OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 1919-1926

Implementasi Kriptografi Untuk Mengamankan Database Administrasi Menggunakan Metode *CAESAR CIPHER* dan BASE64

Syakur Nurokhman[1], Jaka Sutrisna[2*]

[1,2]Fakultas Teknik, Teknik Informatika, Universitas Pamulang, Jl. Raya Puspiptek No. 46, Kel. Buaran, Kec. Serpong, Kota Tangerang Selatan. Banten 15310, Indonesia
Email: [1]syakur97.sn@gmail.com, [2*]dosen00833@gmail.com
(* : coressponding author)

Abstrak− Perkembangan teknologi informasi saat ini telah mengalami kemajuan yang sangat pesat dalam berkomunikasi, mengakses suatu data atau informasi melalui bermacam-macam media salah satunya melalui media website dalam internet. Keamanan dalam penyimpanan suatu data atau informasi adalah hal yang sangat penting. PT. Pegadaian menjadi khawatir jika akan menggunakan aplikasi tersebut tidak aman dan saat tersimpan kedalam database, karena data dan informasi yang bersifat penting dan masih rentan terhadap pencurian serta penyalahgunaan oleh pihak tertentu yang dapat menimbulkan kerugian yang sangat besar. Dalam perancangan aplikasi ini, penulis membuat suatu metode dengan cara proses enkripsi. Kriptografi Caesar Cipher menggunakan kunci angka untuk menenkripsi dan Base64 sistem untuk mewakili data byte sebagai karakter ASCII.

Kata Kunci: Caesar Cipher, Chiper, Enkripsi, Kriptograf.

Abstract− The development of information technology has now experienced very rapid advances in communicating, accessing data or information through various media, one of which is through website media on the internet. Security in the storage of data or information is very important. Pt. Pegadaian are worried that if they will use the application, it is not safe and when stored in a database, because data and information are important and are still vulnerable to theft and misuse by certain parties which can cause huge losses. In designing this application, the author created a method by means of an encryption process. Caesar Cipher cryptography uses number keys to encrypt and Base64 systems to represent byte data as ASCII characters.

Keywords: Human Resources, Decision Support Systems, SMART (Simple Multi Attribute Rating Technique).

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini telah mengalami kemajuan yang sangat pesat dalam berkomunikasi, mengakses suatu data atau informasi melalui bermacam-macam media salah satunya melalui media website dalam internet. Seseorang dengan mudah menyimpan, mengunduh, dan mengakses suatu data atau informasi. Keamanan dalam penyimpanan suatu data atau informasi adalah hal yang sangat penting dan tidak dapat diabaikan. Salah satu dampak negatif dalam perkembangan teknologi adalah pencurian data. Pencurian data ini tentunya merugikan bagi pemilik data, untuk menghindari kejahatan tersebut maka dibutuhkan pengamanan dalam penyimpanan data yang dianggap penting agar terhindar dari kejahatan teknologi informasi.Setiap perusahaan didirikan dengan tujuan mendapatkan keuntungan dalam jangka panjang. Namun terkadang perusahaan cenderung mengabaikan begitu saja bahwa keamanan data merupakan hal yang sangat penting dalam mencapai tujuan tersebut, sehingga banyak perusahaan yang kurang memperhatikan keamanan data. Seharusnya perusahaan dapat memperhatikan hal-hal yang dianggap penting oleh penggunanya, karena memperhatikan keamanan data merupakan salah satu faktor penting dan sangat menentukan kelanjutan hidup sebuah perusahaan dalam persaingan sekarang ini.PT. Pegadaian adalah anak perusahaan Bank Rakyat Indonesia yang bergerak pada tiga lini bisnis, yakni pembiayaan, emas dan aneka jasa, terkait dengan sistem keamanan jaringan dan keamanan aplikasi dan keamanan data juga perlu dijaga supaya data yang dimiliki perusahaan tidak dapat dibaca atau enskripsi data gadai, pembayaran, dan nasabah tidak disalahgunakan oleh pihak yang tidak diinginkan. Oleh karena itu agar tidak ada orang yang berkepentingan dapat mengubah data yang

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 1919-1926

sudah disimpan atau dapat mencuri data yang ada, dibutuhkan sebuah metode untuk dapat mengamankan data dalam record database. Penerapan kriptografi dalam tugas akhir ini akan difokuskan bagaimana kriptografi bisa mengamankan data yang disimpan melalui sistem database menjadi aman sampai dengan data dibuka oleh orang yang berkepentingan.Banyak teknik yang dapat digunakan untuk mengamankan data-data tersebut diantranya adalah kriptografi. Teknik tersebut memiliki fungsi masing-masing, kriptografi yang bertujuan untuk menyamarkan suatu pesan menjadi suatu pesan yang sulit dibaca atau dimengerti .Berdasarkan kenyataan diatas, perlu ada suatu sistem pengamanan informasi saat menginput data kedalam database. Untuk melakukan hal ini ada suatu cara yang biasa disebut penyandian data. Dalam penelitian ini akan mencoba mengimplementasikan suatu cabang ilmu matematika yang disebut dengan kriptografi. Dengan kriptografi data dapat diubah menjadi sandi-sandi yng tidak di mengrti oleh sembarang orang serta mengembalikannya kebentuk semula, proses ini disebut enkripsi dan dekripsi. Algoritma enkripsi ternyata sudah cukup beragam. Dalam laporan tugas akhir ini penulis akan akan menggunakan 2 metode algoritma *Caesar Cipher* dan Base64 untuk proses enkripsi dan dekripsi data kedalam sistem *database.*

2. METODOLOGI PENELITIAN

2.1 Metode Pengumpulan Data

Metode yang digunakan pada pengumpulan data dalam program aplikasi ini adalah sebagai berikut:

a. Studi Pustaka
   Mengumpulkan data yang berkaitan dengan metode Caesar Cipher dan Base64 ataupun yang berhubungan dari berbagai buku, artikel, dan modul.
b. Wawancara dan Observasi
   Melakukan wawancara terhadap data perusahaan dan mengadakan penelitian untuk mengumpulkan data secara langsung.

2.2. Metode Pengembangan Sistem

2.2.1 Algoritma Kriptografi Caesar Cipher

Caesar Cipher merupakan salah satu algoritma cipher tertua dan paling diketahui dalam perkembangan ilmu kriptografi. Caesar cipher merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada chiperteks. Teknik seperti ini disebut juga sebagai chiper abjad tunggal.Algoritma kriptografi Caesar Cipher sangat mudah untuk digunakan. Inti dari algoritma kriptografi ini adalah melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama.

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

a. Menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks
b. Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya. Algoritma dari Caesar Cipher adalah C = E (P) = (P + K) mod 26 untuk fungsi enkripsi. Sedangkan untuk fungsi dekripsi adalah P = D (C) = (C - K) mod 26.

2.2.2 Algoritma Base64

Base64 adalah istilah umum untuk sejumlah skema pengkodean serupa yang mengkodekan data biner dan menerjemahkannya ke dalam representasi basis 64. Istilah Base64 berasal dari konten pengkodean MIME tertentu. Skema encoding base64 biasanya digunakan ketika ada kebutuhan untuk menyandikan data biner yang perlu disimpan dan ditransfer melalui media yang dirancang untuk menangani data tekstual. Hal ini untuk memastikan bahwa data tetap utuh tanpa perubahan selama pengiriman. Base64 digunakan umum dalam beberapa aplikasi termasuk email melalui MIME, dan penyimpanan data yang kompleks dalam XML. Transformasi Base64 termasuk dalam

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 1919-1926

kriptografi dan banyak digunakan di dunia internet sebagai media data format untuk mengirimkan data. Dikarenakan hasil dari transformasi base64 berupa plaintext, maka nilai ini akan jauh lebih mudah dikirim, dibandingkan format data berupa binary.

Teknik Encoding Base64 sebenarnya sederhana, jika ada satu (string) byte yang akan disandikan ke Base64 maka caranya adalah :

a. Pecah string bytes tersebut ke per-3 bytes.
b. Gabungkan 3 bytes menjadi 24 bits. Dengan catatan 1 bytes =8 bit, sehingga 3x8=24 bits.
c. Lalu 24 bits yang disimpan di-buffer (disatukan) dipecah-pecah menjadi 6bits, maka akan menghasilkan 4 pecahan.
d. Masing-masing pecahan diubah ke dalam nilai decimal, dimana maksimal nilai 6bit adalah 63.
e. Terakhir, jadikan nilai-nilai decimal tersebut menjadi indeks untuk memilih karakter penyusunan dari Base64 dan maksimal adalah 63 atau indeks ke 64.

Dan seterusnya sampai akhir string bytes yang mau kita konversikan. Jika ternyata dalam proses encoding terdapat sisa pembagi, maka tambahkan sebagai penggenap sisa tersebut karakter =. Maka terkadang pada Base64 akan muncul satu atau dua karakter (=).

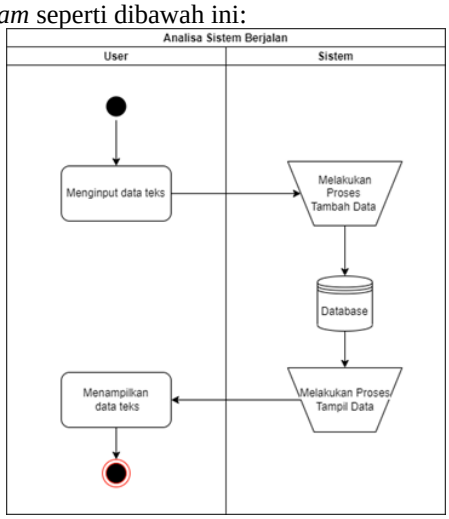
2.2.3 Kriptografi

Kriptografi (cryptography) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yangmempelajari teknik-teknik matematika yang berhubungan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data (Menezes, Oorschot and Vanstone, 1996). Secara umum kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita (bruce SchneireApplied Cryptography). Selain defenisi tersebut ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi.

3. ANALISA DAN PEMBAHASAN

3.1 Analisa Sistem Berjalan

Analisis ini direncanakan untuk sistem aplikasi yang sedang berjalan bertujuan untuk mengetahui bagimana cara kerja suatu sistem dan mengetahui masalah yang dihadapi untuk dapat dijadikan sebagai landasan usulan perancangan. Tahap analisis ini diperlukan untuk mengetahui bagai mana proses sistem berjalan. Tahap perancangan ini penulis menggambarkan sistem yang sedang berjalan dalam bentuk *activity diagram*. Adapun rancangan yang digambarkan dengan menggunakan *activity diagram* seperti dibawah ini:

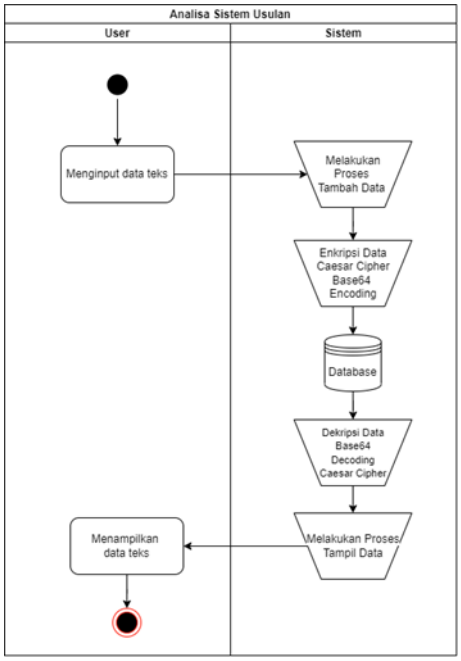


Gambar 1. *Activity Diagram* Sistem Berjalan

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 1919-1926

3.2 Analisa Sistem Usulan

Analisis ini menjelaskan tentang kebutuhan atau kondisi yang harus dipenuhi dalam suatu sistem. Adapun rancangan yang digambarkan dengan menggunakan *activity diagram* seperti dibawah ini:

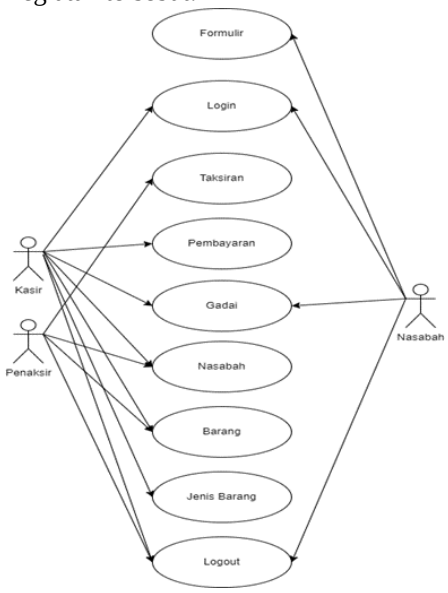


Gambar 2. *Activity Diagram* Sistem Usulan

3.3 Perancangan Basis Data

a) Use Case Diagram

Use case diagram menjelaskan urutan kegiatan yang dilakukan aktor dan sistem untuk mencapai suatu tujuan tertentu. Walaupun menjelaskan kegiatan namun *use case* diagram hanya menjelaskan apa yang dilakukan oleh aktor dan sistem, bukan bagaimana aktor dan sistem melakukan kegiatan tersebut.

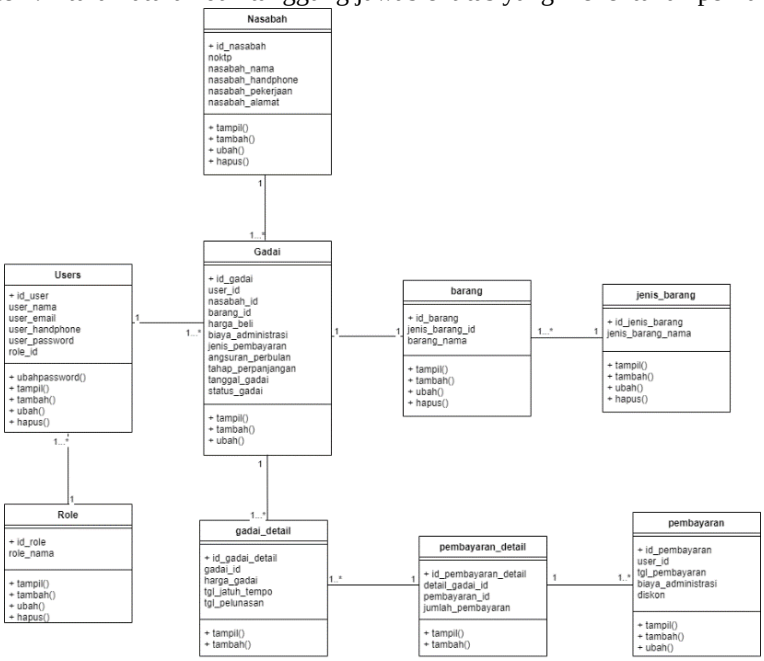


Gambar 3. *Use Case Diagram*

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 1919-1926

b) Class Diagram

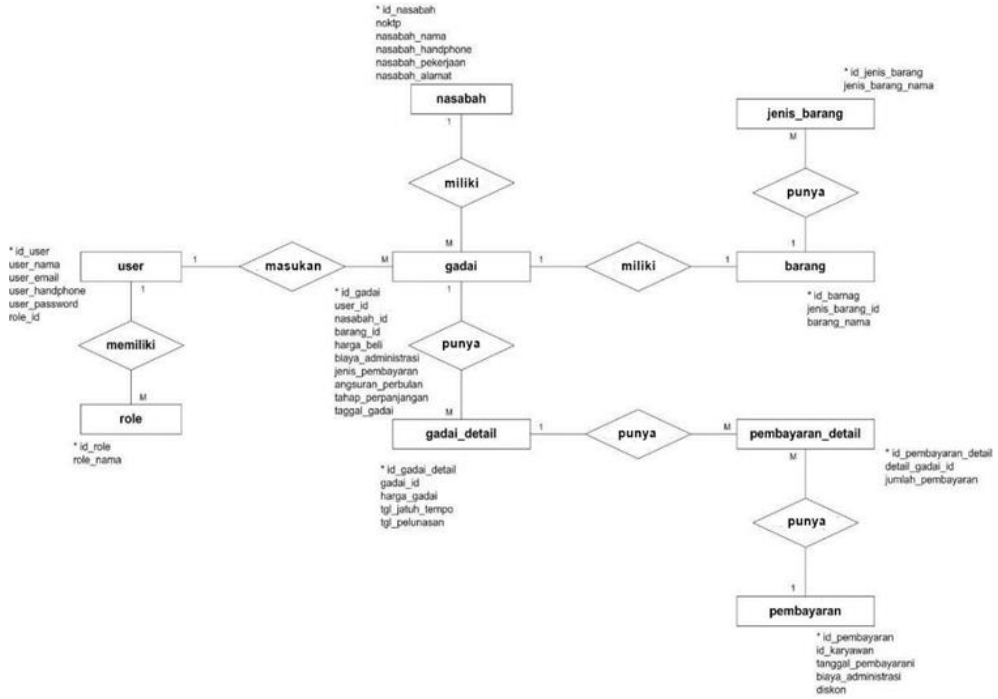
Class Diagram ini menjelaskan hubungan antar *table* di dalam model *desain* dari suatu sistem. Aturan-aturan dan tanggung jawab entitas yang menentukan perilaku sistem.



Gambar 4. *Class Diagram*

c) *Entity Relationship Diagram* (ERD)

Entity Relationship Diagram (ERD) dibuat untuk menggambarkan atau membuat model suatu database dengan diagram yang sederhana sehingga memudahkan dalam membuat sebuah database yang kompleks maupun yang sederhana.



Gambar 5. *Entity Relationship Diagram (ERD)*

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 1919-1926

4. IMPLEMENTASI

Berdasarkan perancangan sistem yang telah dibuat sebelumnya maka selanjutnya sistem diimplementasikan dalam bentuk aplikasi melalui pengkodean. Pengkodean dapat dikatakan sebagai penerjemahan dari desain ke dalam bahasa pemrograman tertentu yang dikenali oleh komputer untuk menjadi sebuah aplikasi (Ahmad, 2021), Berikut tampilan:

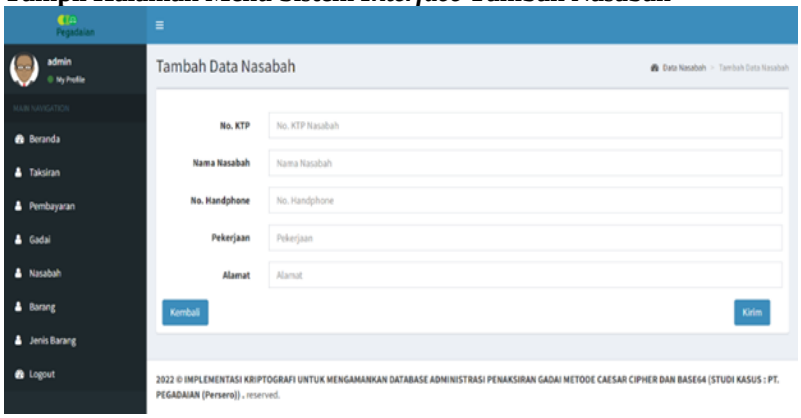
a. Tampil Halaman Login

Gambar 6. Tampilan Halaman *Login*

b. Tampil Halaman Menu Sistem *Interface* Taksiran

Gambar 7. Tampilan Halaman Sistem *Interface* Taksiran

c. Tampil Halaman Menu Sistem *Interface* Tambah Nasabah



Gambar 8. Tampilan Halaman Menu Sistem *Interface* Tambah Nasabah

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 1919-1926

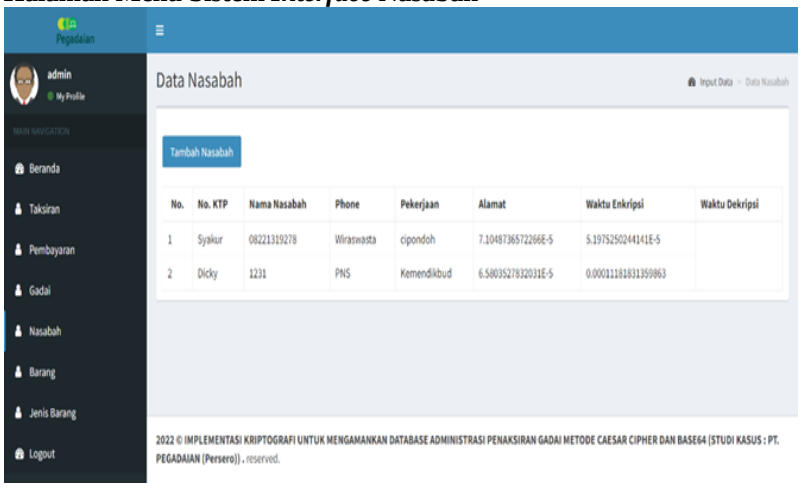
d. Tampil Halaman Menu Sistem *Interface* Tambah Barang

Gambar 9. Tampilan Halaman Menu Sistem *Interface* Tambah Barang Halaman Data User

e. Halaman Menu Sistem *Interface Home*

Gambar 10. Tampilan Halaman Menu Sistem *Interface Home*

f. Halaman Menu Sistem *Interface* Nasabah



Gambar 11. Tampilan Halaman Menu Sistem *Interface Nasabah*

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 11, November 2022
ISSN 2828-2442 (media online)
Hal 1919-1926

5. KESIMPULAN

Berdasarkan analisis yang dilakukan dimulai dari pengumpulan informasi, pemecahan masalah hingga pengembangan aplikasi ini, maka dapat ditarik beberapa kesimpulan dan saran yang perlu diperhatikan demi kelancaran sistem yang dibangun ini:

a. Aplikasi yang telah di implementasikan dapat berguna dan dipakai sistem keamanannya oleh PT. Pegadaian (Persero).
b. Aplikasi ini telah diatur oleh demikian rupa data yang di input dan di tampilkan tersebut otomatis telah dienkripsi dengan baik.
c. Diimplementasikan menggunakan bahasa pemograman *PHP* dengan menggunakan algoritma *Caesar Cipher dan Base64* untuk *enkripsi* dan *dekripsi.*

REFERENCES

Aliman. Wilianti. (2021). Perancangan Perangkat Lunak Untuk Menggambar Diagram Berbasis Android. *Jurnal Ilmiah Indonesia. p–ISSN: 2541-0849 e-ISSN: 2548-1398 Vol. 6, No. 6,* Juni 2021.

Kurniawan, A., (2008), Konsep dan Implementasi Cryptography Dengan .NET, Penerbit PC Media, Jakarta.

Al-Anshori, F., & Aribowo, E. (2014). Implementasi Algoritma Kriptografi Kunci Publik Elgamal Untuk Proses Enkripsi Dan Dekripsi Guna Pengamanan File Data. Jurnal Informatika Februari 2014.

Rinaldi Munir, "Kriptografi", Penerbit Informatika, Bandung, 2006.

Jumrin. Sutardi, dan Subardin. 2016. Aplikasi Sistem Keamanan Basis Data Dengan Teknik Kriptografi RC4 Stream Cipher, semanTIK. Vol.2, No.1