PENGAMANAN DATA PENJUALAN PADA CV. MONOCHROME DENGAN KRIPTOGRAFI ALGORITMA CAESAR CIPHER DAN RSA

Obby Oktafianto[1)], **Achmad Solichin**[2)]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : obbyracer8@gmail.com[1)], achmad.solichin@budiluhur.ac.id[2)]

Abstrak

CV. Monochrome Custom Motor Cycle adalah perusahaan yang menjual produk sparepart motor. CV. Monochrome Custom Motor Cycle mengalami kesulitan untuk melakukan pengontrolan pada laporan penjualan, Maka dari itu diperlukan aplikasi penjualan produk agar lebih efektif dan efisien, hal ini bertujuan untuk melakukan analisa keuntungan dan memonitor penjualan secara langsung. Untuk menjaga keamanan database penjualan dapat menggunakan metode kriptografi untuk mengamankan data pada database penjualan sehingga data tersebut tidak dilihat oleh pihak yang tidak bertanggung jawab. Aplikasi yang dibangun ini menggunakan metode algoritma Caesar cipher dan Algoritma RSA untuk mengenkripsi data penjualan. Data-data penjualan akan di enkripsi terlebih dahulu dengan menggunakan algoritma Caesar Cipher ketika data disimpan di report maka data akan di enkrip kembali menggunakan algoritma RSA. Hasil dari implementasi algoritma Caesar Cipher dan RSA pada perusahaan tersebut dapat membantu proses pelaporan data penjualan menjadi lebih terjamin keamanan dan kerahasiaan data.

Kata Kunci : *Caesar Cipher*, RSA, enkripsi, dekripsi, database.

1. PENDAHULUAN

1.1 Latar Belakang

Keamanan dalam penyimpanan suatu data atau informasi adalah hal yang sangat penting dan tidak dapat diabaikan, data yang dulunya berupa data tertulis telah berubah menjadi elektronik atau digital.

Kriptografi adalah satu metode yang digunakan dalam penelitian ini untuk merahasiakan data penting tersebut. Database adalah tempat penyimpanan dari data yang disimpan dalam kurun waktu tertentu. Pada penelitian ini algoritma yang akan digunakan adalah algoritma *Caesar Cipher* dan algoritma *RSA*.

Dasar pemilihan algoritma yaitu karena algoritma *Caesar Cipher* dan algoritma *RSA* memiliki keamanan yang cukup tinggi untuk menjaga keamanan Database penjualan. Berdasarkan latar belakang yang telah disampaikan di atas, rumusan masalah yang dihadapi dalam perancangan sistem yaitu :

a. CV. Monochrome Custome Motor Cycle belum memiliki sistem keamanan dan kerahasiaan data sehingga siapapun dapat melihat data penjualan
b. Bagaimana mengamankan database dari pencurian informasi dengan cara mengimplementasikan kriftografi dengan menggunakan metode *Caesar Cipher* dan *RSA*.

Maksud dan tujuan dari penelitian ini adalah untuk mengimplementasikan algoritma kriptografi dengan metode algoritma *Caesar Cipher* dan algoritma *RSA*. Secara umum, tujuan dari penulis adalah untuk membangun aplikasi pengamanan database pada dokumen penjualan yang bersifat penting dan rahasia agar tidak mudah diakses atau dimanipulasi oleh pihak yang tidak bertanggung jawab.

Adapun batasan masalah pada penelitian ini adalah sebagai berikut;

a. File yang dienkripsi adalah data yang tersimpan dalam database
b. Aplikasi ini digunakan 1 *user*

2. TINJAUAN PUSTAKA

2.1 Algoritma *Caesar Cipher*

Salah satu kriptografi yang paling tua dan paling sederhana adalah kriptografi Caesar yang ditemukan oleh Julius Caesar [1]. Kriptografi Caesar digunakan untuk menyembunyikan pesan surat cinta kaisar untuk kekasihnya Cleopatra. Dalam kriptografi Caesar, digantikan dengan huruf lain dengan pergeseran beberapa huruf. Kriptografi Caesar ini merupakan kriptografi substitusi karena setiap huruf akan digantikan huruf lain.

Langkah-langkah yang dilakukan untuk membentuk chiperteks dengan Caesar Cipher adalah:

1. Menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks.
2. Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya.

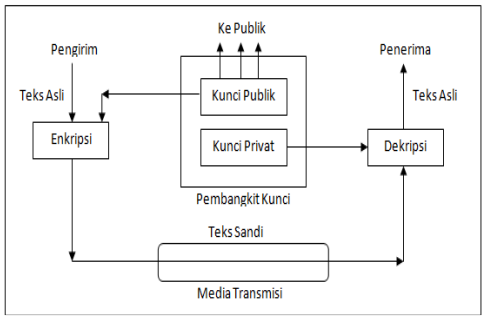
Dengan cara sebagai contoh berikut, huruf A akan digeser 3 huruf menjadi huruf D, B akan digeser 3 huruf menjadi E, J akan digeser menjadi M, O akan menjadi R dan seterusnya. Pergeseran ini juga berputar kembali ke awal abjad. sehingga sesudah huruf Z diikuti kembali oleh huruf A. Kriptografi Caesar ini dikenal sebagai monoalphabetic substitution cipher karena satu huruf tertentu pasti akan berubah menjadi huruf tertentu yang lain.

- **Plaintext :**
  ABCDEFGHIJKLMNOPQRSTUVWXYZ
- **Ciphertext :**
  DEFGHIJKLMNOPQRSTUVWXYZABC

Walaupun termasuk algoritma kriptografi yang sangat sederhana, algoritma Caesar masih diterapkan di beberapa penelitian, tentunya dengan melakukan modifikasi tertentu. Perkasa dkk. [5] menerapkan algoritma Caesar Cipher yang digabungkan dengan algoritma kompresi Shannon-Fano untuk mengamankan data digital.

2.2 Algoritma RSA *(Rivest Shamir Adleman)*

Algoritma RSA menggunakan 2 angka (e dan d) sebagai kunci publik dan kunci *private* [1][2]. Pada algoritma RSA e dan n diumumkan untuk umum sedangkan d dirahasiakan. Meskipun RSA dapat digunakan untuk mengenkripsi dan mendekripsi pesan, sangat lambat jika pesan tersebut panjang. Oleh karena itu, algoritma RSA berguna untuk pesan singkat. Sejak algoritma menggunakan 2 kunci untuk enkripsi dan dekripsi, algoritma RSA dianggap sebagai contoh kunci asimetrik kriptografi. Desain konseptual dari algoritma RSA dapat disajikan pada Gambar.



Gambar 1. Konsep kriptografi kunci publik RSA

Algoritma RSA dibagi menjadi 3 langkah :

(1) Pembangkit Kunci
   (a) Pilih 2 bilangan prima besar untuk nilai *p* dan *q*
   (b) Hitung nilai modulus $n = p \times q$
   (c) Hitung menggunakan fungsi Euler . $(n) = (p\text{-}1) \times (q\text{-}1)$
   (d) Pilih nilai integer *e* acak sebagai kunci publik, dengan syarat memenuhi *Greater Common Divisor* (GCD) $(e, . (n)) = 1$, $1 < e < . (n)$
   (e) Hitung kunci privat d sehingga $d \times e = 1 \pmod{. (n)}$

(2) Enkripsi

$$C = Me \bmod n$$

(3) Dekripsi

$$M = Cd \bmod n$$

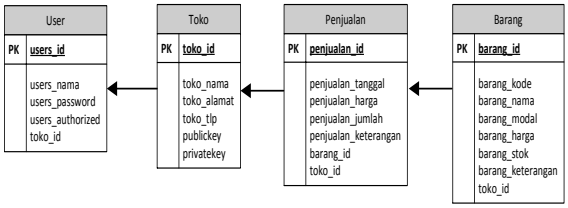
3. METODOLOGI DAN PENYELESAIAN MASALAH

3.1 Analisis dan Penyelesaian Masalah

Dari permasalahan yang telah diuraikan diatas, diperlukan adanya aplikasi yang dapat menjaga kerahasiaan laporan penjualan dengan menggunakan teknik kriptografi pada database sehingga tidak semua orang bisa melihat isi file yang berisikan laporan tersebut. Kerahasiaan isi file menjadi faktor penting karena apabila isi file tersebut diketahui pihak lain yang tidak bertanggung jawab maka isi file dapat dimanipulasi dan merugikan perusahaan. Oleh sebab itu dibutuhkan sebuah aplikasi yang bisa melindungi keamanan data, sehingga algoritma kriptografi *caesar cipher* dan *RSA* pada database adalah solusi yang tepat digunakan untuk keamanan dokumen. Aplikasi ini dibuat sangat sederhana agar mudah digunakan dan dipahami user. Tingkat kerahasiaan ini tinggi selama kata kunci dapat dijaga dengan baik. Dengan adanya aplikasi ini diharapkan dapat membantu mengatasai ancaman pencurian yang terjadi pada keamanan informasi dari file penjualan yang bersifat rahasia.

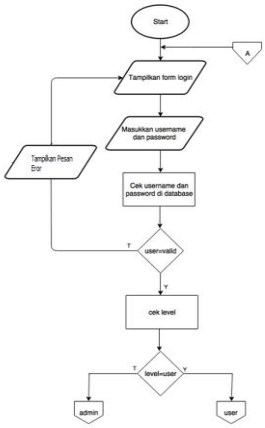
3.2 Perancangan Database

Dalam hal perancangan laporan penjulan dengan teknik kriptografi berbasis web ini diperlukan perancangan database untuk menampung data laporan dan database inilah yang nantinya akan dienkripsi.



Gambar 2. LRS (Logical Record Structured)

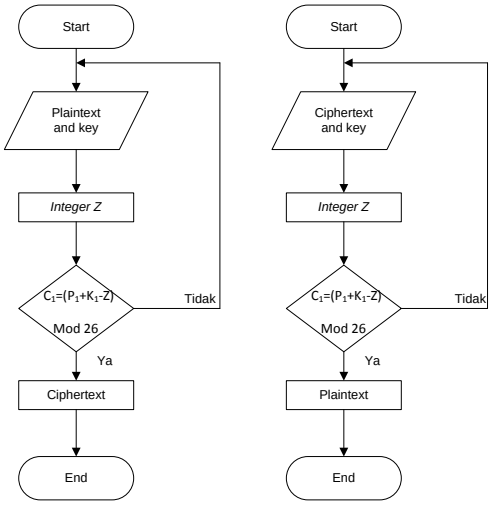
3.3 Flowchart Dan Algoritma



Gambar 3. Flowchart Menu Log In

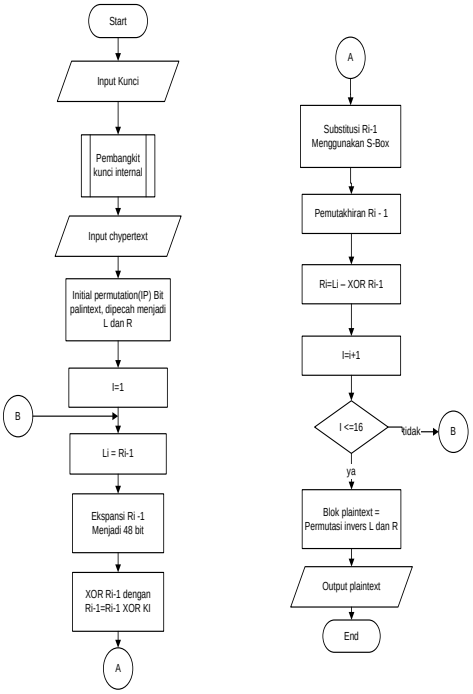
Flowchart menu utama seperti di atas adalah proses saat pengguna melakukan log in. Kemudian

setelah login maka pengguna akan masuk ke dalam menu utama sistem.



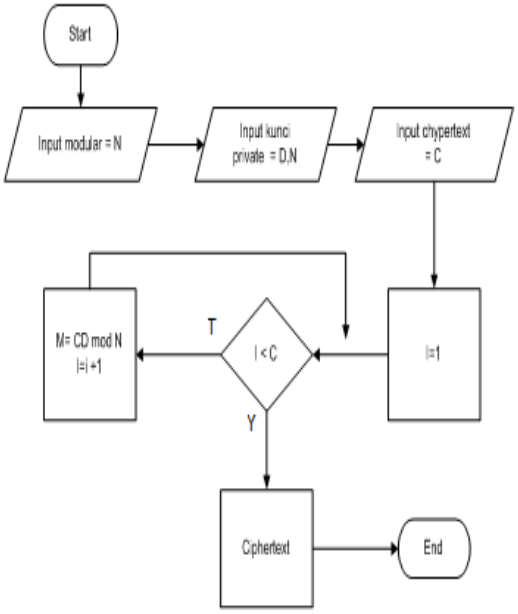
Gambar 4. Flowchart Proses Enkripsi Dan Dekripsi Database Pada Algoritma Caesar Cipher

Pada gambar di atas menjelaskan proses atau alur dari enkripsi atau proses penyembunyian atau pengacakan data. Proses enkripsi dimulai dengan membaca data di *database* dan panjang data di database.



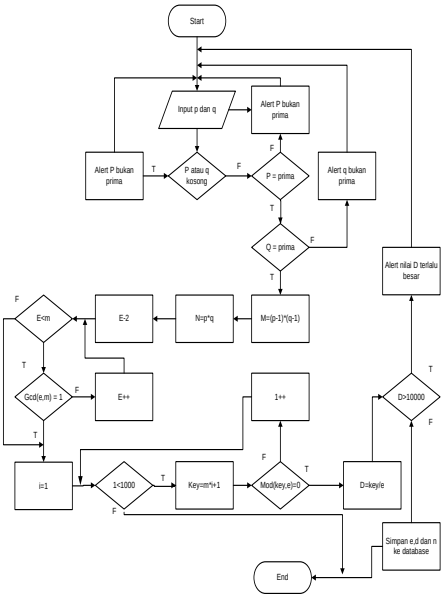
Gambar 5. Flowchart Enkripsi RSA

Gambar di atas adalah Flowchart Enkrisi RSA.



Gambar 6. Flowchart Dekripsi RSA

Gambar di atas adalah Flowchart Dekripsi RSA.



Gambar 7. Flowchart Generate Key RSA

Gambar di atas adalah Flowchart Generate Key RSA.

1. Start
2. Tampilkan Halaman Sign in
3. Input Full name
4. Input Password
5. If pilih tombol "sign in" then
6. Cek Full name and Password
7. If Full name = users_nama and Password = users_password then
8. Cek akses Level
9. If users_authorized = admin then

10. masuk halaman Home Admin
11. Else masuk halaman Home User End if
12. Else Full name != users_nama and Password != users_password then
13. Tampil pesan "full name dan password tidak sesuai"
14. Else
15. Kembali ke baris 2
16. End If
17. End

Algoritma di atas adalah algoritma yang menjelaskan tentang menu utama. Yang mana menjelaskan cara kerja dari menu utama sistem.

1. Start
2. Select database for enkripsi
3. Input password
4. Pengecekan Password
5. Baca pesan serta panjang pesan, baca output lokasi & nama database.
6. Mulai enkripsi
7. Ubah pesan dan password ke caesar chiper, ubah bits pesan ke caesar cipher untuk pesan dan password
8. Enkripsisi pesan dan password
9. Tulis kembali enkripsi pesan dan password , simpan dilokasi output stream
10. **If** "enkripsisi sukses?" **Then**
11. Proses simpan data databse dari crypto file ke output file.
12. **Else**
13. Kembali ke baris 1
14. **End If**

Algortima di atas adalah penjelasan tentang proses bagaimana sistem penggajian dienkripsi menggunakan algoritma caesar cipher.

1. *Start*
2. Input Modular = n
3. Input kunci public = e, n
4. Input plaintext = m
5. Inisialisasi variable i = 1
6. If i< = panjang m
7. C= m^e mod n
8. i = i+1
9. Kemba like 6
10. Else c = ciphertext
11. End

Algoritma di atas adalah enkripsi RSA menjelaskan tentang proses enkripsi yang digunakan pada database.

1. *Start*
2. *Input* Modular = n
3. *Input* kunci Privat = d, n
4. *Input ciphertext* = c
5. Inisialisasi*variable* i = 1
6. *If* i < = panjang m
7. m = c^d mod n
8. i = i+1
9. Kembalike 6
10. *Else* c = ciphertext
11. *End*

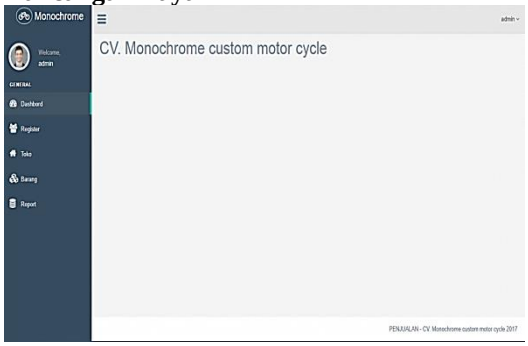
Algoritma di atas adalah dekripsi RSA menjelaskan tentang proses dekripsi yang digunakan pada database.

1. If p prima then
2. If q prima then
3. M= (p-1)*(q-1)
4. N= p*q
5. E= 2
6. If e < m then
7. If gdc(e,m) = 1 then
8. I=1
9. If i<1000 then
10. Key = m*i+1
11. If mod(e,key) = 0 then
12. D=key/e
13. If d > 10000 then
14. Alert nilai d terlalu besar
15. Else
16. Simpan e,d,n ke database
17. Endif
18. Endif
19. Else
20. I++
21. Kembali ke 12
22. Endif
23. Else
24. E++
25. Kembali ke 9
26. Endif
27. Else
28. Return 2
29. Endif
30. Else
31. Return 1
32. Endif

Algoritma di atas adalah Generate Key RSA menjelaskan tentang proses pembuatan kunci *Private* dan *Public* yang digunakan untuk proses Enkrip dan Dekrip.

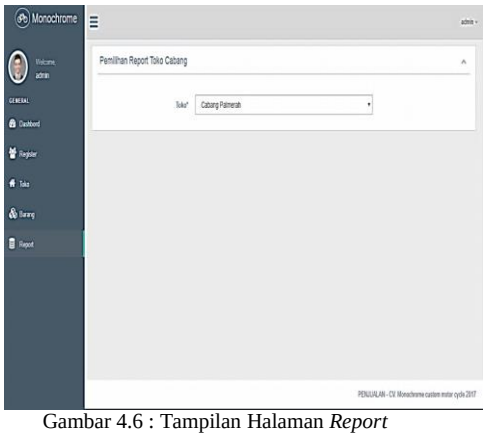
4. HASIL DAN PEMBAHASAN

4.1 Rancangan Layar



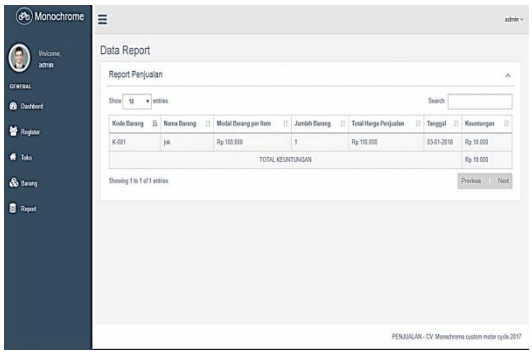
Gambar 8. Rancangan Layar Menu Utama

Berikut adalah tampilan *Report* penjualan, admin dapat melihat report setiap cabang.



Gambar 4.6 : Tampilan Halaman *Report*

Berikut adalah tampilan *Report Detail*, admin dapat melihat secara *detail report* setiap cabang.



Gambar 9. Tampilan Halaman Tambah *Report Detail*

4.2 Analisa Hasil Implementasi Dan Uji Coba Sistem

Berikut merupakan tabel hasil dari percobaan enkripsi dan dekripsi dengan menggunakan algoritma Caesar dan RSA

a. Tabel Percobaan Enkripsi

Tabel 1, Hasil Enkripsi

barang_id	barang_kode	barang_modal	barang_nama
1	K-001	H92q5q+OZ2WiYd1kxRsJsCidwX2NOUxw05gkQzQRLsnY3OS+TMlrq4UILGRnXjNyeRG/NEgalUaigzbWkeGsrVbv54lXS6CbGVZO6KcZcdnnJC6nyA/eX7wLgLuOocNMxXqSh7xDzti4zWYIIJDyoHo0XqX66eb1xuLqLk6Ia3k=	jok
2	B-0012	TkFAFLiNMxhQ6LkUHG2q2J039TC+QClbZjFYzQ5j5qTJz2kBi4LWWqeosAWzgibbyZpvj+6TImTWF+XJR7AXIjHbrpnyp5M6I+Zx6MWsnZsqmM5zYIJ4Fm3k/ebooPlZNUTMxy9XFyPCZjLBQP/tEHzmCgmwWN42z0lkz4zkHeY=	kenalpot

a. Tabel Percobaan Dekripsi

Tabel 2, Hasil Dekripsi

barang_id	barang_kode	barang_modal	barang_nama
1	K-001	Rp.100.000	jok
2	B-0012	Rp.234.000	kenalpot

4.3 Kelebihan dan Kekurangan Program

a. Kelebihan Aplikasi

1) Tampilan aplikasi *user friendly* sehingga mudah digunakan.
2) Database penjualan menjadi lebih aman karena sudah melalui proses enkripsi.
3) Hasil report penjualan bisa langsung dilihat oleh admin setiap hari dan dapat melihat langsung menghitung estimasi kebutuhan serta keuntungan.
4) Mempermudah pencarian data pada database.

b. Kekurangan Aplikasi

1) Banyaknya data penjualan yang tampil adalah sesuai yang user input.
2) Belum terdapat menu faktur dan mutasi

5. KESIMPULAN

Melalui proses pengerjaan dan pengujian dalam penelitian ini, dapat disimpulkan beberapa hal, yaitu :

a. Dengan adanya implementasi kriptografi, informasi pada Database yang telah dilakukan proses enkripsi dapat terjaga keamanan dan kerahasiaannya.
b. Informasi penjualan dapat di rahasiakan dan di amankan dari penyalahgunaan dan pencurian informasi.
c. Aplikasi dapat mengenkripsi informasi pada data penjualan di toko cabang dengan baik menggunakan algoritma *Caesar Cipher* dan *RSA* sehingga sulit untuk di pecahkan.
d. Mempermudah pencarian data report pada database

6. DAFTAR PUSTAKA

[1] Ariyus, D. (2008) 'Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi'.

[2] Ginting, A., Isnanto, R. R. and Windasari, I. P. (2016) 'Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email', *Jurnal Teknologi dan Sistem Komputer*, 3(2), pp. 253–258. doi: 10.14710/JTSISKOM.3.2.2015.253-258.

[3] Kadir, A. (2000) 'Konsep dan Tuntunan Praktis Basis Data', *Yogyakarta*, p. 14186.

[4] Munir, R. (2004) 'Pengolahan Citra Digital dengan Pendekatan Algoritmik', *Universitas Gunadarma*, pp. 1–10. Available at: http://amutiara.staff.gunadarma.ac.id/Downloads/folder/0.58.

[5] Perkasa, S., Syahrizal, M. and Simangunsong, P. B. N. (2017) 'IMPLEMENTASI KEAMANAN DATA TEKS DENGAN ALGORITMA MODIFIKASI

CAESAR CIPHER DAN MENGKOMPRESI FILE MENGGUNAKAN ALGORITMA SHANNON FANO', *Jurnal INFOTEK*, 2(1), pp. 69–73.

[6] Wahyadyatmika, A. P., Isnanto, R. R. and Somantri, M. (2014) 'Implementasi Algoritma Kriptografi RSA pada Surat Elektronik (E-Mail)', *Jurusan Teknik Elektro*, 3(4), pp. 1–9.