Perancangan Aplikasi Pengamanan Basis Data Menggunakan Algoritma Caesar Cipher

Agustin Siburian[1], Andy Paul Harianja[2]
[1]Teknik Informatika Unika St. Thomas S.U; Jln. Setia Budi No.479-F Medan, 061-8210161
[2]Teknik Informatika Unika St. Thomas S.U; Jln. Setia Budi No.479-F Medan, 061-8210161
e-mail : agustinsiburian10@gmail.com; [2]apharianja@gmail.com

Abstrak

Keamanan dan kerahasiaan data yang tersimpan dalam basis data merupakan salah satu aspek penting dari suatu sistem informasi, seperti data-data tersebut aman dari kebocoran informasi. Jaringan komputer yang terhubung dengan basis data sudah tidak lagi menjamin keamanan data karena kebocoran data dapat disebabkan oleh orang dalam atau pihak-pihak yang langsung berhubungan dengan basis data seperti administrator basis data. Pada aplikasi pengamanan ini disediakan sistem login dengan password dan jika yang mengakses data secara ilegal maka yang akan ditampilkan berupa data nilai cipherteks. Dalam penelitian ini akan menggunakan cara dengan mengenkripsi basis data dengan algoritma caesar cipher. Algoritma Caesar Cipher akan mengenkripsi plainteks dengan cara menggeser posisi plainteks sebanyak jumlah kunci. Hasil akhir dari penggunaan algoritma caesar cipher ini diperoleh pengamanan data nilai pada basis data lebih terjamin keamanannya.

***Kata Kunci** : Kriptografi, Keamanan Data, Basis Data*

Abstract

The security and confidentiality of data stored in the database is one important aspect of an information system, as these data are safe from information leakage. Computer networks connected to the database no longer guarantee data security because data leaks can be caused by insiders or parties directly related to databases such as database administrators. In this security application provided login system with password and if the data access illegally then that will be displayed in the form of ciphertext value data. In this research will use the way by encrypting the database with caesare cipher algorithm. The Caesar Cipher algorithm will encrypt plaintext by shifting the plaintext position by the number of keys. The end result of the use of Caesare Cipher algorithm obtained security data value on the database more secure.

***Keywords :** Cryptography, Data Security, Database*

1. PENDAHULUAN

Keamanan dan kerahasiaan data yang tersimpan dalam basis data merupakan salah satu aspek penting dari suatu sistem informasi, seperti data - data tersebut aman dari kebocoran informasi. Pengamanan terhadap jaringan komputer yang terhubung dengan basis data sudah tidak lagi menjamin keamanan data karena kebocoran data dapat disebabkan oleh orang dalamatau pihak - pihak yang langsung berhubungan dengan basis data seperti administrator basis data.

Basis data adalah sekumpulan informasi yang disimpan didalam komputer secara sistematik yang dapat digunakan melalui sebuah program komputer tertentu untuk menjalankannya. Untuk menjaga keamanan dan kerahasiaan data tersebut diperlukan beberapa pengamanan agar data tidak dapat dimengerti oleh sembarang orang, kecuali oleh penerima yang berhak. Beberapa cara untuk menangani masalah keamanan ini salah satunya adalah teknik penyandian data yang dikenal dengan ilmu kriptografi.

Kriptografi adalah suatu teknik penyandian data atau penyembunyian informasi yang terkandung pada suatu data dengan cara enkripsi. Penerapan kriptografi pada Tugas akhir ini akan difokuskan bagaimana kriptografi dapat mengamankan data dengan tetap memperhatikan integritas data dan kewenangan setiap pengguna basis data.

Dalam ilmu komputer terdapat beberapa algoritma yang dapat digunakan untuk mengamankan sebuah basis data misalnya MD5, Stream Cipher dan Caesar Cipher. Pada sistem ini algoritma kriptografi yang akan digunakan adalah algoritma Caesar Cipher. Algoritma Caesar cipher akan mengenkripsi plainteks dengan cara menggeser posisi plainteks sebanyak jumlah kunci yang biasanya menggunakan huruf alfabetik dari A – Z saja sehingga mempunyai 26 kunci, namun dalam hal ini penulis melakukan sedikit modifikasi sehingga dapat digunakan untuk mengenkripsi basis data yang terdiri dari huruf, angka dan karakter - karakter lainnya dan penulis menggunakan Kode ASCII dengan memiliki 95 kunci.Berdasarkan informasi tersebut tulisan ini membahas perancangan aplikasi pengamanan basis data menggunakan algoritma Caesar Cipher.

2. METODE PENELITIAN

Dalam penyusunan laporan dibutuhkan data yang sangat akurat dan objektif agar dapat dilaksanakan pembahasan dan pengevaluasian serta penyimpulan untuk lebih mengerti dan memahami isi dari penyusunan laporan tersebut. Di dalam pengumpulan data yang akurat ini, penulis menggunakan beberapa metode untuk memperoleh data tersebut.

2.1. Kriptografi

Kriptografi berasal dari bahasa Yunani, yaitu *cryptos* yang berarti rahasia dan *graphein* yang berarti tulisan. Jadi, kriptografi adalah tulisan rahasia. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya [3]. Atau dalam defenisi yang lainnya kriptografi adalah seni dan ilmu dalam mengamankan pesan [1].

Dalam arti lain, Kriptografi adalah ilmu dan seni yang mempelajari tentang merahasiakan pesan atau informasi kedalam suatu bentuk yang tidak dapat dimengerti sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak berhak.

Kriptografi bertujuan untuk memberi layanan keamanan, yang dinamakan aspek – aspek keamanan yaitu [3]:

1. Kerahasiaan adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak – pihak yang tidak berhak.
2. Integritas data adalah layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman.
3. Otentikasi adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak – pihak yang berkomunikasi.
4. Non-repudiation adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan.

2.2. Algoritma Caesar Cipher

Dalam kriptografi terdapat beberapa algoritma, salah satunya yaitu algoritma Caesar cipher. Sandi Caesar atau sandi geser, kode Caesar atau geseran Caesar adalah sandi substitusi

dimana setiap huruf pada teks terang (plainteks) digantikan oleh huruf lain yang memiliki selisi posisi tertetu dalam alphabet [2]. Caranya adalah dengan mengganti setiap karakter dengan karakter lain dalam susunan abjad (alphabet). Misalnya tiap huruf disubstitusikan dengan huruf yang ketiga berikutnya dari susunan abjad. Misalnya A akan digantikan oleh D dan B akan digantikan oleh E, dan seterusnya. Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu $k = 3$).

Dengan mengkodekan setiap huruf abjad dengan bilangan biner sebagai berikut : A = 0, B = 1,…, Z = 25, maka secara matematis caesar cipher menyandikan plainteks p_i menjadi c_i dengan aturan :

$$c_i = E(p_i) = (p_i+k) \bmod 26$$

dan dekripsi chiperteks c_i menjadi p_i dengan aturan :

$$p_i = D(c_i) = (c_i-k) \bmod 26$$

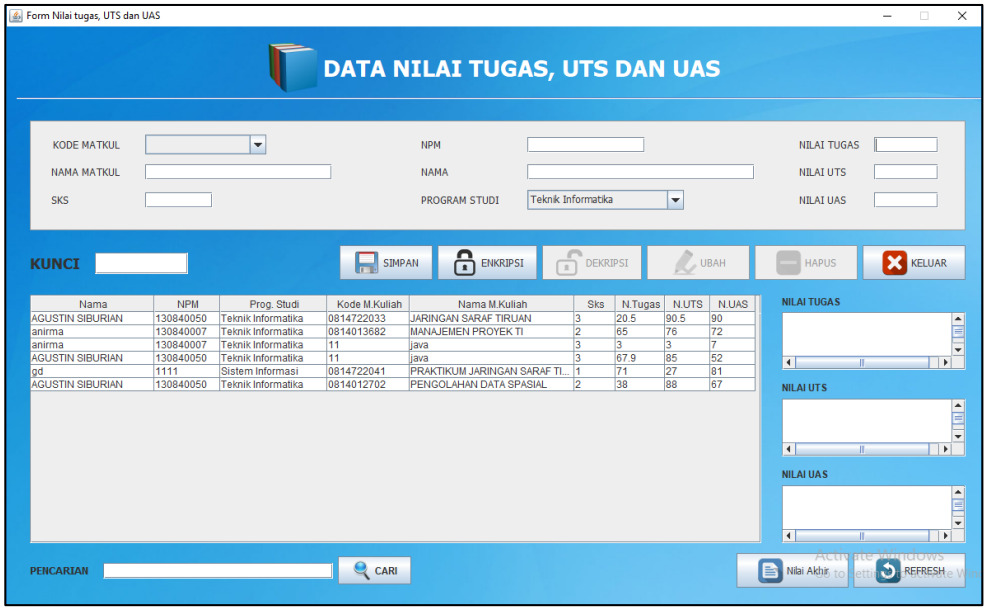
3. HASIL DAN PEMBAHASAN

3.1. Hasil

Sistem ini terdiri dari 7 form, yaitu form login, form utama, form mahasiswa, form matakuliah, form nilai tugas uts dan uas, form nilai akhir dan form tentang penulis. Pada bagian ini disajikan form nilai serta form proses enkrips dan dekripsi.

3.1.1. Form Nilai

Form nilai merupakan form yang digunakan untuk melakukan enkripsi, dekripsi, ubah serta menghapus data nilai mahasiswa. Selain itu dapat digunakan untuk mencari data nilai tiap mahasiswa dan melihat nilai akhir. Tampilan form nilai dapat dilihat pada Gambar 1.



Gambar 1. Form Nilai

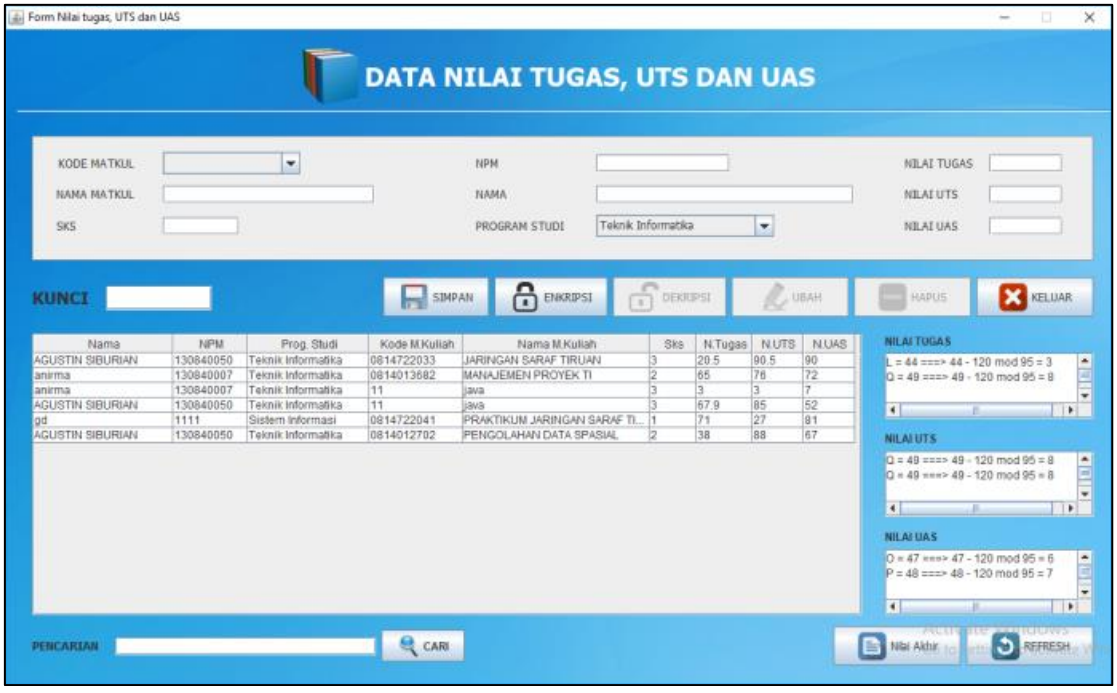
3.1.2. Proses Enkripsi Nilai Mahasiswa

Pada form nilai terdapat tombol enkripsi yang digunakan untuk melakukan proses enkripsi data tersebut. Untuk melakukan proses enkripsi, pengguna harus memasukkan kunci, misalkan kunci yang digunakan adalah "120", setelah mengisi kunci tersebut maka klik tombol enkripsi dan data nilai akan terenkripsi dan tampil di tabel, Seperti pada Gambar 2.

Gambar 2. Tampilan Data Nilai yang di-Enkripsi

3.1.3. Proses Dekripsi Nilai Mahasiswa

Proses dekripsi digunakan untuk mengembalikan cipherteks nilai menjadi nilai awal (plainteks). Untuk melakukan proses dekripsi pengguna harus memasukkan kunci yang digunakan pada proses enkripsi sebelumnya, selanjutnya klik tombol dekripsi maka seluruh cipherteks dari nilai akan kembali ke pada bentuk nilai awal, seperti Gambar 3.



Gambar 3. Tampilan Data Nilai yang di-Dekripsi

3.2. Pembahasan

Berikut ini penulis akan memberikan contoh proses enkripsi dan dekripsi pada basis data. Misalkan plainteks yang akan di enkripsi adalah :

Plainteks = 80.5
Kunci = 5

Maka tahapan-tahapan prosesnya adalah sebagai berikut :

Tahap 1 : Proses Enkripsi

Dilakukan perhitungan plainteks dengan rumus :

p + k mod 95

p : plainteks
k : kunci

Tabel 1. Contoh Perhitungan Proses Enkripsi

Plainteks	Dec	P + k mod 95	Karakter
8	24	24+5 mod 95 = 29	=
0	16	16 + 5 mod 95 = 21	5
.	14	14 + 5 mod 95 = 19	3
5	21	21 + 5 mod 95 = 26	:

Berdasarkan hasil proses enkripsi yang dilakukan, maka diperoleh nilai cipherteks yaitu 53.

Tahap 2 : Proses Dekripsi

Dilakukan perhitungan plainteks dengan rumus :

p - k mod 95
p : plainteks
k : kunci

Tabel 2 Contoh perhitungan proses dekripsi

Cipherteks	Dec	P – k mod 95	Karakter
=	29	29 – 5 mod 95 = 24	8
5	21	21 – 5 mod 95 = 16	0
3	19	19 – 5 mod 95 = 14	.
:	26	26 – 5 mod 95 = 21	5

Berdasarkan hasil proses dekripsi yang dilakukan, maka diperoleh plainteks seperti nilai awal sebelum dilakukan proses enkripsi yaitu 80.5.

4. KESIMPULAN

Berdasarkan hasil penelitian, perancangan, dan pengujian yang telah dilakukan maka penulis memperoleh beberapa kesimpulan, diantaranya adalah sebagai berikut :

1. Algoritma caesar cipher dapat diimplementasikan kedalam koding bahasa pemrograman java.
2. Sistem yang dibangun mampu meningkatkan keamanan basis data dan memberikan kemudahan bagi pengguna dengan menggunakan algoritma caesar cipher.

5. SARAN

Untuk pengembangan lebih lanjut, maka penulis memberikan saran-saran sebagai berikut :

1. Untuk penelitian selanjutnya diharapkan dapat dikembangkan menjadi sistem yang berbasis Web.
2. Penelitian dapat dikembangkan dengan menggunakan atau menambahkan algoritma yang lain, seperti algoritma RSA, Base64, Hill Cipher dan lain-lain.

DAFTAR PUSTAKA

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

[2] Marisman,A.F, dan A.Hidayati. 2015. Pembangunan Aplikasi Pembanding Kriptografi Dengan *Caesar Cipher* dan *Advance Encryption Standart* (AES) Untuk File Teks,*Jurnal Penelitian Komunikasi dan Opini Publik.*Vol.19 No.3

[3] Pabokory,F.N.; I.F.Astuti, dan A.H.Kridalaksana. 2015. Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen dan File Dokumen menggunakan Algoritma *Advanced Encryption Standard*, *Jurnal Informatika Mulawarman.*Vol.10 No.1.