KEAMANAN DATABASE NOTA PENJUALAN DENGAN ALGORITMA AFFINE CIPHER DAN WAKE BERBASIS WEB

Anjar Imam Prasetyo[1)], Pipin Farida Ariyani[2)]
Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Email: *anjarimamp@gmail.com[1)], pipin.faridaariyani@budiluhur.ac.id[2)]*

Abstrak

Keamanan database merupakan hal yang esensial bagi perusahaan, karena informasi database yang ada pada perusahaan juga merupakan sebuah asset bagi perusahaan itu sendiri. Semakin informasi database tersebut terjaga keamanannya, maka tingkat kepercayaan dari perusahaan tersebut juga semakin tinggi. Khususnya untuk GROSIR SPREI JAKARTA, Karena banyak menyimpan data – data informasi tentang tertanggung yang harus dijaga keamanannya dari pihak yang tidak berwenang, karena database masih bisa diakses oleh seluruh staff. Masalah tersebut dapat diatasi dengan menggunakan teknik kriptografi yaitu dengan algoritma Affine Cipher dan WAKE untuk menjaga kerahasiaan database. Perancangan proses aplikasi dimulai dengan mengenkripsi database menggunakan algoritma Affine cipherdan WAKE, kemudian dilakukan proses pembangkitan kunci oleh penerima untuk memperoleh nilai N (hasil perkalian dua bilangan prima), kunci public dan kunci private. Aplikasi yang dibuat merupakan aplikasi berbasis web dengan menggunakan bahasa pemrograman PHP dan MySQL sebagai basis data. Dari penelitian ini disimpulkan bahwaa plikasi ini dapat mengenkripsi dan mendekripsi database. Aplikasi dapat berjalan dengan baik dalam mengenkripsi dan mendekripsi database. Dengan adanya aplikasi enkripsi ini, database dapat terjaga kerahasiaannya, karena data hanya dapat didekripsi dengan aplikasi yang sama yang hanya dapat diakses oleh pengguna yang sudah didaftarkan.

Kata Kunci: *Kriptografi, Database, Affine Cipher, WAKE*.

1. PENDAHULUAN

Keamanan *database* merupakan hal yang esensial bagi perusahaan. Setiap data yang tersimpan harus dijaga agar semua informasi tentang perusahaan aman, artinya semua informasi tersebut tidak bisa dengan mudah diakses oleh semua orang yang ada di dalam perusahaan terutama *database*, tetapi hanya orang - orang yang mempunyai otoritas ataupun kewenangan yang bisa mengaksesnya.

Selain itu, *database* yang ada pada perusahaan juga merupakan sebuah aset bagi perusahaan itu sendiri. Semakin *database* tersebut terjaga keamanannya maka tingkat kepercayaan dari perusahaan tersebut juga semakin tinggi. Kehilangan maupun tersebarnya informasi *database* kepada pihak eksternal yang tidak mempunyai kepentingan, akan menyebabkan kerugian bagi perusahaan. Dampak lainnya, keberlangsungan bisnis perusahaan mungkin tidak akan bertahan.

GROSIR SPREI JAKARTA adalah perusahaan atau kewirausahaan kecil yang bergerak dibidang penjualan sprei dan produksi sprei. Grosir Sprei Jakarta ini sudah berdiri sejak tahun 2015, hingga saat ini sudah berkembang cukup baik seiring berkembang teknologi, khususnya dipenjualan *online*. Pada prosesnya penulis mendapati celah yang berpotensi bocornya informasi *database*. Pengamanan terhadap jaringan komputer yang terhubung dengan *database* sudah tidak lagi menjamin keamanan data karena kebocoran *database* dapat disebabkan oleh pihak – pihak yang langsung berhubungan dengan *database* seperti administrator *database*. Dalam hal ini data barang dan data pelanggan, untuk mendukung hal tersebut maka dibutuhkan keamanan informasi yang baik agar kredibilitas dan citra perusahaan terjaga dimata publik dan klien.

Melihat dari permasalahan yang ada, maka penulis mengusulkan untuk membuat suatu aplikasi atau program web yang mampu mengamankan informasi berbasis data pada Grosir Sprei Jakarta, yaitu dengan cara mengenkripsi *database* menggunakan dua algoritma, yaitu algoritma *Affine Cipher* dan Algoritma *Word Auto Key Encryption* (WAKE).

Berdasarkan uraian latar belakang diatas, dirumuskan masalah dalam penelitian ini yaitu, bagaimana cara mengamankan basis data dari pihak yang tidak bertanggung jawab dengan cara mengimplementasikan kriptografi menggunakan algoritma Affine Cipher dan algoritma WAKE *(Word Auto Key Encryption)*.Bagaimana membuat aplikasi atau program web yang aman dan mudah digunakan oleh pengguna.

Berdasarkan latar belakang dan permasalahan yang dihadapi maka dibutuhkan solusi, untuk mengatasi hal tersebut. Adapun tujuan yang hendak dalam penelitian yaitu, membuat aplikasi atau program web yang dapat mengenkripsi dan mendekripsi basis data, dengan dua algoritma, yaitu algoritma Affine *Cipher* dan algoritma WAKE *(Word Auto Key Encryption)*, sehingga hanya pihak yang mempunyai kewenangan yang bisa mengakses informasi basis data tersebut.Membuat aplikasi atau program web yang hanya bisa diakses oleh *user* yang sudah terdaftar agar tidak ada kebocoran informasi basis data.

Agar tidak menyimpang dari pokok pembahasan permasalahan yang dibahas, maka penulis membatasi penelitian ini yaitu, menggunakan metode Affine *Cipher* dan WAKE untuk enkripsi dan dekripsi data.Data yang akan dienkripsi dan dekripsi adalah *database*.

2. METODE PENELITIAN

Metode penelitian ini digunakan sebagai pedoman penelitian dalam pelaksanaan penelitian agar hasil yang dicapai tidak menyimpang dari tujuan yang sudah ditetapkan.

a. Studi Pustaka

Pada tahap ini penulis melakukan pemahaman, dan mencari jurnal dan buku yang berhubungan dengan *Affine Cipher*, *WAKE* dan hal – hal yang berhubungan dengan keamanan *database*.

b. Analisa

Pada tahap ini merupakan tahapan dimana dilakukan identifikasi masalah.Tahap ini bertujuan untuk menentukan solusi yang didapat dari aktivitas – aktivitas tersebut.

c. Design

Pada tahap ini dilakukan pembuatan dari model perangkat lunak atau program web yang akan dibuat. Tujuan dari pembuatan model ini adalah untuk mendapatkan gambaran awal tentang program yang akan dibuat.

d. Coding dan Testing

Coding merupakan penerjemahan design dalam bahasa yang dikenali oleh komputer, dalam tahap ini penulis menggunakan bahasa pemrograman PHP dengan editor *Notepad* ++ dan *Database* menggunakan *MySQL* dengan editor *phpMyAdmin 4.5.1*.

e. Penerapan

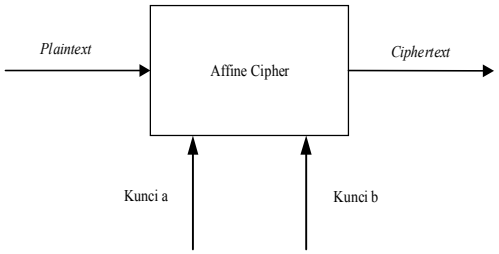
Dalam tahap ini penulis mengimplementasikan dan memberikan training penggunaan aplikasi enkripsi*database* berbasis web yang telah selesai buat, serta mengevaluasi jika masih ada kesalahan dan kekurangan.

2.1 Algoritma Affine Cipher

Affine *cipher* adalah perluasan dari Caesar *cipher*.Affine *cipher* tergolong dalam algoritma klasik yang merupakan algoritma penyandian yang sudah ada sebelum era digital sekarang ini [1]. Algoritma klasik pada dasarnya hanya terdiri dari *cipher* subtitusi dan *cipher* transposisi. *Cipher* subtitusi yaitu proses mensubtitusi karakter – karakter yang ada pada *plaintext*. Sedangkan *cipher* transposisi adalah proses pertukaran huruf – huruf yang terdapat dalam suatu *string* [2].

a. Proses Enkripsi

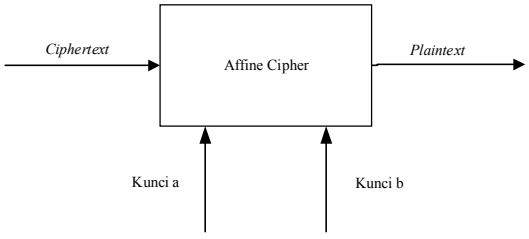
Proses enkripsi menggunakan Affine *cipher* membutuhkan dua buah kunci untuk dapat menghasilkan *ciphertext*. *Plaintext* (p) akan dikonversikan menggunakan tabel konversi sehingga menjadi bentuk desimal, kemudian *ciphertext* (c) akan diperoleh dengan mengenkripsi *plaintext* dengan persamaan. Secara matematis enkripsi *plaintext* menghasilkan *ciphertext* dinyatakan dengan fungsi kongruen



Gambar 1. Proses Enkripsi

b. Proses Dekripsi

Proses dekripsi menggunakan Affine Cipher membutuhkan dua buah kunci yang sama dengan kunci yang digunakan untuk proses enkripsi. Untuk memperoleh kembali *plaintext* dari contoh diatas, maka kita harus memperoleh fungsi dekripsi terlebih dahulu [3].



Gambar 2. Proses Dekripsi

2.2 Algoritma WAKE

Metode WAKE merupakan salah satu algoritma *stream cipher* yang telah digunakan secara komersil. Medote ini ditemukan oleh David Wheeler pada tahun 1993.Metode WAKE menggunakan kunci 128

bit dan sebuah tabel 256x32 bit. Dalam algoritmanya, metode ini menggunakan operasi XOR, AND, OR dan SHIFT RIGHT. Metode WAKE ini telah digunakan pada program Dr.Solomon Anti Virus versi terbaru [4].

Metode WAKE dapat dibagi menjad beberapa proses, yaitu proses pembentukan tabel dan kunci, enkripsi dan dekripsi. Proses penyelesaian metode ini cukup rumit dan sulit untuk dikerjakan secara manual berhubung karena algoritmanya yang cukup panjang dan kompleks. Schneier (1996) melakukan penelitian mengenai Penerapan Algoritma Kriptografi WAKE pada Aplikasi *Chatting* dan Internet Monitoring Berbasis LAN.Penelitian bertujuan untuk memberikan informasi guna menyelesaikan masalah berdasar pada objek yang diteliti, yaitu penerapan kriptografi WAKE pada alpikasi *chatting*[5].

Proses utama WAKE terdiri dari :

a. Proses pembentukan tabel Substitution – Box

Berfungsi untuk membentuk tabel *S-Box* sebesar 256x32 bit. Isi dari tabel *S-Box* ini akan digunakan pada proses pembentukan kinci.Inti dari metode WAKE terletak pada proses pembentukan tabel *S-Box* dan proses pembentukan kunci. Tabel *S-Box* dari metode WAKE bersifat fleksibel dan berbeda – beda untuk setiap putaran.Proses pembentukan tabel *S-Box* terdiri atas 8 proses utama.

b. Proses pembentukan kunci

Proses ini berfungsi untuk membangkitkan bit – bit kunci yang akan digunakan pada proses enkripsi dan dekripsi. Proses pembentukan kunci dari metode WAKE dapat ditentukan sendiri, yaitu sebanyak n putaran. Semakin banyak putaran dari proses pembentukan kunci, maka keamanan datanya akan semakin terjamin.

c. Proses Enkripsi

Proses enkripsi dari metode WAKE untuk menghasilkan ciphertext adalah berupa XOR dari *plaintext* dan 32bit kunci yang dihasilkan dari proses pembentukan kunci.

d. Proses Dekripsi

Proses dekripsi dari metode WAKE untuk menghasilkan *plaintext* adalah berupa hasil operasi XOR dari *ciphertext* dan 32 bit kunci yang dihasilkan dari proses pembentukan kunci [6].

3. ANALISA MASALAH DAN RANCANGAN APLIKASI

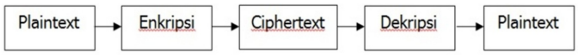
3.1 Analisa Masalah

Grosir Sprei Jakarta adalah jenis wirausaha yang bergerak dibidang produksi dan penjualan sprei.Dalam prosesnya penjualan masih dilakukan secara manual, dimana tingkat kerahasiaan dan keamanan informasi database masih sangat beresiko dari tindak pencurian, kecurangan dan kebocoran rahasia.Hal tersebut dinilai masih kurang efektif.Begitu juga jika dalam prosesnya dilakukan dengan menggunkan teknologi tanpa keamanan yang kuat, informasi database masih bisa dilakukan proses *edit* dan *delete* dengan mudah.Hal tersebut masih bisa disalah gunakan oleh pihak yang tidak bertanggung jawab.

3.2 Penyelesaian Masalah

Dari permasalahan yang telah diuraikan diatas, diperlukan adanya sebuah program web yang dapat menjaga kerahasiaan dari sebuah database. Sehingga isi dari database tersebut tidak bisa dibaca oleh orang lain yang tidak berkepentingan atau tidak berhak mengetahui isi dari database tersebut. Program tersebut nantinya dapat mengubah sebuah database menjadi databaseyang isinya tidak bisa dibaca.Agar isi database tersebut terjaga kerahasiaannya.Kemudian mengembalikan isi basis data tersebut menjadi seperti semula tanpa mengalami cacat atau perubahan sedikitpun.

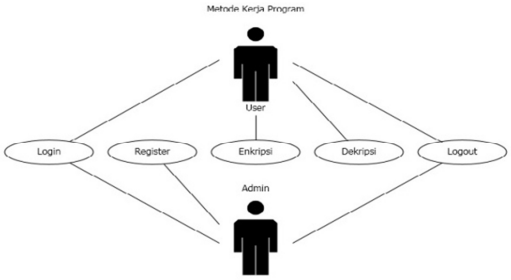
Dengan demikian, penulis menggunakan teknik kriptografi yang diharapkan dapat mengamankan database walaupun database tersebut dicuri dengan syarat database tersebut telah dilakukan enkripsi, Untuk mengimplementasikan kriptografi pada basis data tersebut dibutuhkan algoritma kriptografi, dengan adanya program web ini diharapkan dapat menjaga kerahasiaan dari isi basis data penting agar tidak disalah gunakan oleh orang lain yang tidak berkepentingan.



Gambar 3. Proses Enkripsi dan Dekripsi

3.3 Metode Kerja Aplikasi Usulan

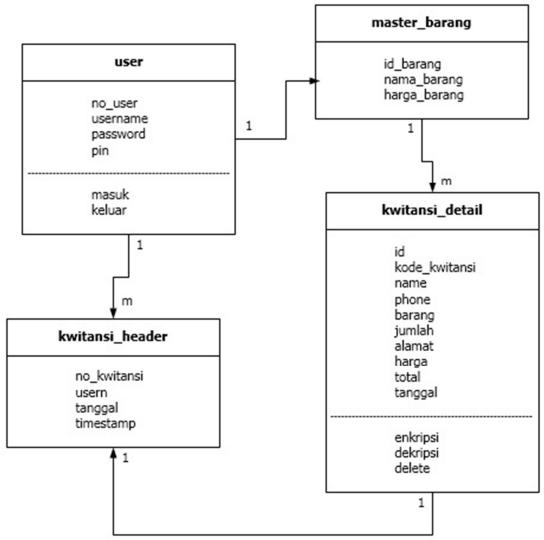
Aplikasi ini terdiri dari beberapa halaman atau *form* yaitu, *form login, form home, form change password, form create nota, form managemen, form master barang, form bantuan,* dan *form logout.*
Berikut adalah gambar interaksi atau apa yang dapat dilakukan *user* dan admin.



Gambar 4. Metode kerja aplikasi

3.4 Class Diagram

Berikut adalah *class diagram* dari program yang akan dibangun.



Gambar 5. Class Diagram

2.5 Spesifikasi Basis Data User

Tabel 1: Struktur Tabel User

No	*Nama field*	Jenis	Lebar	keterangan
1.	*no_user*	*int*	*8*	*nomor urut user*
2.	*username*	*Varchar*	*25*	*Nama user*
3.	*Password*	*Varchar*	*25*	*password*
4.	*Pin*	*Varchar*	*25*	*Key*

Tabel 2: Struktur Tabel Kwitansi_Detail

No	*Nama field*	*Jenis*	*Lebar*	*Keterangan*
1.	*Id*	*Int*	*8*	*Kode berkas*
2.	*No_kwitansi*	*Varchar*	*100*	*Nomor kwitansi*
3.	*Name*	*Varchar*	*120*	*Nama pelanggan*
4.	*Phone*	*Varchar*	*20*	*Nomor telpon*
5.	*Barang*	*Varchar*	*100*	*Nama barang*
6.	*Jumlah*	*Varchar*	*20*	*Jumlah barang*
7.	*Alamat*	*Varchar*	*120*	*Alamat pelangga*
8.	*Harga*	*Varchar*	*20*	*Harga barang*
9.	*Total*	*Varchar*	*20*	*Total harga*

Tabel 3: Struktur Tabel Kwitansi_header

No	*Nama field*	*Jenis*	*Lebar*	*Keterangan*
1.	*No_kwitansi*	*Int*	*100*	*Nomor kwitansi*
2.	*Username*	*Varchar*	*25*	*Nama user*
3.	*Tanggal*	*Datetime*	*10*	*Tanggal berkas*
4.	*Timestamp*	*Timestamp*	*25*	*Tanggal berkas*

Tabel 4: Struktur Tabel Master_barang

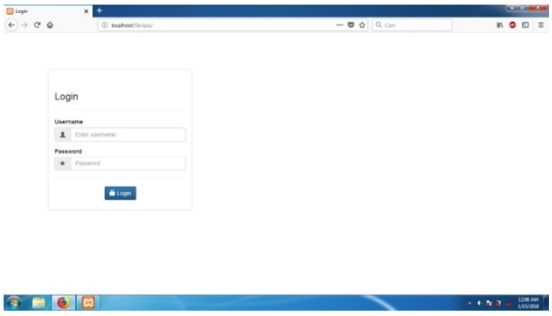
No	*Nama field*	*Jenis*	*Lebar*	*Keterangan*
1.	*Id_barang*	*Int*	*100*	*Id barang*
2.	*Nama_barang*	*Varchar*	*100*	*Nama barang*
3.	*Harga_barang*	*Varchar*	*20*	*Harga barang*

4. IMPLEMENTASI

Pada bagian ini akan diuraikan mengenai tampilan layar program enkripsi dan dekripsi basis data mulai dari pertama kali aplikasi ini dijalankan sampai selesai dijalankan. Berikut ini akan diberikan penjelasan dan gambar mengenai tampilan – tampilan yang ada pada program enkripsi dan dekripsi basis data ini.

4.1 Tampilan Layar Form Login

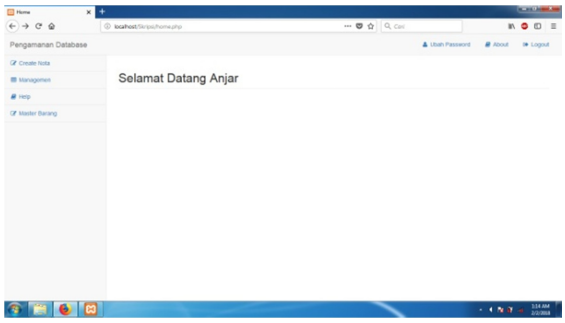
Form login adalah tampilan awal ketika program ini diakses oleh *user*.*User* harus memasukkan *username* dan *password* agar dapat masuk dan menggunakan aplikasi ini. Hanya *user* yang sudah terdaftar yang dapat mengakses atau masuk kedalam program ini.



Gambar 6. Form Login

4.2 Tapilan Layar Form Home

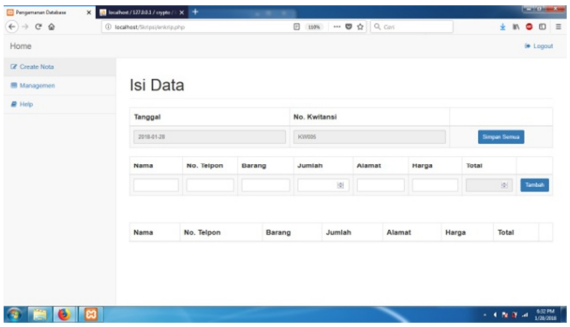
Form ini akan muncul ketika *user* sudah berhasil masuk kedalam program. Didalam *home* terdapat beberapa menu lain seperti, *create nota, managemen,* bantuan, master barang, *change password,* dan *logout.*



Gambar 7. Form Home

4.3 Tampilan Layar Form Create Nota

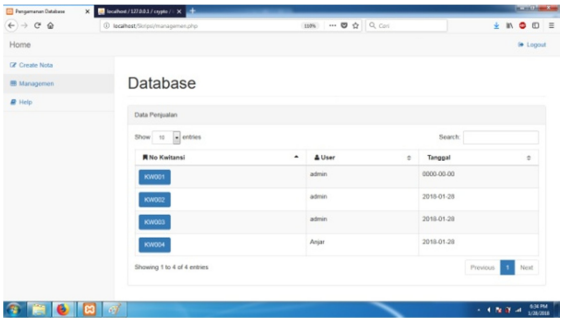
Form ini digunakan untuk memasukkan data pelanggan yang kemudian dienkripsi dan tersimpan di *database*. Terdapat tombol "Simpan Semua" untuk proses enkripsi dan simpan kedalam *database*, dan tombol "tambah" untuk memasukkan data lain jika pelanggan membeli lebih dari satu jenis barang.



Gambar 8. Form Create Nota

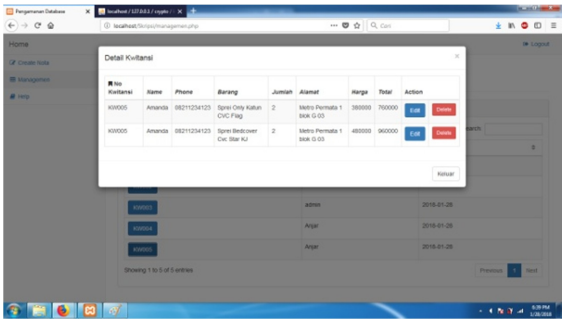
4.4 Tampilan Layar Form Managemen

Form ini berfungsi untuk melihat semua data yang sudah tersimpan di *database*. Dan *user* dapat merubah data pelanggan jika terjadi kesalahan, dan menghapus data pelanggan. *User* diminta memasukkan pin sebelum melakukan proses selanjutnya. Pin tersebut merupakan kunci dan berfungsi untuk proses dekripsi.



Gambar 9. Form Managemen

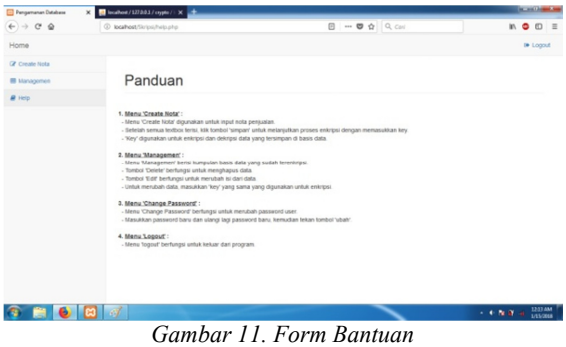
Berikut adalah tampilan layar *form managemen* untuk proses hapus data dan ubah data.



Gambar 10. Form Edit dan Delete

4.5 Tampilan Layar Form Bantuan

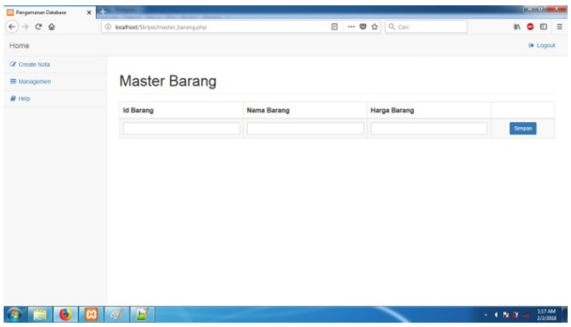
Form ini berisikan informasi tentang cara penggunaan program tersebut.



Gambar 11. Form Bantuan

4.6 Tampilan Layar Form Master Barang

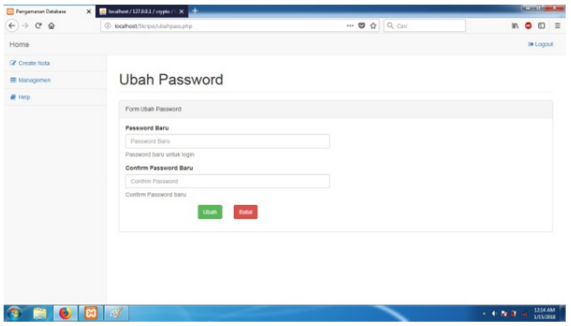
Form ini berfungsi untuk memasukkan data barang kedalam *database*.



Gambar 12. Form Master Barang

4.7 Tampilan Layar Form Change Password

Form ini berfungsi untuk merubah *password* lama *user*.



Gambar 13. Form Change Password

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah melalui beberapa tahapan mulai analisa, perancangan, implementasi, percobaan dan pengujian yang dilakukan dalam penelitian ini maka kesimpulan yang diperoleh diantaranya sebagai berikut :

a. Program mampu melakukan proses enkripsi maupun dekripsi pada tahap uji coba aplikasi.
b. Program mampu memberikan keefektifitasan dalam perihal keamanan basis data karena

dengan program pengamanan basis data, tidak perlu dilakukan secara manual.

c. Data yang telah terenkripsi hanya dapat didekripsi dengan aplikasi ini.

5.2 Saran

Dengan berbagai keterbatasan aplikasi ini maka untuk perbaikan dan pengembangan aplikasi lebih lanjut, maka berikut ini saran yang dapat dijadikan acuan yaitu, program diharapkan dapat melakukan cetak nota.

6. DAFTAR PUSTAKA

[1] Puspitaningrum, Diah Ayu., Ajib Susanto. 2013. "Implementasi Algoritma Vegenere, Caesar, dan Affine Cipher pada Database System Inventori Toko Wiwin Elektronik Grobogan". Junal.Semarang : Universitas Dian Nuswantoro.

[2] Munir, Rinaldi. 2006. "Kriptografi". Buku.Bandung : ITB.

[3] Religia, Yoga. 2013. "Implementasi Algoritma Affine Cipher dan Vigenere Cipher untuk Keamanan Login Inventori TB Mita Jepara". Jurnal. Semarang : Universitas Dian Nuswantoro.

[4] Dahria, Muhammad.,Rahim, Abdul.,& Hendra Jaya. 2012. "Perangkat Lunak Pembelajaran Kriptografi Metode WAKE". Jurnal Ilmiah Saintikom. Medan : STMIK Triguna Dharma.

[5] Eddy, Mohammad R.P. 2014. "Pembelajaran Enkripsi Metode WAKE". Jurnal Ilmiah SISFOTENIKA. Pontianak : Sekolah Tinggi Manajemen dan Komputer.

[6] Gultom, Halasson. 2013. "Penyediaan Email Menggunakan Algoritma Kriptografi WAKE". Jurnal. Pelita Informatika Budi Darma, Volume : IV, 1. Medan : STMIK Budi Darma.