IMPLEMENTASI ALGORITMA CAESAR CIPHER DAN HILL CIPHER PADA *DATABASE* SISTEM INVENTORI TB MITA JEPARA

EGAR DIKA SANTOSA
Program Studi Teknik Informatika - S1, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
JL. Imam Bonjol 207 Semarang 50131
Telp.(024)3517261, Fax(024)3520165
URL : http://dinus.ac.id, email : Dikasantosaegar@gmail.com

ABSTRAK

Perkembangan teknologi informasi berkembang pesat, menyebabkan keamanan data membutuhkan keamanan yang cukup baik. Sekarang setiap orang dapat dengan mudah bertukar informasi dalam hal apapun, termasuk diantaranya adalah berbagi pengetahuan untuk mengakses data secara ilegal. Gudang data dalam tabel *database* telah dipasang sistem login dengan pasword, begitu pula dengan sistem inventori TB Mita. Namun orang jahat mencari cara lain untuk mengakses data tersebut dengan cara mengakses langsung pada tabel *database* tanpa melalui sistem aplikasi tersebut.
Dengan kemungkinan dari akses data ilegal yang mengakses langsung pada tabel *database* tersebut, diperlukan keamanan yang lebih baik terhadap *database* sistem inventori TB Mita. Ada banyak cara yang bisa dilakukan untuk meningkatkan keamanan. Dalam penelitian ini akan menggunakan cara dengan mengenkripsi database dengan algoritma Caesar cipher dan Hill cipher. Caesar cipher dan Hill cipher merupakan bagian dari algoritma simetris, yang artinya pada proses enkripsi dan dekripsi memiliki kunci yang sama. Proses enkripsi dan dekripsi pada algoritma Caesar cipher dan Hill cipher masing-masing memiliki satu kunci, gabungan dari kedua algoritma ini menghasilkan dua kunci sehingga menjadi lebih kuat.

Kata kunci: Caesar cipher, Hill cipher, *Database.*

1. PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan dan kerahasiaan database merupakan salahsatu aspek penting dari suatu sistem informasi. Sebuah informasi hanya ditujukan bagi segolongan tertentu, hal tersebut terkait dengan bagaimana informasi tidak dapat diakses oleh orang yang tidak berhak. Oleh karna itu sangat penting untuk mencegah jatuhnya informasi kepada pihak-pihak lain yang tidak berkepentingan [1].

TB Mita adalah toko bangunan dikota Jepara yang menjual berbagai macam barang bangunan.Pelaksanaan transaksi penjualan pada toko ini sudah memanfaatkan sistem informasi inventori yang menggunakan bahasa pemrograman PHP. Agar dapat memasuki sistem, *user* harus melakukan autentikasi dengan menginputkan *username* dan *password* terlebih dahulu sebagai keamanan untuk mengamankan data pada database. Namun database ini dapat diketahui jika ada orang yang tidak berkepentingan mengakses Mysql secara langsung tanpa harus memasuki sistem inventori TB Mita.

Menurut Wikipedia dalam kriptografi, sandi caesar atau caesar cipher adalah salah satu teknik enkripsi klasik yang terkenal, Sandi ini termasuk sandi subtitusi dimana setiap huruf pada plainteks digantikan oleh huruf lain yang memiliki selisih posisi tertentu.

Hill cipher merupakan salah satu algoritma kriptografi kunci simetris dan merupakan salah satu kripto polyalfabetic. Hill cipher di ciptakan oleh Lester S. Hill pada tahun 1929. Teknik kriptografi ini diciptakan dengan maksud untuk menciptakan cipher yang tidak dapat dipecahkan menggunakan

teknik anlisis frekuensi. Berbeda dengan caesar cipher, Hill cipher tidak mengganti setiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada cipherteks karna menggunakan perkalian matriks pada dasar enkripsi dan dkripsinya.

Dengan menggunakan dan menggabungkan dua algoritma caesar cipher dan Hill cipher ini diharapkan akan menghasilkan algoritma yang lebih kuat.Keduanya metode subtitusi dan metode tranposisi mudah di lakukan dengan komputer, kombinasi dari kedua teknik clasik kriptografi ini menghasilkan keamanan yang lebih dan cipher yang lebih kuat [4].

Caesar cipher dan Hill cipher menggunakan huruf alfabetik dari a-z saja sehingga mempunyai 26 kunci, namun dalam pengimplementasiannya penulis akan menggunakan atau membuat sedikit modifikasi pada sehingga dapat digunakan untuk menenkripsi database yang terdiri huruf dan angka dan beberapa karakter lain. Kedua algoritma ini akan menggunakan 93 karakter dan dapat memperkuat sistem keamanan dari enkripsi caesar cipher normal.

Berdasarkan pertimbangan diatas, maka diperlukan " **Implementasi Algoritma Caesar cipher dan Hill cipher pada Database Sistem Inventori TB Mita Jepara**".

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang yang di kemukakan diatas maka rumusan masalah dalam tugas akhir ini adalah: bagaimana mengimplementasikan algoritma caesar cipher dan Hill cipher untuk keamanan *database* pada sistem inventori TB Mita jepara agar dapat menjadi lebih aman.

1.3 Batasan Masalah

Berdasarkan uraian latar belakang yang di kemukakan diatas maka rumusan masalah dalam tugas akhir ini adalah:

1. Enkripsi caesar cipher dan Hill cipher ini hanya diterapkan pada sistem inventori TB Mita Jepara.
2. Enkripsi caesar cipherdan Hill cipher ini hanya untukmengenkripsi *database* pada sistem inventori TB Mita Jepara.
3. Enkripsi caesar cipherdan Hill cipher ini menggunakan pemrograman PHP.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah diatas maka tujuan dari penulisan tugas akhir ini adalah:

1. Merancang keamanan sistem inventori TB Mita menggunakan enkripsi caesar cipherdan Hill cipher.
2. Membuat enkripsi *database* pada sitem inventori TB Mita supaya menjadi lebih aman digunakan.
3. Merancang enkripsi *database*agar dapat diterapkan pada sitem inventori TB Mita menggunakan PHP.

1.5 Manfaat Penelitian

Adapun manfaat yang dapat diperoleh dalam tugas akhir ini adalah sebagai berikut :

1. Bagi Pembaca
   Dapat dijadikan sebagai acuan untuk melakukan penelitian dengan topic yang serupa maupun sebagai bahan acuan untuk melakukan penelitian lebih lanjut
2. Bagi Penulis
   Penelitian ini digunakan sebagai tugas akhir atau skripsi untuk memenuhi syarat kelulusan Teknik Informatika, Program Sarjana, Universitas Dian Nuswantoro serta menambah pengetahuan dan pengalaman tentang penggunaan enkripsi untuk keamanan *database*.
3. Bagi Akademik
   Mengetahui perkembangan teknologi informasi dengan implementasi Enkripsi untuk keamanan suatu sistem, sehingga menjadi acuan untuk lebih mengenali potensi mahasiswa dengan ilmu pengetahuan lebih luas lagi.
4. Bagi TB Mita
   Penelitian ini dapat memberikan solusi peningkatan keamanan informasi TB Mita Jepara, sehingga informasi yang dimiliki oleh TB Mita Jepara tidak disalahgunakan oleh pihak yang tidak bertanggung jawab.

2. LANDASAN TEORI

2.1 Kriptografi

Kata kriptografi berasal dari bahasa Yunani, *krupto* (tersembunyi) dan *grafh* (tulisan) yang artinya tulisan yang tersembunyi. Kriptografi ilmu yang mempelajari teknik teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan

data, integritas data, serta autentikasi data. Secara umum, kriptografi terdiri atas dua buah bagian utama yaitu bagian enkripsi dan bagian dekripsi.

Enkripsi adalah proses transformasi informasi atau plaintext menjadi bentuk lain sehingga isi pesan yang sebenarnya tidak dapat dipahami atau sering disebut ciphertext, hal ini dimaksudkan agar informasi tetap terlindungi dari pihak yang tidak berhak menerima. Sedangkan dekripsi adalah proses kebalikan dari enkripsi, yaitu transformasi data ke data bentuk semula. Dalam kriptografi terdapat prinsip-prinsip dasar yang harus terpenuhi, yaitu:

a. Kerahasiaan (*confidelity*)
   Layanan kerahasiaan harus menjadikan pesan yang dikirim menjadi tetap rahasia dan tidak diketahui oleh pihak lain kecuali pihak penerima pesan atau pihak yang memiliki ijin. Biasanya haltersebut dilakukan dengan menggunakan suatu algoritma matematis yang mamu mengubah data yang ada menjadi sulit dibaca dan dipahami.
b. Keutuhan data (*data integrity*)
   Merupakan layanan yang dapat mendeteksi atau mengenali jika terjadi perubahan data (penambahan, perubahan, penghapusan) yang dilakuan oleh pihak lain.
c. Otentikasi (*authentication*)
   Layanan ini berhubungan dengan proses identifikasi keaslian data/informasi serta identifikasi pihak-pihak yang terlibat dalam pengiriman data/informasi.
d. Anti penyangkalan (*non-repudiation*)
   Layanan ini mencegah suatu pihak menyangkal aksi yang telah dilakukan sebelumnya.

Dalam kriptografi juga terdapat istilah-istilah, yaitu:

- *Plaintext* (M) adalah pesan yang hendak dikirimkan (berisi data asli).
- *Ciphertext* (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
- *Enkripsi*(fungsi E) adalah proses pengubahan *plaintext* menjadi *ciphertext*.
- *Dekripsi* (fungsi D) adalah mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli.
- *Kunci* adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

Sistem kriptografi yang baik seharusnya tahan terhadap serangan analisis sandi. Analisis sandi atau juga dikenal dengan istilah *Criptanalysis* merupakan ilmu yang mempelajari tentang cara memecahkan teks sandi sehingga akan didapat teks yang asli beserta kunci rahasianya. Apabila terdapat *cipher*t*ext*dapat berubah menjadi *plaintext* dengan menggunakan kunci yg benar maka proses tersebut dinamakan *breaking code* sedangkan yang melakukannya adalah *cryptanalyst.*

Berdasar kunci yang dipakai, kriptografi dapat dibedakan menjadi dua bagian yaitu:

1. Algoritma Simetrik (*Symmetric Algorithms*)
   Algoritma simetris disebut juga sebagai algoritma konvensional. Algoritma simetris menggunakan menggunakan suatu kunci yang sama untuk proses enkripsi dan dekripsi. Penggunaan kunci yang sama menjadikan kekuatan algoritma simetrik menjadi sangat bergantung pada satu kunci yang digunakan, selain itu proses dekripsi pada algoritma simetrik juga menjadi kebalikan dari proses enkripsi. Apabila pengeriman kunci dapat dilakukan secara aman, akan menjadikan kesempatan *cryptanalyst* untuk mendapatkan *ciphertext* dan *plaintext* semakin kecil.
   Terdapat dua tipe dasar dalam algoritma asimetrik yaitu *Steam Cipher* dan *Block Cipher*.Proses pada *Steam Cipher* akan lebih mudah untuk diimplementasikan dalam *hardware* karena menggunakan pengkodean 1 bit atau byte dalam satukali proses. Sedangkan *hardware* bekerja berdasarkan bit-bit yang menjadi satuan terkecilnya dalam melakukan proses perhitungan. Dalam *Steam Cipher*, *plaintext* atau byte yang sama akan dienkripsi kedalam byte yang berbeda pada setiap enkripsinya.Pada proses *Block Cipher* akan melakukan pengkodean pada 1 block dalam sekali proses. Umumnya ukuran block yang digunakan akan memenuhi rumus 2^ndengan n adalah bilangan integer dan ukuran blocknya dapat ditentukan sesuai keinginan.
2. Algoritma Asimetrik (*Asymetric Algorithms*)

Kunci public (*public key*) yang merupakan nama lain dari algoritma asimetrik. Enkripsi dan dekripsi pada algoritma asimetrik menggunakan kunci yang berbeda.Kunci dalam algoritma asimetrik dibagi menjadi dua yaitu kunci umum (*public key*) dan kunsi pribadi (*private key*).

Pada kunci umum, kunci tersebut dapat diketahui oleh semua orang (*public*).Sedangkan pada kunci pribadi hanya dapat diketahui oleh orang yang bersangkutan.Penggunaan kunci umum memungkinkan seseorang untuk dapat mengenkripsi suatu pesan tetapi tidak dapat mendeskripsikan pesan tersebut.Hanya orang yang memiliki kunci pribadi yang dapat mendeskripsikan pesan yang telah dienkripsi.Sehingga keedua kunci tersebut (kunci umum dan kunci pribadi) harus saling berhubungan satu dengan yang lainnya.

2.2 Algoritma Caesar Cipher

Dalam kriptografi, sandi Caesar, atau sandi geser, kode Caesar atau Geseran Caesar adalah salah satu teknik enkripsi paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet.

Ini adalah algoritma kriptografi yang mula-mula digunakan oleh kaisar Romawi, Julius Caesar (sehingga dinamakan juga *caesar chiper*), untuk menyandikan pesan yang ia kirim kepada para gubernurnya.

Caranya adalah dengan mengganti (menyulih atau mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet). Misalnya, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan akjad. Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu $k = 3$).

Dengan mengkodekan setiap huruf abjad dengan *integer* sebagai berikut: $A = 0$, $B = 1$, …, $Z = 25$, maka secara matematis *caesar chiper* 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:

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

Karena hanya ada 26 huruf abjad, maka pergeseran huruf yang mungkin dilakukan adalah dari 0 sampai 25. Secara umum, untuk pergeseran huruf sejauh k (dalam hal ini k adalah kunci enkripsi dan deksripsi), fungsi enkripsi adalah

$$c_i = E(p_i) = (p_i + 3) \bmod 26$$

dan fungsi dekripsi adalah

$$p_i = D(c_i) = (c_i - 3) \bmod 26$$

Setiap huruf yang sama digantikan oleh huruf yang sama di sepanjang pesan, sehingga sandi Caesar digolongkan kepada, substitusi monoalfabetik.

2.3. Algoritma Hill Cipher

Hill cipher diperkenalkan pertama kali pada tahun 1929 oleh Letser S.Hill. Proses enkripsi dan dekripsi pada Hill cipher menggunakan oprasi perkalian matriks atas ring Z26. Ide dasar dari Hill adalah untuk membuat kombinasi linier dari plaintext untuk mendapatkan ciphertext. Kunci yang digunakan berupa matriks persegi z26 yang determinan nya invertibel pada z26 [4].

Hill cipher termasuk dalam salah satu kriptosistem polialfabetik, artinya setiap karakter alfabetbisa dipetakan ke lebih dari satu macam karakter alfabet. Cipher ini ditemukan pada tahun 1929 oleh Lester S. Hill. Misalkan m adalah bilangan bulat positif, dan P = C = (Z26)m.

Ide dari Hill cipher adalah dengan mengambil m kombinasi linier dari m karakter alfabet dalam satuelemen plaintext, sehingga menghasilkan m alfabet karakter dalam satu elemen plaintext.Misalkan m = 2, maka dapat ditulis suatu elemen plaintext sebagai x = (x1, x2) dan suatuelemen ciphertext sebagai y = (y1, y2). Di sini, y1, y2 adalah kombinasi linier dari x1 dan x2.misalkan

$y1 = 11x_1 + 3x_2$

$y2 = 8x_1 + 7x_2$

maka dapat ditulis dalam notasi matriks sebagai berikut:

$$(y_1, y_2) = (x_1, x_2) \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$$

Secara umum, dengan menggunakan matriks K m x m sebagai kunci. Jika elemen pada baris idan kolom j dari matriks K adalah ki,j, maka dapat ditulis K = (ki,j).

Untuk x = (x1, …, xm) ∈Pdan K ∈*K*, di hitung y = eK(x) = (y1, …, ym) sebagai berikut:

$$(y_1, y_2, ..., y_m) = (x_1, x_2, ..., x_m) \begin{pmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,m} \\ k_{2,1} & k_{2,2} & \cdots & k_{2,m} \\ \vdots & \vdots & & \vdots \\ k_{m,1} & k_{m,2} & \cdots & k_{m,m} \end{pmatrix}$$

Gambar 2.2. Perkalian Matriks Hill Cipher

$(y_1, y_2,...,y_m) = (x_1, x_2,...,x_m) \begin{pmatrix} k1,1 & \cdots & k1,m \\ \vdots & \ddots & \vdots \\ km,1 & \cdots & km,m \end{pmatrix}$

dengan kata lain, y = xK.

Dikatakan bahwa ciphertext diperoleh dari plaintext dengan cara *transformasi linier*.Untuk melakukan dekripsi dengan menggunakan matriks invers K-1. Jadi dekripsi dilakukandengan rumus x = yK-1.

3. METODE PENELITIAN

Pada pembangunan sistem penulis menggunakan basis *System Development Life Cycle* (SDLC) dan dengan metode waterfall. SDLC (Software Development Life Cycle) merupakan sebuah siklus hidup pengembangan perangkat lunak yang terdiri dari beberapa tahapan-tahapan penting dalam membangun perangkat lunak yang dilihat dari segi pengembangannya. Dengan siklus SDLC, proses membangun sistem dibagi menjadi beberapa langkah dan pada sistem yang besar, masing-masing langkah dikerjakan oleh tim yang berbeda.

Tahapan tahapan yang digunakan dalam penelitian ini :

1. Tahap Perencanaan
   Tahap ini mengenali dan menganalisa masalah serta mendefinisikan masalah yang diterima pemakai. Dalam hal ini adalah masalah keamanan database.
   Data yang tersimpan di dalam basis data harus dapat terjamin keamanannya. Pengamanan data dapat dilakukanmelalui dua cara. Cara pertama ialah pengaturan hak akses setiap pengguna oleh administrator basis data. Carakedua ialah pengamanan data dari sisi kandungan data yang tersimpan pada basis data [7].
   Kegiatan yang dilakukan adalah :
   Dalam pengembangan sistem yang pertama dilakukan adalah perencanaan dengan melakukan pengumpulan data dan sumber-sumber informasi terkait. Kemudian melakukan pembelajaran atau pemahaman pada algoritma kriptografi Caesar Cipher dan Hill Cipher dan juga memahami dasar dasar dari pemrograman *php* dan *html.*
2. Tahap Analisa
   Tahap ini proses pencarian kebutuhan di intensifkan dan di fokuskan pada software. Untuk mengetahui sifat dari program yang akan dibuat maka para software engineer harus mengerti tentang domain informasi dari software, misalnya bagaimana menentukan bilangan prima, menentukan kunci yang dipakai pada setiap algoritma enkripsi, menentukan kunci invers pada Hill Cipher.
3. Tahap Desain
   Merupakan pengembangan , perencanaan, pembuatan desain atau pengetesan dari berbagai elemen yang terpisah dalam suatu kesatuan yang utuh dan berfungsi. Tahap ini menyangkut konfigurasi komponen-komponen perangkat lunak dan perangkat keras dari suatu sistem sehingga setelah instlisasi sistem akan benar benar memuaskan rancang bangun yang telah ditetapkan pada tahap analisis sistem.
   Kegiatan yang dilakukan adalah :
   Menyiapkan rancangan bentuk program Kriptografi file menggunakan algoritma Caesar cipher dan Hill cipher dan dengan menggunakan pemrograman *php*.
4. Tahap Implementasi
   Implementasi dari penerapan Caesar cipher dan Hill cipher untuk keaman *database,* akan dibangun menggunakan bahasa pemrograman PHP. Adapaun tools yang akan digunakan adalah Adobe Dreamweaver, notepad, XAMPP, browser. Rancangan program kriptografi file dengan menggunakan algoritma Caesar cipher dan Hill cipher dan unit unit sistem inventori yang telah dibuat untuk kemudian disisipkan ke sistem inventori tersebut.
5. Setelah tahapan implementasi selesai akan dilanjutkan dengan tahapan pengujian.
   Pengujian yang dilakukan akan menggunakan pengujian *black-box testing. Black-box testing*merupakan pengujian suatu perangkat lunak atau sistem dengan menguji secara fungsional berdasarkan pada spesifikasi kebutuhan perangkat lunak. *Black-box testing*melakukan

pengujian tanpa mengetahui struktur internal dari sistem atau komponen yang diuji.

Pengujian menggunakan *black-box testing* bertujuan untuk mendapatkan beberapa hasil diantaranya :

- Fungsi yang hilang atau tidak benar
- Kasalahan dari struktur data atau eksternal *database*
- Kesalahan dari inisialisasi dan terminasi
- Kesalahan dari antarmuka

Teknik pengujian *black-box testing*berfokus pada domain informasi dari perangkat lunak dengan melakukan *test case* yang mempartisi domain input dari suatu program dengan cara yang memberikan cakupan pengujian yang mendalam. Langkah-langkah yang akan dilakukan dalam menguji keamanan *database*pada TB Mita adalah:

1. Membuka sistem inventori TB Mita
2. Membuka tabel dan *database* dari sistem
3. Data *database* langsung dapat dilihat

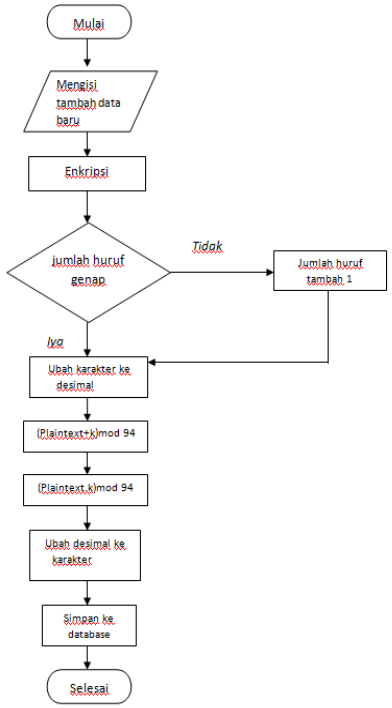
Sedangkan untuk pengujian keamanan database yang telah ter enkripsi menggunakan Caesar cipher dan Hill cipher pada TB Mita adalah :

1. Membuka sistem inventori TB Mita
2. Membuka sistem inventori TB Mita
3. Data *database* langsung di akses namun hanya berupa data enkripsi yang tidak memiliki arti.

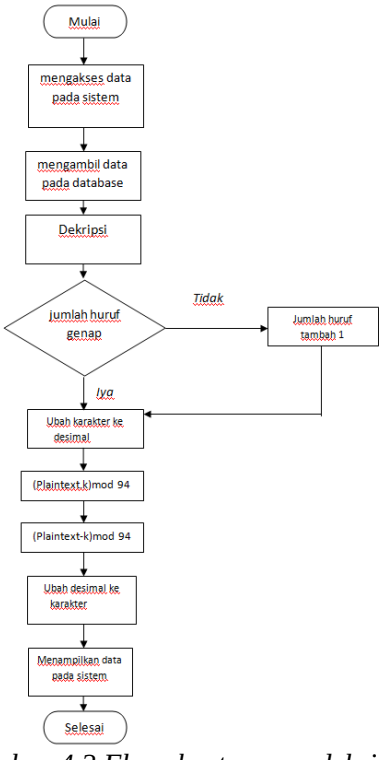
4. IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi

Untuk menyipan suatu data baru atau *plaintext* yang akan di inputkan kedalam sistem, maka data di enkripsi terlebih dahulu oleh fungsi enkripsi.php menjadi sebuah *ciphertext* lalu di simpan pada *database*, untuk menjaga kerahasiaan isi dari *database* itu sendiri agar pada saat *database* di akses tanpa melalui sistem data tidak dapat terbaca. Gambar Flowchart alur data setelah implementasi algoritma Caesar cipher dan Hill cipher :



Gambar 4.1 Flowchart proses enkripsi



Gambar 4.2 Flowchart proses dekripsi

4.2 Proses Enkripsi

Masukan data untuk di inputkan kedalam sistem, nantinya data inilah yang akan di enkripsi dan kemudian disimpan kedalam database. Untuk contoh maka kita gunakan data seperti contoh diatas.

Gambar 4.3 Tampilan form input data baru

Setelah tombol simpan di jalankan maka terjadilah proses enkripsi, untuk proses enkripsinya adalah sebagai berikut.

Datanya adalah sebagai berikut
- BRG002
- 4p obeng
- 20
- 15
- 8000
- 4250
- PT.CSA

Setiap data di atas akan di enkripsi per field nya.

1. Pertama data akan di cek nilai decimalnya sesuai kamus ASCII yang digunakan :
   - BRG002 = 34, 50, 39, 16, 16, 18
   - 4p obeng = 20, 48, 0, 79, 66, 69, 78, 71
   - 20 = 18, 16
   - 15 = 17, 21
   - 8000 = 24, 16, 16, 16
   - 4250 = 20, 18, 21, 16
   - PT.CSA = 48, 52, 14, 35, 51, 33

2. Setelah didapatkan nilai desimalnya data akan di cek apakah jumlah data ganjil atau genap, jika ganjil maka akan ditambahkan karakter ”spasi” yang dimana nilai desimal nya adalah 0.
3. Setelah data di cek maka di enkripsi dengan Caesar cipher terlebih dahulu, sesuai dengan pembahasan pada bab bab sebelumnya.
   Dengan rumus
   $c_i = E(p_i) = (p_i + K) \bmod 94$
   K adalah 3.
   - ((34,50,39,16,16,18)+3)mod94 = 37, 53, 42, 19, 19, 21
   - ((20,48,0,79,66,69,78,71)+3)mod94 = 23, 51, 3, 82, 69, 72,81, 74
   - ((18,16)+3)mod94 = 21, 19
   - ((17,21)+3)mod94 = 20, 24
   - ((24,16,16,16)+3)mod94 = 27, 19, 19, 19
   - ((20,18,21,16)+3)mod94 = 23, 21, 24, 19
   - ((48,52,14,35,51,33)+3)mod94 = 51, 55, 17, 38, 54, 36

4. Setelah ditemukan nilai hasil enkripsi Caesar ciphernya maka di lanjut untuk enkripsi hill cipher, dengan rumus
   Y = X . K mod94
   K adalah = $\begin{bmatrix} 2 & 7 \\ 3 & 11 \end{bmatrix}$
   Setiap karakter di masukan kedalam matriks dengan format sebagai berikut:
   $$\begin{pmatrix} X1,1 & X2,1 & Xn,n \\ X1,2 & X2.2 & Xn,n \end{pmatrix}$$
   - Maka dari text BRG002 :
   $\begin{pmatrix} 34 & 42 & 19 \\ 53 & 19 & 21 \end{pmatrix} \begin{pmatrix} 2 & 7 \\ 3 & 11 \end{pmatrix}$ mod94
   Hasilnya 69, 36, 29, 53, 91, 6 ~> eD=U{&
   - Maka dari text 4P obeng :
   $\begin{pmatrix} 23 & 3 & 69 & 81 \\ 51 & 82 & 72 & 74 \end{pmatrix} \begin{pmatrix} 2 & 7 \\ 3 & 11 \end{pmatrix}$ mod94
   Hasilnya 12, 66, 16, 65, 78, 59, 22, 23 ~> ;b0an[67
   - Maka dari text 20 :
   $\begin{pmatrix} 21 \\ 19 \end{pmatrix} \begin{pmatrix} 2 & 7 \\ 3 & 11 \end{pmatrix}$ mod94
   Hasilnya 81, 84 ~> qt
   - Maka dari text 15 :
   $\begin{pmatrix} 20 \\ 24 \end{pmatrix} \begin{pmatrix} 2 & 7 \\ 3 & 11 \end{pmatrix}$ mod94
   Hasilnya 20, 42 ~> 4J
   - Maka dari text 8000 :
   $\begin{pmatrix} 27 & 19 \\ 19 & 19 \end{pmatrix} \begin{pmatrix} 2 & 7 \\ 3 & 11 \end{pmatrix}$ mod94
   Hasilnya 5, 18, 87, 93 ~> %2w}
   - Maka dari text 4250 :
   $\begin{pmatrix} 23 & 24 \\ 21 & 19 \end{pmatrix} \begin{pmatrix} 2 & 7 \\ 3 & 11 \end{pmatrix}$ mod94
   Hasilnya 93, 8, 77, 78 ~> }9mn

- Maka dari text PT.CSA :

$$\begin{bmatrix}51 & 17 & 54\\ 55 & 38 & 36\end{bmatrix}\quad\begin{bmatrix}2 & 7\\ 3 & 11\end{bmatrix}\ \text{mod94}$$

Hasilnya 17, 6, 18, 93, 78, 88~> 1&2}nx

4. Maka setelah melewati proses enkripsi data Caesar cipher dan hill cipher data disimpan ke database sepeti pada gambar di bawah

id_persediaan	nama_barang	kode_barang	jumlah_barang	jumlah_minimal	harga_beli	harga_jual	grosir
9	;b0an[67	eD=U{&	qt	4J	}(mn	%2w}	1&2}nx

Gambar 4.4 Database setelah di enkripsi

Pada proses enkripsi dalam sistem ini dibuat bentuk penkodean yang berfungsi untuk mengamankan data yang nantinya akan disimpan dalam *database*. dalam implementasi ini terdapat dua tahap proses yang di implementasikan yaitu proses enkripsi dan proses dekripsi. Kedua proses ini merupakan implementasi dari algoritma caesar cipher dan hill cipher yang di implementasikan kedalam bahasa PHP.

4.3 Proses Dekripsi

Dari data- data ini kita dekripsi seperti di bawah ini

eD=U{&
;b0an[67
qt
4J
%2w}
}(mn
1&2}nx

Maka kita deskripsikan dengan Hill cipher terlebih dahulu.

Dekripsi dengan hill, rumusnya sebagai berikut

$Y = X \cdot K^{-1} \bmod 94$

K^{-1} adalah $= \begin{bmatrix}11 & 87\\ 91 & 2\end{bmatrix}$

K^{-1} adalah invers dari K.

Cari nilai decimal dari masing masing karakter :

eD=U{& = 69, 36, 29, 53, 91, 6
;b0an[67 = 12, 66, 16, 65, 78, 59, 22, 23
qt = 81, 84
4J = 20, 24
%2w} = 5, 18, 87, 93
}(mn = 93, 8, 77, 78
1&2}nx = 17, 6, 18, 93, 78, 88

1. Setelah ketemu nilai desimalnya kita mulai proses dekripsinya
   - Maka dari text eD=U{&

$$\begin{bmatrix}69 & 29 & 91\\ 36 & 53 & 6\end{bmatrix}\begin{bmatrix}11 & 87\\ 91 & 2\end{bmatrix}\ \text{mod94}$$

hasilnya 37, 53, 42, 19, 19, 21

- Maka dari text ;b0an[67

$$\begin{bmatrix}12 & 16 & 78 & 22\\ 66 & 65 & 59 & 23\end{bmatrix}\quad\begin{bmatrix}11 & 87\\ 91 & 2\end{bmatrix}\ \text{mod94}$$

hasilnya 23, 51, 3, 82, 69, 72, 81, 74

- Maka dari text qt

$$\begin{bmatrix}81\\ 84\end{bmatrix}\quad\begin{bmatrix}11 & 87\\ 91 & 2\end{bmatrix}\ \text{mod94}$$

hasilnya 21, 19

- Maka dari text 4J

$$\begin{bmatrix}20\\ 42\end{bmatrix}\quad\begin{bmatrix}11 & 87\\ 91 & 2\end{bmatrix}\ \text{mod94}$$

Hasilnya 20, 24

- Maka dari text%2w}

$$\begin{bmatrix}5 & 87\\ 18 & 93\end{bmatrix}\quad\begin{bmatrix}11 & 87\\ 91 & 2\end{bmatrix}\ \text{mod94}$$

Hasilnya 27, 19, 19, 19

- Maka dari text }(mn

$$\begin{bmatrix}93 & 77\\ 8 & 78\end{bmatrix}\begin{bmatrix}11 & 87\\ 91 & 2\end{bmatrix}\ \text{mod94}$$

Hasilnya 23, 21, 24, 19

- Maka dari text 1&2}nx :

$$\begin{bmatrix}17 & 18 & 78\\ 6 & 93 & 88\end{bmatrix}\quad\begin{bmatrix}11 & 87\\ 91 & 2\end{bmatrix}\ \text{mod94}$$

Hasilnya 51, 55, 17, 38, 54, 36

2. Hasil dari dekripsi hill cipher di atas di dapatkan nilai decimal yang kemudian di dekripsi kembali dengan caesar cipher.

Dengan rumus

$p_i = D(c_i) = (c_i - 3) \bmod 94$

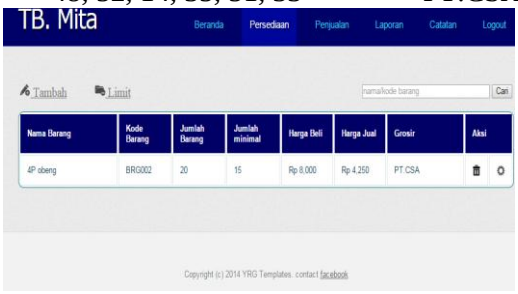
maka

((37,53,42,19,19,21)-3)mod94 =34,50,39, 16, 16, 18
((23,51,3,82,69,72,81,74)-3)mod94=20,48, 0,79,66,69,78,71
((21,19)-3)mod94 = 18, 16
((20, 24) -3)mod94 = 17, 21
((27, 19, 19, 19) -3)mod94 = 24, 16, 16, 16
((23, 21, 24, 19) -3)mod94 = 20, 18, 21, 16
((51,55,17,38,54,36)-3)mod94=48,52, 14,35, 51, 33

Setelah berhasil di dekripsi sekarang saatnya di konversi kembali kedalam karakter sesuai kamus ASCII

- 34, 50, 39, 16, 16, 18 ~> BRG002
- 20, 48, 0, 79, 66, 69, 78, 71 ~> 4p obeng
- 18, 16 ~> 20

- 17, 21 ~>15
- 24, 16, 16, 16 ~> 8000
- 20, 18, 21, 16 ~> 4250
- 48, 52, 14, 35, 51, 33 ~> PT.CSA

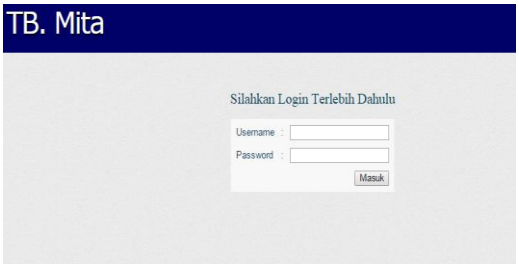


Gambar 4.5 Gambar database yang telah di dekripsi

4.3 Pengujian

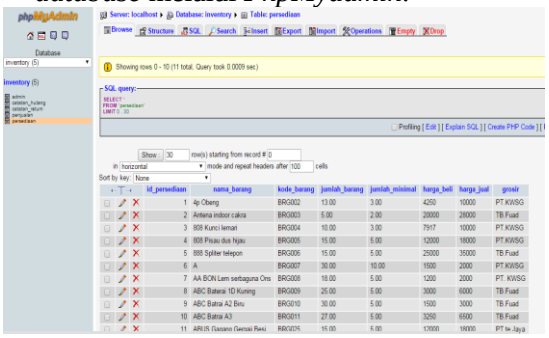
Adapun langkah- langkah yang akan dilakukan untuk menguji keamanan database pada TB Mita Jepara adalah:

1. Membuka Sistem inventori TB MITA



Gambar 4.14 Login TB Mita inventori

2. Karna tidak memiliki Login dan Password, maka mengakses secara langsung pada *database* melalui *PhpMyadmin*.



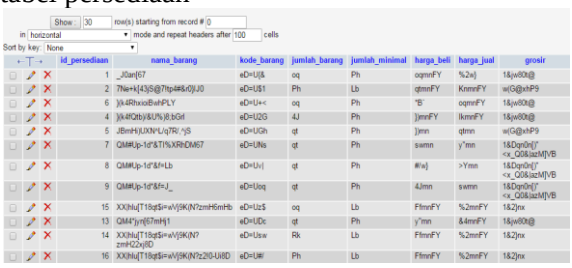
Gambar 4.15 Database Sistem

3. Pada gambar diatas kita dapat melihat salahsatu tabel *database* yaitu tabel persediaan yang dapat di akses dengan mudah.

   Sedangkan Langkah- langkah yang akan digunakan untuk menguji keamanan database dari sistem inventori setelah menggunakan implementasi algoritma Caesar cipher dan Hill cipher sebagai berikut:

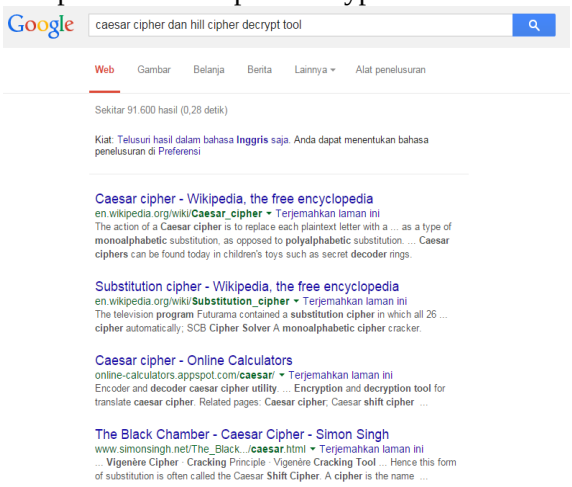
   1. Membuka PhpMyAdmin dan mengakses *database*

2. Membuka *database* sistem dan mengakses tabel persediaan



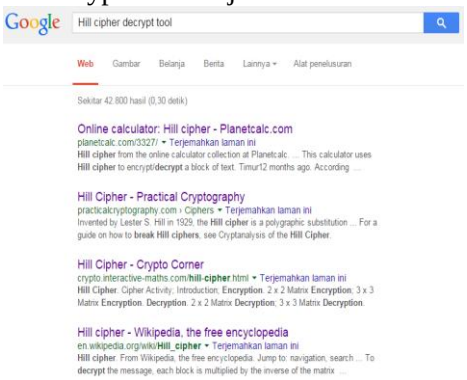
Gambar 4.16 Database setelah enkripsi

3. Pada gambar 4.15 dapat ditunjukan bahwa database dari persediaan telah terenkripsi dan tidak memiliki makna yang berarti, namun untuk selanjutnya dilakukan pengujian untuk apabila *database* ini di dekripsi menggunakan program dekripsi yang ada pada internet.
4. Membuka internet dan *searchengine*.
5. Karna algoritma enkripsi ini adalah Caesar cipher dan Hill cipher maka ketikan "caesar cipher dan hill cipher decrypt tool"

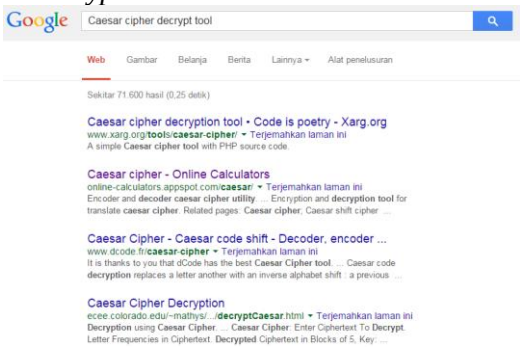


Gambar 4.17 Pencarian Caesar cipher and hill cipher decript

6. Pada gambar diatas tidak ditemukan alat atau program dekripsi otomatis dari Caesar cipher dan Hill cipher.
7. Ganti kata kunci pada search engine "Hill cipher decrypt tool" atau "Caesar cipher decrypt tool " saja.

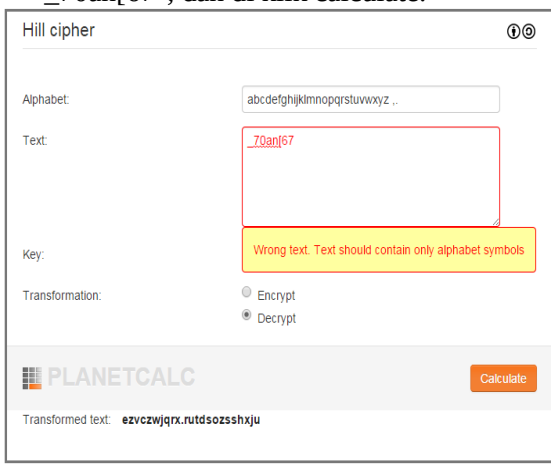


Gambar 4.18 hasil pencarian Hill cipher decrypt tool



Gambar 4.19 hasil pencarian Caesar cipher decryp tool

8. Kita ambil salah satu untuk enkripsi hill cipher, pada contoh ini akan menggunakan http://planetcalc.com/3327/.
9. Masukan salah satu data yg ada pada field database untuk di enkripsikan yaitu "_70an[67", dan di klik calculate.



Gambar 4.20 uji coba Hill cipher

Pada gambar 4.20 kita memasukan salah satu data yg ada pada *fielddatabase* untuk di enkripsikan yaitu "_70an[67", dan ketika di klik *calculate* terjadi error dan gagal utuk dekripsi. Hal ini terjadi karna jumlah kamus karakter yang digunakan dan kunci yang digunakan adalah berbeda, sehingga program gagal atau tidak bisa mendeskripsinya.

10. kita ambil salah satu situs program dekrip tools yaitu http://www.dcode.fr/caesar-cipher.
11. Masukan salah satu data yg ada pada field database untuk di enkripsikan yaitu "_70an[67", dan di klik *decrypt*.

Gambar 4.21 uji coba Caesar cipher

Pada gambar 4.21 kita memasukan salah satu data yg ada pada *fielddatabase* untuk di enkripsikan yaitu "_70an[67", dan ketika di klik *decrypt* menghasilkan *plaintext* yaitu "_70xk[67", dan hasilnya berbeda yang seharusnya menjadi "4P obeng". Hal ini terjadi karnawalaupun jumlah kunci yang digunakan benar namun jumlah kamus karakter yang digunakan berbeda, sehingga program gagal atau tidak bisa mendeskripsinya.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan Hasil dari perancangan dan Implementasi algoritma Caesar cipher dan Hill cipher pada *database* sistem inventori, serta hasil pengujian yang telah dilakukan dapat disimpulkan bahwa :

1. Fungsi Algoritma Caesar cipher dan Hill cipher dapat di implementasikan kedalam koding bahasa pemrograman PHP.
2. Algoritma Caesar cipher dan Hill cipher dapat di imlementasikan ke dalam sistem Inventori dengan baik.
3. Perancangan keamanan *database* sistem inventori TB Mita dengan algoritma Caesar cipher dan Hill cipher dapat meningkatkan keamanan dari *database* sistem.

5.2 Saran

Dari hasil penelitian implementasi algoritma Caesar cipher dan Hill cipher pada sistem inventori TB Mita ini, dihasilkan beberapa saran yang dapat diperhatikan supaya dapat menjadi lebih baik kedepannya diantaranya adalah sebagai berikut :

1. Implementasi algoritma untuk keamanan database dapat menggunakan kemungkinan algoritma lain.
2. Penerapan algoritma Caesar cipher dan Hill cipher untuk keamanan database dapat dijadikan referensi untuk dikembangkan menjadi keamanan *database* yang lebih baik.
3. Penerapan algoritma Caesar cipher dan Hill cipher tidak hanya dapat diterapkan pada *database* sistem inventori TB Mita namun juga dapat diterapkan pada sistem lain.

DAFTAR PUSTAKA

[1] Antonius Wahyu Sudrajat, "Implementasi Enkripsi Database Menggunakan

Transparent Data Encription Pada Database Engine Oracle," *Jurnal Ilmiah STMIK GI MDP*, vol. 2, no. 3, Oktober 2006.

[2] Novi Dian Nathasia, Anang Eko Wicaksono, "Penerapan Teknik Kriptografi Stream Cipher Untuk Pengaman Basis Data," *Jurnal Basis Data*, vol. 6, no. 1, p. 22, Mei 2011.

[3] M Didik R Wahyudi, "Enkripsi Field Database Dengan PGP," *Jurnal Teknologi*, vol. 2, no. 1, p. 7, Juni 2009.

[4] Anupama Mishra, "Enhancing Security of Caesar Cipher Using Different Method," *International Journal of Research in Engineering and Technology*, vol. 02, p. 332, september 2013.

[5] Rinaldi Munir, *Kriptografi*. Bandung, Indonesia: Penerbit Informatika, 2006.

[6] Malay B Pramanik, "Implementation of Criptography Technicue Using Columnar Transposition," *International Jurnal of Computer Aplication*, january 2014.

[7] Saipul Bahri, Diana, Susan Dian PS, "Studi dan Implementasi Pengamanan Basis Data Menggunakan Metode Enkripsi MD5," *Jurnal Ilmiah*, vol. x, no. x, April 2012.

[8] Zulkifli, "Model Prediksi Berbasis Neural Network untuk Pengujian Perangkat Lunak Metode Blackbox," *Seminar Nasional Aplikasi Teknologi informasi*, juni 2013.

[9] Bambang Sugiarto, Jazi Eko Istianto, "Analisa Keamanan Database Server Menggunakan Teknologi Virtual Private Database dan Notifikasi Database Server Menggunakan Agent Bergerak," *Seminar Nasional Informatika* , Mei 2010.