

# IMPLEMENTASI PENGAMANAN DATA ARSITEKTUR MENGUNAKAN METODE KRIPTOGRAFI DENGAN ALGORITMA RIVEST CODE 4(RC4) PADA PT. NAVIRI INDAH CEMERLANG

Ricky Rivaldi<sup>1)</sup>, Subandi<sup>2)</sup>

Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur  
Jl.Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260  
Email : [Ricky.aseleole@gmail.com](mailto:Ricky.aseleole@gmail.com), [Subandionline@gmail.com](mailto:Subandionline@gmail.com)

## Abstrak

Keamanan dan kerahasiaan data merupakan aspek yang sangat penting dalam dunia informasi saat ini. Terlebih jika data yang disimpan berisi informasi penting dan rahasia, dimana pihak luar tidak diperbolehkan untuk mengetahuinya. Namun di era teknologi informasi dan komunikasi yang semakin maju, semakin marak pula terjadinya pencurian data. Di PT. NAVIRI INDAH CEMERLANG tentu saja terdapat berbagai macam data berupa file yang berisi informasi penting dan rahasia, untuk itu perlu adanya pengamanan agar tidak terjadi pencurian data oleh pihak yang tidak bertanggung jawab. Dengan adanya pencurian data maka aspek keamanan dalam penyimpanan data menjadi sangat penting, karena data yang disimpan dalam keadaan asli (*plain*) sangat rentan terhadap pencurian data sehingga informasi yang ada didalamnya dapat bocor. Untuk mengatasi masalah diatas maka diperlukan suatu cara untuk mengamankan data. Dengan cara mengimplementasikan suatu metode yang dapat menjaga kerahasiaan informasi, menggunakan Metode kriptografi dengan algoritma Rivest Code 4 (RC4). Algoritma RC4 merupakan bagian dari algoritma simetris yaitu algoritma kriptografi yang mempunyai kunci (*key*). Disamping dari masalah keamanan file, masalah kecepatan dalam memproses enkripsi dan dekripsi juga harus diperhatikan, dalam membangun aplikasi kriptografi ini, penulis menggunakan Bahasa pemrograman Java. Aplikasi yang dibuat dapat memberikan keamanan lebih terhadap *file* pada PT.NAVIRI INDAH CEMERLANG sehingga kerahasiaannya terjaga.

**Kata kunci:** Kriptografi, RC4, Enkrip, Dekrip

## 1. PENDAHULUAN

Teknologi Informasi saat ini telah memberikan kemudahan didalam melakukan aktivitas manusia, perkembangannya pun sudah sedemikian pesat.Maka dari itu tidak menutup kemungkinan seseorang dituntut agar dapat memiliki dan mengikuti perkembangan teknologi.Perkembangan Teknologi Informasi ini tentunya memiliki dampak yang besar , baik itu positif maupun negatif.

PT. NAVIRI INDAH CEMERLANG mengalami kendala terhadap pengamanan data dan setelah tim melakukan analisa bahwa ada pihak yang tidak bertanggung jawab atas data tersebut,dan dapat mengakibatkan kerusakan di perusahaan tersebut. *Kriptografi* merupakan matematika yang mempunyai hubungan persamaan dengan aspek keamanan informasi seperti integrasi data, keaslian entitas, dan keaslian data. Berbagai macam teknik dan upaya yang digunakan *Kriptografi* untuk mengamankan data. Data

tersebut harus tetap rahasia selama penyimpanan. Untuk memenuhi hal tersebut, dilakukan proses penyandian (*encryption and decryption*) terhadap data yang akan disimpan.

*Enkripsi* dilakukan pada saat penyimpanan dengan cara mengubah data asli menjadi data rahasia data asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Data asli hanya bisa dilihat oleh pemilik dengan menggunakan kunci rahasia.

Tujuan dan maksud dari penelitian ini adalah bertujuan untuk membuat sebuah aplikasi pengamanan untuk mengamankan data yang penting, agar tidak terjadi lagi pencurian data pada PT. NAVIRI INDAH CEMERLANG oleh orang yang tidak bertanggung jawab, untuk itu dalam penelitian ini penulis Membuat pengamanan data aplikasi menggunakan algoritma *Rivest Code 4* (RC4) dan Mencegah terjadinya penyalahgunaan informasi yang terdapat pada dokumen.

Supaya penelitian ini lebih jelas dan tidak meluas nya pembahasan, maka penulis akan memberikan beberapa batasan masalah yaitu:

- a. Algoritma yang digunakan yaitu algoritma *Rivest Code 4 (RC4)*,
- b. Bahasa pemrograman yang digunakan untuk membuat aplikasi adalah bahasa pemrograman Java,
- c. Aplikasi ini hanya bisa mengenkripsi dan mendekripsi *file* yang berformat.pdf.

Dalam pembuatan aplikasi pengamanan data ini penulis menggunakan metode RC4, agar mempermudah si penulis dalam melakukan proses penelitian.

Penelitian ini memperoleh data dan informasi dengan cara mengumpulkan, mempelajari, dan membaca berbagai macam referensi baik itu dari jurnal, makalah, buku, artikel, dan berbagai macam sumber lainnya. Penelitian ini analisis data menggunakan algoritma Rivest Code 4 (RC4).

Membuat aplikasi pengamanan data dengan implementasi algoritma Rivest Code 4 (RC4) menggunakan bahasa pemrograman Java. Menguji aplikasi yang sudah dibuat dengan melakukan beberapa uji coba yang bertujuan untuk mengetahui kekurangan pada aplikasi sampai aplikasi tersebut berjalan sesuai dengan yang diharapkan.

**2. PENELITIAN SEBELUMNYA**

**2.1 Kriptografi**

Kriptografi adalah ilmu yang mempelajari tentang metode untuk membuat tulisan atau pesan rahasia. Pada transformasi ini ada dua macam masalah keamanan data , yaitu masalah privasi dan keotentikan. Privasi mengandung arti bahwa data yang dikirimkan hanya dapat di mengerti informasinya oleh penerima yang berhak. Sedangkan keasliannya mencegah pihak ketiga untuk mengirim data yang salah atau mengubah data yang dikirimkan [1].

**2.2 RC4**

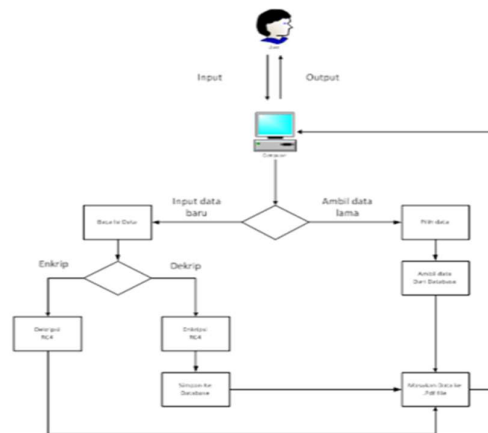
RC4 adalah bagian dari protocol *enkripsi* yang standard dan factor yang sering digunakan menjadi kesuksesan dari RC4 adalah kecepatannya dan kesederhanaannya dalam menangani berbagai banyak aplikasi, sehingga mudah untuk mengembangkan implementasi yang efisien ke *software* dan *hardware*.RC4 adalah algoritma *kriptografi* simetris. Disebut algoritma *kriptografi* simetris karena menggunakan kunci yang sama

untuk *mengenkripsi* atau *mendekripsi* suatu pesan, data, ataupun informasi [2].

**3. METODE PENELITIAN**

**3.1. Arsitektur Sistem**

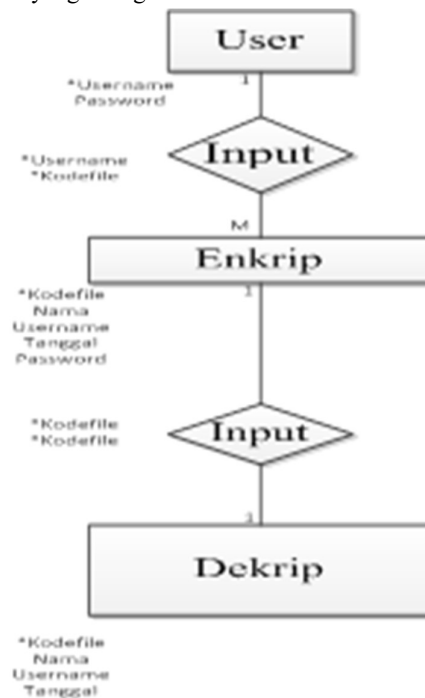
Arsitektur system ini menggambarkan garis besar proses dari keseluruhan alur program yang dibuat oleh si penulis, agar dapat dipahami konsep aplikasi yang di buat:



Gambar 1. Arsitektur Sistem

**3.2. Entity Relationship Diagram (ERD)**

ERD merupakan gambaran untuk menjelaskan hubungan antar data dalam basis data berdasarkan objek data yang saling berkaitan.



Gambar 2. ERD Basic Data

### 3.3. Algoritma proses Enkrpsi RC4

Dibawah ini adalah penjelasan mengenai algoritma mengenai proses enkripsi RC4

```

1. Tampilkan Form Enkrpsi
2. If input pilih = browse file then
3. Input file then
4. Kembali kebaris 1
5. Else if input user = isi key then
6. Isi key then
7. Kembali kebaris 1
8. Else if input user = save file then
9. Save file then
10. Kembali kebaris 1
11. If input user = pilih Enkrip file then
12. Cek validasi
13. If file = kosong
14. Tampil Pesan Peringatan
15. Kembali ke baris 1
16. Else if save password = kosong
17. Tampil pesan peringatan
18. Kembali Kebaris 1
19. Else if key password < $
20. Tampil pesan peringatan
21. Kembali Kebaris 1
22. Else
23. Proses Enkrpsi
24. Tampil Pesan Sukses Enkrpsi
25. Kembali kebaris 1
26. Endif
27. Else if input user = Clean then
28. Proses clean form
29. Else
30. End

```

Gambar 3. Algoritma Enkrpsi

### 3.4. Algoritma Dekripsi

Dibawah ini adalah penjelasan mengenai algoritma mengenai proses enkripsi RC4.

```

1. Tampilkan Form Dekripsi
2. If input user = browse file then
3. Input file then
4. Kembali kebaris 1
5. Else if input user = isi key then
6. Isi key then
7. Kembali kebaris 1
8. Else if input user = save file then
9. Save file then
10. Kembali kebaris 1
11. If input user = pilih Enkrip file then
12. Cek validasi
13. If file = kosong
14. Tampil Pesan Peringatan
15. Kembali ke baris 1
16. Else if password = kosong
17. Tampil pesan peringatan
18. Kembali Kebaris 1
19. Else if password < $
20. Tampil pesan peringatan
21. Kembali Kebaris 1
22. Else
23. Proses Dekripsi
24. Tampil Pesan Sukses Dekripsi
25. Kembali kebaris 1
26. Endif
27. Else if input user = Clean then
28. Proses clean form
29. Else
30. Kembali kebaris 1
31. Endif

```

Gambar 4. Algoritma Dekripsi

## 4. HASIL DAN PEMBAHASAN

### 4.1. Rancangan Layar Form Enkrpsi

Form ini digunakan untuk mengenkrip file sebelum di simpan. Dengan cara melampirkan file yang ingin di enkrip, dan memasukan password, maka file akan terenkrip dan file akan terjaga kerahasiaannya.

Gambar 5. Form Enkrpsi

### 4.2. Rancangan Layar form Dekripsi File

Form ini digunakan untuk mendekrip file yang sudah di enkrip sebelumnya, guna untuk membuka file yang sebelumnya telah di enkrip. Dan dapat di lihat keaslian data nya.

Gambar 6. Form Dekripsi

Kebutuhan yang akan dibutuhkan dalam memenuhi sebuah kebutuhan spesifikasi. Program aplikasi ini agar dapat bias berjalan dengan baik

dan lancer. Agar memenuhi kebutuhan untuk mengaplikasikan program, maka dari itu terdiri dari dua kebutuhan yang harus di persiapkan, yaitu kebutuhan perangkat Lunak dan Kebutuhan perangkat keras.

Berikut spesifikasi minimum perangkat keras untuk mengoperasikan aplikasi tersebut, yaitu:

**Tabel 1.** Spesifikasi Perangkat keras

No	Perangkat	Kebutuhan
1	CPU	Intel ®Core™ i3-2357M CPU @ 1.30GHZ
2	RAM	2 GB
3	MONITOR	14''
4	KEYBOARD	Internal Keyboard laptop
5	HARD DISK	200GB

**4.3. Kebutuhan perangkat lunak**

Untuk menjalankan aplikasi tersebut harus membutuhkan perangkat lunak yang sudah sewajarnya di gunakan, demi kelancaran proses menjalankan program, berikut adalah kebutuhan perangkat lunak untuk menjalankan program tersebut, yaitu: windows 7, Netbeans, Mysql Font, Xampp

**4.4. Form login**

Sebelum melakukan akses ke menu utama user akan dihadapkan pada form login, dimana setiap user harus memiliki username dan password, berikut adalah tampilan form login.



Gambar 7. Interface Login

**4.5. Form Beranda**

Setelah user memasukan username dan password berhasil maka user akan di alihkan ke

menu beranda, dimana dimenu tersebut terdapat banyak pilihan seperti, enkripsi, dekripsi, registrasi dan melihat history.



Gambar 8. Interface Beranda

**4.6. Form Enkripsi**

Form ini berguna untuk melakukan aktifitas enkrip data, supaya data lebih terjaga kerahasiaannya dan tidak berwenang



Gambar 9. Interface Enkripsi

**4.7. Form Dekripsi**

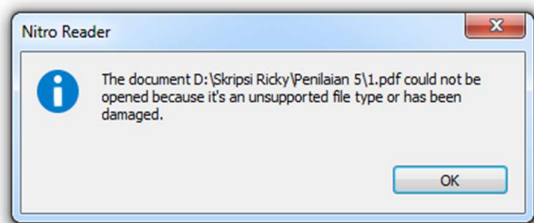
Form ini digunakan untuk mengembalikan file yang sudah di enkripsi menjadi file yang asli.



Gambar 10. Interface Dekripsi

#### 4.8. Form Hasil Enkripsi

Pada form ini memperlihatkan sebuah file yang sudah melakukan proses enkripsi



Gambar 11. Interface File Ter-enkripsi

#### 5. Kesimpulan

Bedasarkan dari hasil analisis yang dilakukan terhadap permasalahan aplikasi yang telah di kembangkan, maka bisa ditarik kesimpulan, yaitu; Dengan adanya aplikasi kriptografi ini data dan dokumen menjadi tidak mudah dicuri dan proses pengamanan data lebih efisien dan mudah dan tingkat keamanan nya lebih tinggi.

#### DAFTAR PUSTAKA

- [1] Subhan, Sapto. Amini, Safrina., & Ariyani, Farida Pipin. (2017). Implementasi Pengamanan Data Enkripsi Sms Dengan Algoritma RC4 Berbasis Android. Jakarta Selatan. *Seminar Nasional Inovasi Dan Aplikasi Teknologi Di Industri*, ITN Malang, pp. 1-6.
- [2] Damanik, Romanus. (2018). Sistem Enkripsi dan Dekripsi Serta Penyembunyian File Teks Menggunakan Algoritma RC4 Dan END OF LIFE Pada Citra Digital, *Jurnal IDN*, vol. 4, no. 1, pp. 50-56.