:




*Gambar 4: Flowchart Algoritma Dekripsi RC6*

**2) Algoritma dekripsi RC6**

| | |
|---|---|
| 1. | Start |
| 2. | Input berkas cipher RC6 |
| 3. | Inisialisasi kunci |
| 4. | Dekripsi |
| 5. | Whitening akhir |
| 6. | C = C – S[2r+3] |
| 7. | A = A – S[2r+2] |
| 8. | Swap register |
| 9. | (A,B,C,D) = (D,A,B,C) |
| 10. | Transformasi |
| 11. | u = (Dx(2D + 1)) <<< 5 |
| 12. | t = (Bx(2B + 1)) <<< 5 |
| 13. | Mixing |
| 14. | C = ((C – S[2i+1]) >>> t) XOR u |
| 15. | A = ((A – S[2i]) >>> u) XOR t |
| 16. | Whitening awal |
| 17. | D = D – S[1] |
| 18. | B = B – S[0] |
| 19. | Output berkas cipher RC6 |
| 20. | Return |

## 4. HASIL DAN PEMBAHASAN

Adalah kebutuhan yang akan dibutuhkan dalam memenuhi sebuah kebutuhan spesifikasi. Pengaplikasian program aplikasi ini agar dapat bisa berjalan dengan baik dan lancar. Implementasi aplikasi ini terdiri dari dua bagian saja, yaitu kebutuhan dalam perangkat keras dan kebutuhan dalam perangkat lunak.

### a. Kebutuhan Dalam Perangkat Keras

Berikut ini merupakan spesifikasi perangkat keras untuk komputer yang akan digunakan ditunjukan pada tabel 1.

Tabel 4:1 Perangkat Keras

| No | Perangkat | Kebutuhan |
|---|---|---|
| 1 | CPU | Intel® Core™ i5-6300U CPU @2.40GHz 2.50GHz |
| 2 | Hard Disk | 500 GB |
| 3 | RAM | 4.00 GB |
| 4 | Monitor | 14.0" |
| 5 | Keyboard | Internal Keyboard Laptop |

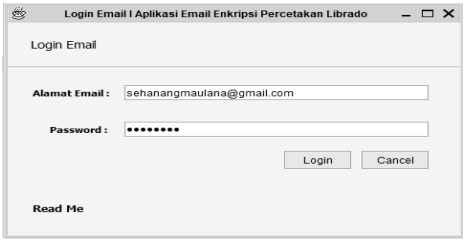
### b. Kebutuhan Perangkat Lunak

Implementasi perangkat lunak merupakan proses instalasi perangkat lunak yang dapat digunakan aplikasi agar beroperasi dengan benar, dalam aplikasi ini perangkat lunak sistem operasi yang digunakan adalah Windows 10.

### 4.1. Interface Aplikasi

### a. Form Login

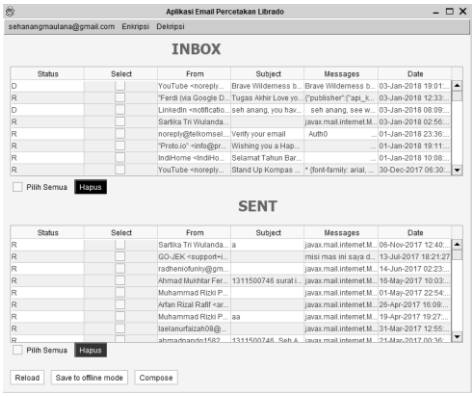
Untuk dapat mengakses menu utama aplikasi maka harus *login* melalui *form login* yang telah disediakan. *User* meng-*input email* dan *password* yang digunakan untuk *login*. Bisa dilihat pada sebuah gambar 5.




*Gambar 5 : Form Login*

### b. Form Menu Utama

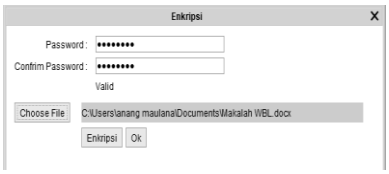
Pada tampilan *form* menu utama aplikasi *email*, *user* dapat melihat pesan masuk yang tampil di *form* ini. Berikut ini adalah tampilan layar *form* menu utama aplikasi *email* pada gambar 6.




*Gambar 6: Tampilan Layar Form Menu Utama Aplikasi Email*

### c. Form Enkripsi File

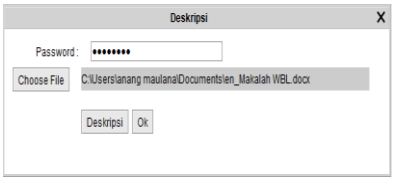
Sebelum *user* masuk ke *form* enkripsi *file*, *user* memilih menu "Enkripsi" yang terdapat submenu "Enkripsi *File*". *Form* enkripsi *file* mempunyai fitur untuk meng*input password* dan *confirm password*, dan *choose file*. Pertama *user* harus meng*input password*, *confirm password*, dan memilih *file* dalam direktori komputer. Bisa dilihat pada gambar 7.




*Gambar 7: Form Enkripsi File*

**d. Form Dekripsi File**

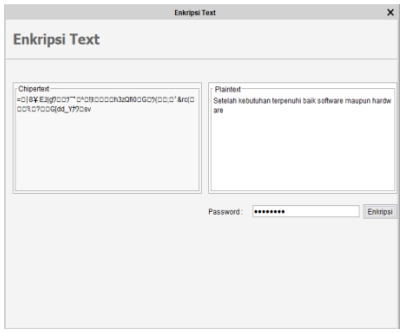
Sebelum *user* masuk ke *form* enkripsi *file*, *user* memilih menu "Dekripsi" yang terdapat submenu "Dekripsi *File*". *Form* dekripsi *file* mempunyai fitur untuk menginput *password* dan *choose file*. Pertama *user* harus meng*input password*. Bisa dilihat pada gambar 8 di bawah ini:




*Gambar 8: Form Dekripsi File*

**e. Form Enkripsi Text**

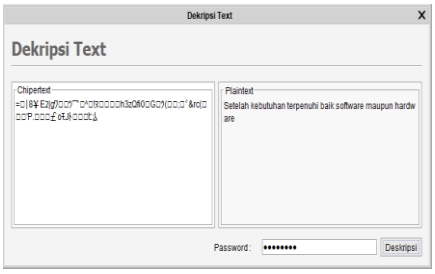
Sebelum *user* menulis ke *form* enkripsi *text*, *user* memilih menu "Enkripsi" yang terdapat submenu "Enkripsi *Text*". *Form* enkripsi *text* mempunyai fitur untuk menulis text serta menambahkan *password* untuk mengenkrip text tersebut dan bisa dijalankan proses enkripsi dengan menekan tombol "Enkrip". Bisa dilihat pada gambar 9 di bawah ini :




*Gambar 9: Tampilan Form Enkripsi Text*

**f. Form Dekripsi Text**

Sebelum *user* masuk ke *form* dekripsi *text*, *user* memilih menu "Dekripsi" yang terdapat submenu "Dekripsi *text*". *Form* dekripsi *text* mempunyai fitur untuk menginput text yang sudah dienkripsi serta menambahkan *password* untuk mendekripsi text tersebut dan bisa dijalankan proses dekripsi dengan menekan tombol "Dekripsi". Bisa dilihat pada gambar 10 di bawah ini :




*Gambar 10: Tampilan Form Dekripsi Text*

## 5. KESIMPULAN

Berdasarkan hasil analisa yang dilakukan terhadap permasalahan dari aplikasi yang telah dikembangkan, maka bisa ditarik menjadi dalam sebuah kesimpulan, sebagai berikut:

a. Dengan adanya sebuah aplikasi kriptografi ini menggunakan sebuah metode *Rivest Code 6* (RC6) ini dapat mengamankan dokumen penting atau sebuah informasi yang ada tempat di Percetakan Librado supaya dapat lebih aman kerahasiaan dan juga mencegah manipulasi data dokumen atau informasi dari orang yang tidak dikenal.
b. Aplikasi ini tidak akan dapat bisa dijalankan dalam keadaan *offline* atau tidak ada koneksi Internet.

## DAFTAR PUSTAKA

[1] Ariyus, D. 2006. Kriptografi Keamanan Data dan Komunikasi. Yogyakarta: Graha Ilmu.

[2] Ariyus, D. 2008. Pengantar Ilmu Kriptografi Teori, Analisis, & Implementasi. Yogyakarta: C.V Andi OFFSET.

[3] Zulham, M., Kurniawan, H. & Rahmad, I.F., 2014. Perancangan Aplikasi Keamanan Data Email Menggunakan Algoritma Enkripsi RC6. Seminar Nasional Informatika, pp.96–101.