PENGAMANAN BASIS DATA SISTEM PENJUALAN DENGAN MENGGUNAKAN TEKNIK ENKRIPSI KRIPTOGRAFI *GOST*

Kodar Udoyono[*1], Ahmad Saepudin[#2]

Program Studi Teknik Komputer dan Jaringan, STMIK Subang
Jl. Marsinu No. 5 - Subang, Tlp. 0206-417853 Fax. 0206-411873
*E-mail: kodarudoyono@yahoo.co.id[*1], ahmadsaepudin87@yahoo.co.id[#2]*

ABSTRAKSI

Sistem keamanan database dan kerahasiaan informasi personal menjadi aspek penting di era informasi dan komukasi digital. Ketika saluran komunikasi yang digunakan kurang aman, maka akan menjadi sasaran bagi hacker. Dalam aplikasi ini akan dibahas penerapan kriptografi GOST (goverment standard) untuk aplikasi penjualan berbasis web. Proses enkripsi pada login form, sehingga password yang tersimpan didalam database terenkripsi dengan memanfaatkan fungsi hash kriptografi GOST R 34-11.94 pada PHP.

Fungsi hash kriptografi GOST merupakan sebuah prosedur yang mengambil blok-blok data sebuah pesan dan mengembalikannya menjadi sebuah pesan String bit dengan panjang yang telah ditentukan (fixed-size). Fungsi GOST hash adalah dasar pembuatan GOST cipher block 64 bit dengan panjang kunci 256 bit yang dikembangkan oleh Federal Agency for Government Communication and Information dan oleh All Russia Scientific and Research Institute of Standardization yang kemudian dipakai sebagai fungsi hash standar di Rusia. Pesan Sting bit dengan blok-blok berukuran 256 akan diproses oleh fungsi GOST hash menjadi nilai hash 256 bit. Jika panjang pesan tidak mencapai kelipatan 256, pesan String bit akan di-padding seminimal mungkin hingga kondisi tercapai (panjang pesan sama dengan klipatan 256 bit)

Proses enkripsi pada login admin dan user sudah di uji dengan menggunakan generator enkripsi, hasil hashing dan enkripsi pada password login admin dan user dengan GOST (govement standart) menghasilkan output HEXADECIMAL dengan panjang fixed 64 bit. Karakter pesan yang di input dengan panjang maksimal 1024 bit dan akan menghasilkan nilai hashing dengan panjang pesan fixed 64 bit

Kata Kunci: **Kriptografi, kriptografi GOST, e-commerce, *fixed-size* dan hashing password**

1. Pendahuluan

1.1. Latar Belakang

Berkembangnya teknik telekomunikasi dan sistem pengolahan data antar pengguna komputer yang satu dengan komputer yang lain yang berfungsi untuk menyalurkan data sehingga masalah keamanan merupakan salah satu aspek penting dari suatu sistem informasi.

Dalam komunikasi data terdapat sebuah metode pengamanan data yang dikenal dengan nama kriptografi. Kriptografi merupakan salah satu metode pengamanan data yang dapat digunakan untuk menjaga kerahasiaan data, keaslian data, serta ke utuhan suatu WEB. Metode ini bertujuan agar informasi yang bersifat rahasia yang dikirim melalui telekomunikasi umum seperti LAN (local area network) atau internet, tidak dapat diketahui atau dimanfaatkan oleh orang yang tidak berkepentingan atau yang tidak berhak menerimanya. Data penting dan vital yang tersimpan pada basis data seringkali menjadi target empuk bagi para penyerang. Serangan yang terjadi dapat dilakukan oleh pihak luar (hacker) maupun pihak dalam (pegawai yang tidak puas)

Kriptografi GOST untuk keamanan database telah banyak digunakan di instansi pemerintahan dan negara-negara yang tergabung dalam CIS (Commonwealth of Independent States) dan juga di gunakan untuk keamanan bank sentral di rusia.

Kriptografi GOST fungsi hash (H) menentukan pesan string bit M yang memiliki berbagai panjang pesan mejadi sebuah nilai hash yang memiliki panjang tetap. Secara formal, fungsi hash yang digunakan harus bisa memenuhi beberapa kebutuhan keamanan. collision resistence: dua pesan yang berbeda harus memiliki nilai hash yang berbeda. Sebuah pesan (M1) yang dipetakan dengan fungsi hash (H) memiliki nilai hash yang tidak mungkin dimiliki oleh pesan lain (M2) yang dipetakan dengan fungsi hash yang sama (H). Second preimage resistance : jika terdapat sebuah pesan M, maka tidak mungkin menemukan sebuah pesan yang berbeda jika terdapat H(M1)=H(M2). Preimage resistance : nilai hash yang dihasilkan dari fungsi GOST hash, tidak dapat dikembalikan menjadi pesan semula. Semua sifat ini secara tidak langsung menyatakan bahwa segala macam lawan yang jahat atau serangan tidak dapat mengganti atau merubah pesan tanpa merubah nilai hash nya.

Fungsi GOST hash adalah fungsi yang digunakan banyak orang di Rusia dan secara spesifik Rusia membuat sebuah fungsi hash standar Russian national standard GOST 34.11-94. Fungsi standar ini dikembangkan oleh GUBS of Federal Agency Goverbnebt Communication and Information dan All Russian Scientific and Research Institute of Standardization. Fungsi GOST hash merupakan satu-satunya fungsi hash yang dapat digunakan untuk Russian digital signature algorithm GOST 34.10-94.

Fungsi GOST hash memproses pesan dengan berbagai macam panjang menjadi sebuah keluaran dengan panjang yang telah ditetapkan sepanjang 256 bit. Pesan masukan akan ditambahkan dengan bilangan nol sampai panjang pesan merupakan kelipatan 256 bit. Bit-bit terakhir akan diisi dengan panjang pesan yang akan di-hash.

Dalam kriptografi terdapat berbagai macam sistem sandi yang tujuan penggunaan dan tingkat kerahasiaannya berbeda sesuai dengan permintaan user, tetapi dalam prakteknya user menginginkan kemudahan-kemudahan seperti: kerahasian data, kecepatan, ketepatan, maupun biaya yang murah. Hal ini merupakan sebuah kendala dalam membuat suatu sistem kriptografi.

Kenyataan dalam proses pengamanan data dengan metode kriptografi sering kali dibutuhkan waktu yang relatif lebih lama dibandingkan tanpa menggunakan metode kriptografi. Oleh karena itu, diusahakan membuat sistem sandi yang lebih cepat dalam proses kriptografi tanpa mengabaikan kaidah kerahasiaan yang ingin dicapai dan hanya membutuhkan biaya yang murah.

Dalam pengamanan data tidak hanya sebatas data tersebut tidak dapat dibaca orang lain, tetapi juga bagaimana agar data tersebut tidak dapat diubah atau dimodifikasi, sehingga dibutuhkan suatu cara untuk memastikan keaslian dari data yang dikirim tersebut.

1.2. Identifikasi Masalah

Keamanan dan kerahasian data pada Sistem penjualan sangat penting artinya, baik pada saat pengiriman ataupun pada saat data atau informasi tersebut diterima, karena data atau informasi tidak akan berguna lagi apabila pada saat pengiriman informasi tersebut disadap atau dibajak oleh orang yang tidak berhak atau berkepentingan, dari uraian di atas, maka dapat didefinisikan masalahnya sebagai berikut:

- Diperlukan sebuah sistem untuk menangani masalah keamanan database sistem penjualan.
- Belum adanya sistem penjualan yang menggunkan pengamanan database login user dengan menggunakan teknik enkripsi kriptografi GOST di indonesia.

1.3. Tujuan

Tujuan dari penelitina ini adalah untuk memahami keamanan sistem dan mengimplementasikan pengamankan database dengan cara mengekripsi password database login user dan admin master menggunakan teknik enkripsi kriptografi GOST.

1.4. Manfaat

Manfaat yang ingin dicapai adalah sebagai berikut:

- Menerapkan ilmu kriptografi GOST khususnya dalam keamanan database login user dan bisa memahami fungsi GOST hash untuk keamanan aplikasi berbasis WEB.
- Mampu membangun aplikasi berbasis WEB sistem penjualan dengan menggunakan teknik enkripsi kriptografi GOST.

1.5. Metodologi Penelitian

Metodologi yang dilakukan untuk merancang bangun aplikasi WEB sistem penjualan keamanan database menggunakan teknik enkripsi kriptografi GOST. Tahapan yang dilaksanakan pada saat penelitian adalah sebagai berikut:

- Studi Literatur

Pada bagian ini penulis mengumpulkan data mengenai aturan-aturan yang ada pada kriptografi GOST dengan pendekatan yang dilakukan sebagai berikut: Yaitu pengumpulan data yang penulis ambil dari buku-buku, situs-situs di internet, jurnal dan sumber lainnya yang menunjang.

- Analisis dan Perancangan Desain Sistem

Pada bagian ini penulis melakukan analisis penerapan kriptografi GOST pada aplikasi sistem penjualan berbasis WEB. Analisis yang dilakukan adalah menggambar flowchart, DFD, dan perancangan antarmuka (interface).

- Implementasi Sistem

Pada bagian ini akan dilakukan pengkodean dan penerapan perancangan aplikasi tersebut kedalam bahasa pemograman PHP.

- Pengujian Sistem

Pada bagian ini akan dilakukan pengujian terhadap aplikasi dengan menggunakan generator enkripsi terhadap password WEB sistem penjualan juga dilakukan pengujian keakuratan enkripsi terhadap password apakah memenuhi kriteria atau tidak.

2. Tinjauan Pustaka

2.1. Keamanan Data

Menurut (Herryawan, I Putu, 2010), Secara umum data dikategorikan menjadi dua, yaitu data yang bersifat rahasia dan data yang tidak bersifat rahasia. Data yang tidak bersifat rahasia biasanya tidak akan terlalu diperhatikan. Yang sangat perlu diperhatikan adalah data yang bersifat rahasia, dimana setiap informasi yang ada didalamnya akan sangat berharga bagi pihak yang membutuhkan karena data tersebut dapat dengan mudah digandakan. Untuk mendapatkan informasi didalamnya, biasanya dilakukan berbagai cara yang tidak sah. Keamanan data biasanya terkait hal-hal berikut:

Fisik, dalam hal ini pihak yang tidak berwenang terhadap data berusaha mendapatkan data dengan melakukan kegiatan sabotase atau penghancuran tempat penyimpanan data.

Organisasi, dalam hal ini pihak yang tidak berwenang untuk mendapatkan data melalui kelalaian atau kebocoran anggota yang menangani data tersebut.

Ancaman dari luar, dalam hal ini pihak yang tidak berwenang berusaha untuk mendapatkan data melalui media komunikasi dan juga melakukan pencurian data yang tersimpan di dalam komputer.

(Herryawan, I Putu, 2010), Fungsi keamanan komputer adalah menjaga tiga karakteristik, yaitu:

Secrecy, adalah isi dari program komputer hanya dapat diakses oleh orang yang berhak. Tipe yang termasuk di sini adalah reading, viewing, printing, atau hanya yang mengetahui keberadaan sebuah objek.

Integrity, adalah isi dari komputer yang dapat dimodifikasi oleh orang yang berhak, yang termasuk disini adalah writing, changing status, deleting, dan creating.

Availability, adalah isi dari komputer yang tersedia untuk beberapa kelompok yang diberi hak.

Data yang aman adalah data yang memenuhi ketiga karakteristik keamanan data tersebut. Melihat pada kenyataan semakin banyak data yang diproses dengan komputer dan dikirim melalui perangkat

komunikasi elektronik, maka ancaman terhadap pengamanan data akan semakin meningkat. Beberapa pola ancaman terhadap komunikasi data dalam komputer dapat diterangkan sebagai berikut:

Interruption, terjadi bila data yang dikirimkan dari A tidak sampai pada orang yang berhak B. Interruption merupakan pola penyerangan terhadap sifat availability (ketersedian data). Contohnya adalah kerusakan pada hardware, kegagalan operating sistem sehingga sistem tidak dapat menemukan file yang dicari.

Interception, terjadi bila pihak ketiga C berhasil membaca data yang dikirimkan. Interception merupakan pola penyerangan terhadap sifat confidentiality/secrecy (kerahasian data), contohnya adalah penggandaan program atau file data yang tidak terlihat, atau pencurian data pada jaringan dengan cara wireteapping.

Modification, pada serangan modification pihak ketiga C berhasil merubah pesan yang dikirimkan. Modification merupakan pola penyerangan terhadap sifat integrity (keaslian data).

Fabrication, pada serangan fabrication penyerang berhasil mengirimkan data ke tujuan dengan memanfaatkan identitas orang lain. Fabrication merupakan pola penyerangan terhadap sifat authenticity (autentifikasi data).

Untuk mengantisipasi ancaman-ancaman tersebut di atas perlu dilakukan usaha untuk melindungi data yang dikirim melalui saluran komunikasi, salah satu usaha tersebut adalah dengan menyandikan informasi yang ada pada data yang akan dikirim. Penyembunyian informasi yang ada dalam suatu bentuk tertentu yang tidak dapat dimengerti pihak lain (yang tidak berkepentingan) merupakan bagian kriptografi.

2.2. Kriptografi

Kriptografi memiliki sejarah yang panjang dan mengagumkan. Penulisan rahasia ini dapat dilacak kembali ke 4000 tahun SM saat digunakan oleh bangsa Mesir (Kahn,1967). Mereka menggunakan hieroglyphcs untuk menyembunyikan tulisan dari mereka yang tidak diharapkan (Kahn, 1967). Hieroglyphcs diturunkan dari bahasa Yunani hieroglyphica yang berarti ukiran rahasia (Kahn, 1967). Hieroglyphs berevolusi menjadi hieratic, yaitu stylized script yang lebih mudah untuk digunakan (Kahn, 1967).

Menurut (Benedict Marthin, dkk, 2017) Kriptografi merupakan studi tentang metode untuk mengirim pesan secara rahasia sehingga hanya penerima pesan yang dituju yang dapat menghilangkan penyamaran dan membaca atau memahami isi pesan yang sebenarnya. Berdasarkan etimologinya, kriptografi terdiri dari kryptos yang berarti tersembunyi, dan graphein yang berarti menulis. Pesan asli disebut dengan plaintext, dan pesan yang disamarkan disebut ciphertext. Pesan yang disamarkan dan dikirim ke penerima disebut dengan cryptogram. Proses mengubah plaintext menjadi ciphertext disebut encryption atau enciphering, dan proses kebalikan dari mengubah ciphertext menjadi plaintext, yang dilakukan oleh penerima yang memiliki pengetahuan untuk menghapus penyamaran, disebut decryption atau deciphering. Siapapun yang terlibat dalam kriptografi disebut cryptographer. Kriptografi (keamanan kriptografi) adalah salah satu cara yang efektif untuk keamanan data. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematis yang berhubungan dengan aspek keamanan informasi seperti (van Oorschot 1996): keabsahan, integritas data, serta autentifikasi data. Kriptografi tidak berarti hanya memberikan keamanan informasi saja, namun lebih ke arah teknik-tekniknya. Ada empat tujuan dari ilmu kriptografi, yaitu: (van Oorschot 1996):

Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas (van Oorschot 1996).

Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah (van Oorschot 1996). Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain menyangkut penyisipan, penghapusan, dan pensubtitusian data lain ke dalam data yang sebenarnya (van Oorschot 1996).

Autentikasi, adalah berhubungan dengan identifikasi, baik secara kesatuan sistem maupun informasi itu sendiri (van Oorschot 1996). Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain (van Oorschot 1996).

Non-repudiasi, Merupakan usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang pihak mengirimkan (van Oorschot1996).

2.3. Fungsi GOST Hash (hasf function)

Menurut (Benedict Marthin, dkk, 2017) Fungsi hash adalah fungsi yang menerima masukan string yang panjangnya sembarang dan mengkonversinya menjadi string keluaran yang panjangnya tetap (fixed) (umumnya berukuran jauh lebih kecil daripada ukuran string semula).

Fungsi hash dapat diketahui oleh siapa pun, tak terkecuali, sehingga semuanya dapat memeriksa keutuhan dokumen atau pesan tertentu. Tak ada algoritma rahasia, dan umumnya tak ada pula kunci rahasianya. Jaminan dari keamanan nilai hash berangkat dari kenyataan bahwa hampir tidak ada dua pre-image yang memiliki nilai hash yang sama. Inilah yang disebut dengan sifat collision free dari suatu fungsi hash yang baik. Selain itu, sangat sulit untuk membuat suatu pre-image jika hanya diketahui nilai hash-nya saja.

Berikut diuraikan sifat-sifat fungsi hash kriptografi:

Tahan pre-image (pre-image resistent): Bila diketahui nilai hash, sulit didapatkan (secara komputasi tidak layak) m dimana h = hash(m).

Tahan pre-image kedua (second pre-image resistant): Bila diketahui input m1, sulit dicari input m2 (tidak sama dengan m1) yang menyebabkan hash(m1) = hash(m2).

Tahan tumbukan (collision-resistant): Sulit dicari dua input yang berbeda, m1 dan m2, yang menyebabkan hash(m1)=hash i (m2).

Selain itu, fungsi hash mempunyai sifat sebagai berikut:

1. Fungsi H dapat diterapkan pada blok data berukuran berapa saja.
2. H menghasilkan nilai (h) dengan panjang tetap (fixed-length output).
3. H(x) mudah dihitung untuk setiap nilai x yang diberikan.
4. Untuk setiap h yang dihasilkan, sangat sulit dikembalikan nilai x sehingga H(x)= h.
5. Untuk setiap x yang diberikan, sangat sulit mencari y $\neq$x sedemikian sehingga H(y) = H(x).
6. Sangat sulit mencari pasangan x dan y sedemikian sehingga H(x) = H(y).

2.4. Fungsi GOST Hash (hasf function)

Algoritma kriptografi merupakan langkah-langkah logis mengenai penyembunyian pesan dari orang-orang yang tidak berhak atas pesan tersebut, algoritma kriptografi terdiri dari 3 (tiga) dasar fungsi, yaitu: (Sons, 1996):

- Enkripsi

Enkripsi merupakan hal yang sangat penting dalam kriptografi yang merupakan pengamanan data yang dikirimkan terjaga kerahasiaannya (Sons,1996). Pesan asli disebut plaintext yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan cipher atau kode (Sons, 1996).

- Dekripsi

Dekripsi merupakan kebalikan dari enkripsi, pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (plaintext) disebut dengan dekripsi pesan (Sons,1996). Algoritma yang digunakan untuk dekripsi tentu berbeda dengan yang digunakan untuk enkripsi (Sons, 1996).

- Kunci

Kunci yang dimaksud adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi jadi 2 (dua) bagian, yaitu kunci pribadi (private key) dan kunci umum (public key) (Sons, 1996).

Berdasarkan jenis kunci yang digunakannya, algoritma kriptografi
dikelompokan menjadi 2 (dua) bagian, yaitu (Sons, 1996):

a. Algoritma Kriptografi Simetri (Algoritma Konvensional)
b. Algoritma Kriptografi Tak Simetri (Algoritma Kunci Publik)

Perbedaan utama antara metode enkripsi simetri dan asimetri terletak pada sama dan tidaknya kunci yang digunakan dalam proses enkripsi dengan kunci yang digunakan pada proses dekripsi (Sons, 1996). GOST merupakan singkatan dari "Gosudarstvennyi Standard" atau "Government Standard" (Schneier, 1995). Metoda GOST merupakan suatu algoritma block cipher yang dikembangkan oleh seorang berkebangsaan Uni Soviet (Schneier, 1995). Metoda ini dikembangkan oleh pemerintah Uni Soviet pada masa perang dingin untuk menyembunyikan data atau informasi yang bersifat rahasia pada saat komunikasi (Schneier, 1995).

Kriptografi GOST merupakan blok cipher 64 bit dengan panjang kunci 256 bit (Saarinen, 1998). Algoritma ini mengiterasi algoritma enkripsi sederhana sebanyak 32 putaran (round) (Saarinen, 1998). Untuk mengenkripsi pertama-tama plaintext 64 bit dipecah menjadi 32 bit bagian kiri, L dan 32 bit bagian kanan, R. Subkunci (i) untuk putaran i adalah K Pada satu putaran ke-i operasinya adalah sebagai berikut (Saarinen,1998).

$Li = Ri-1$

$Ri = Li-1 \oplus f(Ri-1,Ki$

Secara struktural, kriptografi GOST mirip dengan algoritma DES (Data Encryption Standart) (Kelsey, 1996). Algoritma DES merupakan blok cipher 64 bit dengan panjang kunci 56 bit (Kelsey, 1996). Algoritma ini mengiterasi algoritma enkripsi sebanyak 16 putaran (round) (Kelsey, 1996). Karena panjang kunci yang hanya 56 bit, membuat algoritma ini sangat rawan di-brute force sehingga saat ini digunakan 3 buah DES secara berurutan untuk mengenkripsi sebuah paintext yang disebut dengan Triple DES (Kelsey,1996). Panjang kunci juga diperpanjang 3 kali menjadi 168 bit (56*3 = 168) (Kelsey,1996).

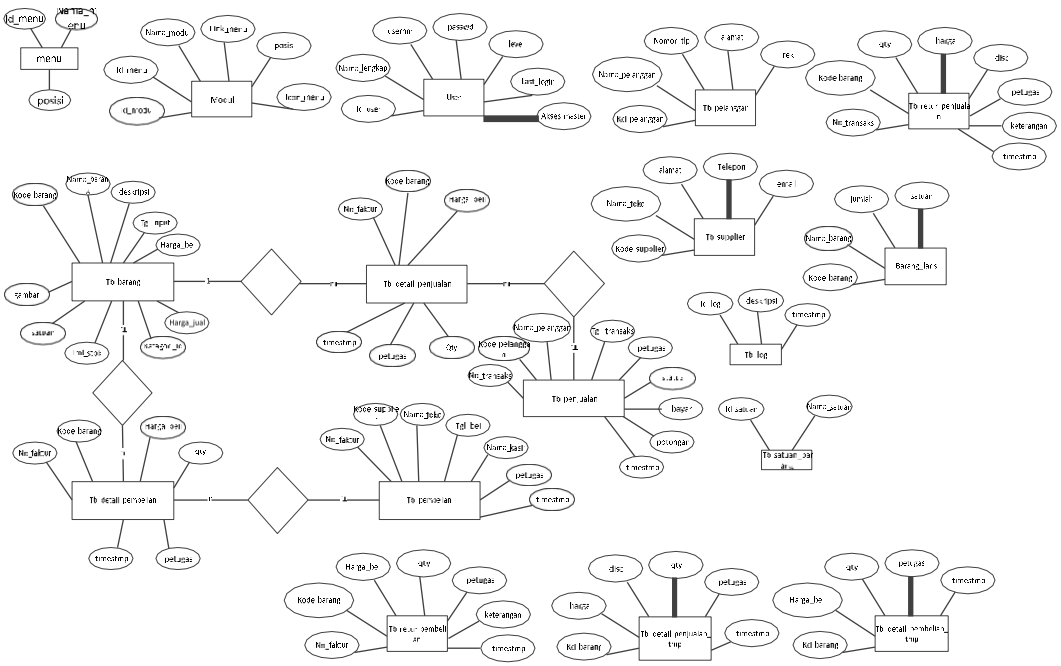
Kelemahan GOST yang diketahui sampai saat ini adalah karena key schedule- nya yang sederhana sehingga pada keadaan tertentu menjadi titik lemahnya terhadap metoda kriptanalisis seperti Related-key Cryptanalysis (Shorin, 2001). Tetapi hal ini dapat diatasi dengan melewatkan kunci kepada fungsi hash yang kuat secara kriptografi seperti SHA-1, kemudian menggunakan hasil hash untuk input inisialisasi kunci (Shorin, 2001). Kelebihan dari metoda GOST ini adalah kecepatannya yang cukup baik, walaupun tidak secepat Blowfish tetapi lebih cepat dari IDEA (Shorin, 2001).

3. Analisa

3.1 Deskripsi Sistem

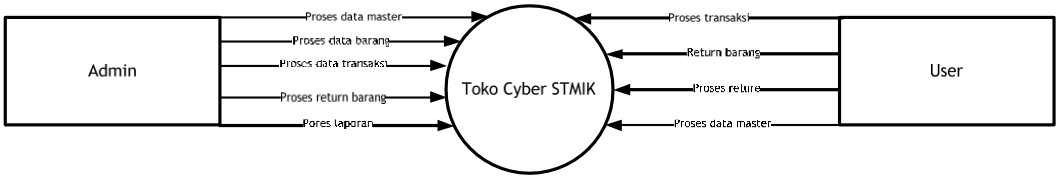
Penerapan algoritma kriptografi GOST (Gosudarstvennyl Standart) atau dalam bahasa inggris (Goverment Standard) untuk enkripsi database sistem penjualan dengan spesifikasi yang terenkripsinya adalah passoword user dan admin saat melakukan login pada sistem, karena pada bagian ini merupakan inti dari keamanan sistem database untuk melindungi password dari serangan external yang menggunakan tools seperti MYSQL injection dan serangan external lainnya yang menggunakan tools penetration.

3.2 Pemodelan ERD (Entity Relationship Diagram)



3.3 Model Proses

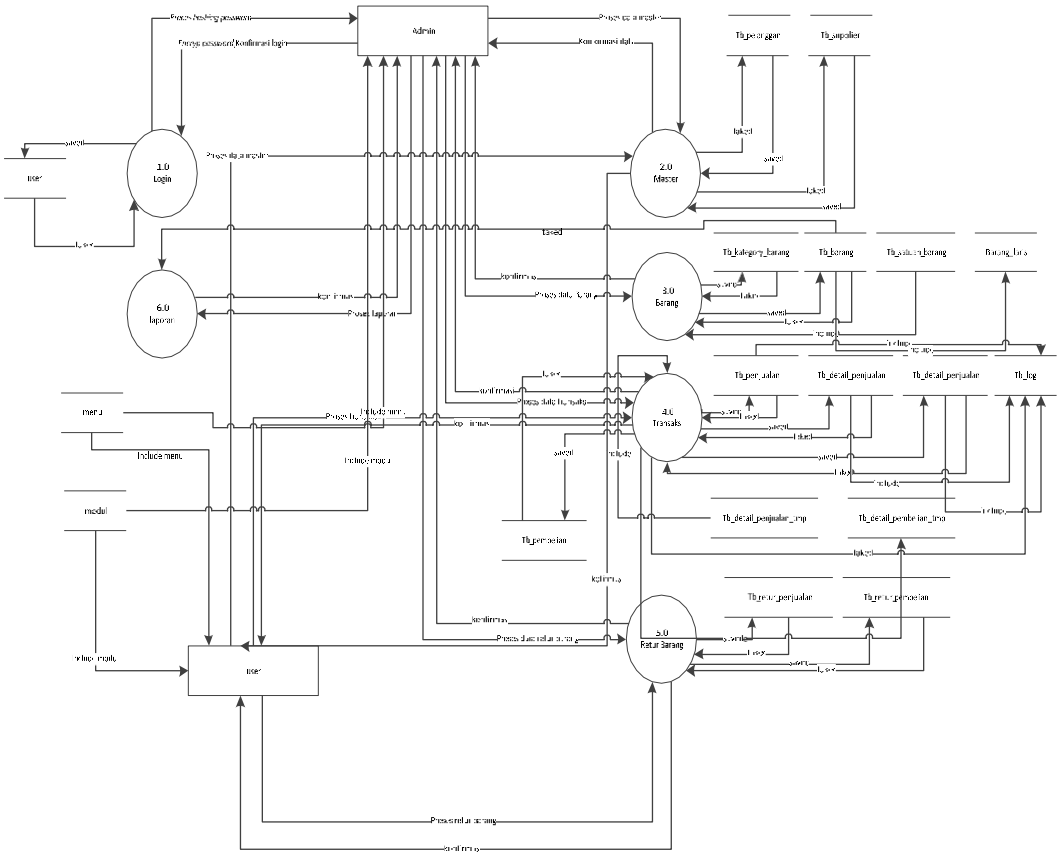
Proses ini menjelaskan pemodelan diagram kontek yang dibuat aplikasi pengamanan basis data sistem penjualan dengan teknik enkripsi.



Gambar 3. 1 Diagram Kontek Sistem Penjualan

Dari gambar 3.1. dapat dijelaskan bahwasanya admin mempunyai hak akses penuh terhadap sistem penjualan. Admin dapat merubah , menambahkan, menghapus dan edit pada data sistem penjualan. Admin mempunya akses untuk melakukan proses data master, proses data barang, proses data transaksi dan proses laporan. Sementara user hanya dapat mengakses proses transaksi, return barang, proses reture dan data master.

Berikut ini adalahh pemodelan DFD keseluruhan yang menapilkan semua bagian dalam aplikasi.

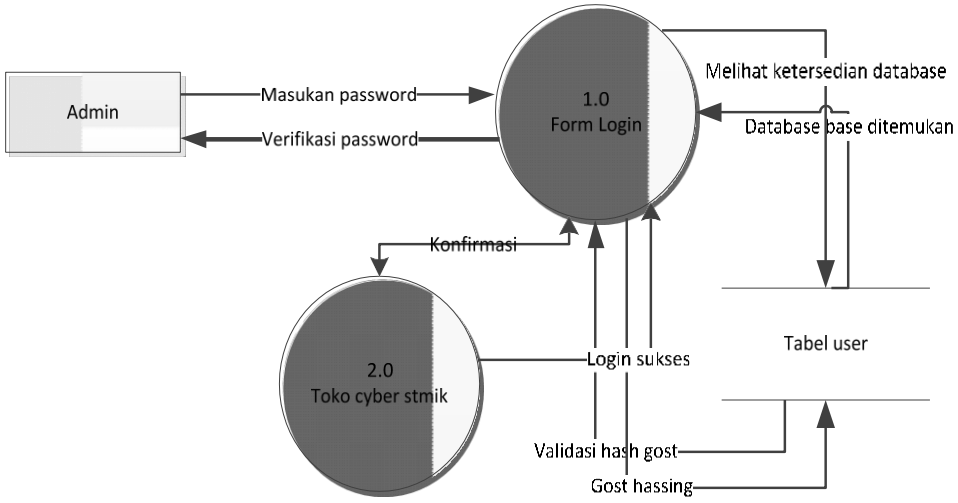


Gambar 3. 2 DFD Keseluruhan Sistem Penjulan

Pada gambar 3.2 menjelaskan semua proses yang dilakukan oleh admin dan user. Admin dapat melakukan semua proses pada sistem penjualan sementara user hanya dapat melakukan transaksi, retur barang dan hak akses master. Demi keamanan sistem, database login pada sistem penjualan dilakukan proses enkripsi terhadap password untuk melindungi data rahasia user dan admin.

Pemodelan Proses Ekripsi Database Login

Pada bagian ini dijelaskan mengenai proses enkripsi terhadap databse login user dan admin.



Gambar 33.3 Proses Enkripsi Pada Database Login

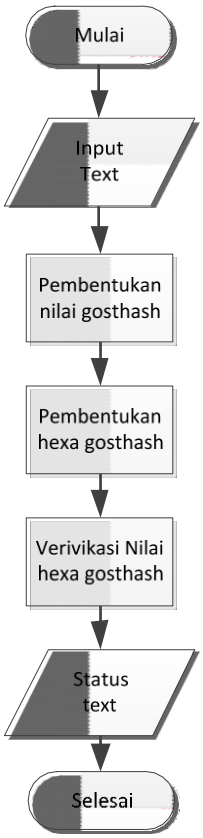
Pada gambar 3.3. Proses enkripsi yang dilakukan dalam sistem penjualan adalah ketika admin dan user melakukan login, proses enkripsi dilakukan ketika sistem melihat ketersediaan pada database setelah di temukan pada tabel user proses enkripsi GOST hashing dilakukan oleh sistem, di validasi GOST hash barulah user dapat melakukan login pada sistem penjualan.

3.4 Analisis Proses enkripsi

Pada sistem ini akan dilakukan analisis terhadap sistem dalam melakukan proses enkripsi, pembentukan nilai GOST hash, pebentukan nilai HEXA dan verifikasi plaintext untuk membuktikan password terenkripsi dengan kriptografi GOST.

Proses Enkripsi GOST Hash

Berikut ini adalah flowchart proses enkripsi dari kriptografi GOST hash function untuk keamanan password yang dapat dilihat pada gambar 3.4



Gambar 3.4 flowchart Proses Enkripsi teks

Seperti yang terlihat pada gambar 3.2.1. menunjukan bahwasanya cara kerja dari kriptografi GOST hash function terdiri dari 3 tahap yaitu pembentukan nilai GOST hash, pembentukan nilai HEXA dan verifikasi nilai HEXA GOST hash.

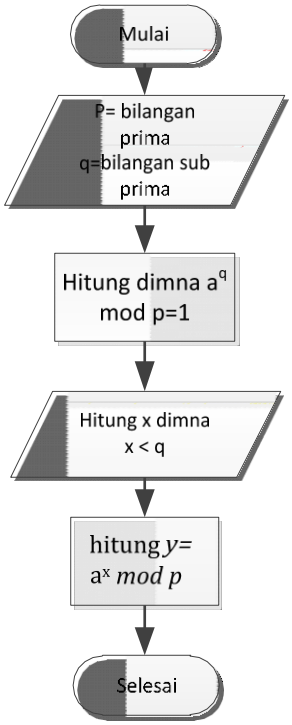
Pada proses pembentukan nilai GOST hash, sistem akan menghsilkan nilai hash dengan panjang 64 bit yang kan digunakan untuk enkripsi password pada database tabel login user.

Pada proses pembentukan HEXA GOST hash, sistem pertama kali akan melakukan proses hashing plainteks (teks asli) terhadap password database login user sehingga menghasilkan keluaran hash yang disebut dengan message digest. Hasil akhirnya yaitu berupa nilai HEXADECIMAL dengan panjang 64 bit.

Kemudian user dapat login dengan aman ke dalam sistem penjualan untuk melakukan kegitan transaksi, memilih produk dan membelinya yang terdapat pada sistem penjualan.

Pembentukan Nilai GOST Hash

Proses pembentukan nilai GOST hash pada krptografi GOST untuk pengamanan basisdata sistem penjualan ini terdapat pada flowchart dari gambar 3.5. dimana proses ini menghasilkan nilai HEXADECIMAL dengan panjang 64 bit.



Gambar 3.5 flowchart Pembentukan nilai GOST hash

Berdasarkan gambar 3.5. pertama sekali sistem akan melakukan proses pembentukan nilai GOST hash sebagai berikut:

Pilih dua bilangan prima sebagai nilai p dan q. Dalam hal ini bilangan prima p memilik panjang 1024-Bit dan bilang prima q memiliki panjang 256-Bit dimana q merupakan pengfaktoran dari p-1.

Misal nilai p=509 dan q=127, maka nilai q memenuhi pengfaktoran p-1. dimna 127*4=509-1.

Hitung nilai acak a dimana a< p-1, sehingga aq mod p=1.

Misal a= 23, (memenuhi 23127 mod p=1).

Tentukan nilai x, yang dalam hal ini x< q.

Misal x= 89.

Kemudian hitung y, dengan rumus Gost Hash.

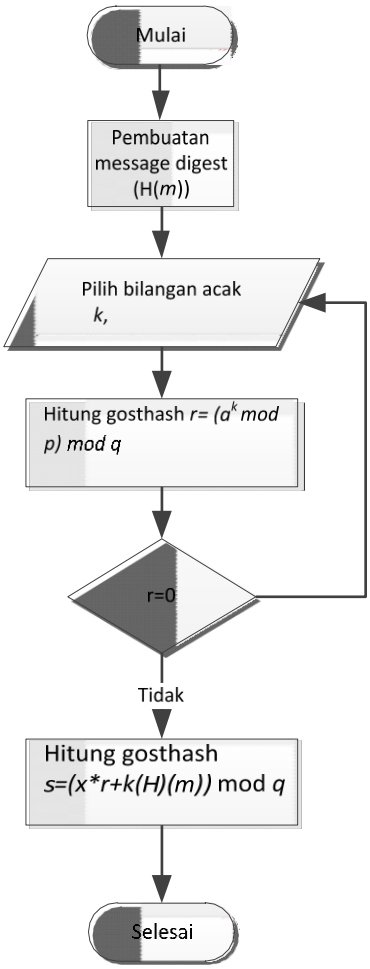
Y = (23)89 mod 509.

Y = 293.

Dalam ini parameter yang beleh diketahui secara umum adalah p, q, a. nilai GOST hash adalah x dan nilai HEXAnya adalah y.

Pembentukan HEXA GOST hash

Proses pembentukan HEXA GOST hash merupakan proses hashing yang dilakukan pada password login user untuk mendapatkan message digest yang nantinya akan di enkripsi sehingga menghasilkan chpertteks dengan bentuk HEXADECIMAL dengan panjang karakter 64-Bit. Proses ini dapat dilihat pada flowchart seperti yang terdapat dalam gambar 3.2.3. berikut:



Gambar 3.6 flowchart pembentukan HEXA GOST hash

Berdasarkan gambar 3.6. sistem akan melakukan pembentukan nilai hash dengan hasil akhir HEXADECIMAL seperti berukut:

Hitung nilai hash dari pesan teks.

Misal hash yang didapat H(m)=4321.

Tentukan nilai acak k dimana k <q.

Pada proses sebelumnya diketahui q=127. Maka permisalan k yang diambil adalah k = 121.

Hitung nilai HEXA r, dengan rumus seperti pada persamaan 2.2.

Maka r= ((23)121 mod 509) mod 127 =103

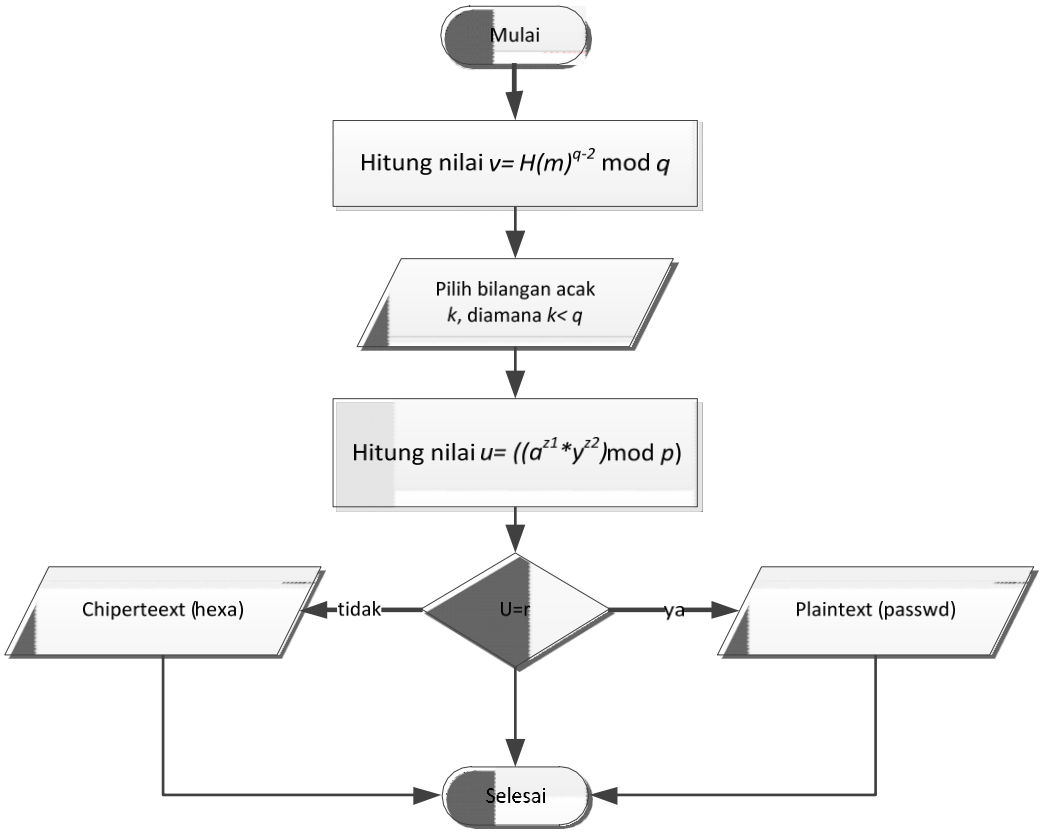
Hitung nilai HEXA s, dengan rumus pada persamaan 2.3.

Maka s =89*103+121(4321) mod 127 = 5

Kemudian kirim pesan m dan HEXA r dan s.

Verifikasi Nilai GOST hash

Proses verifikasi palinteks dan password dibutuhkan untuk membuktikan plainteks tekenkripsi yang secara langsung juga dapat membuktikan keamanan pada database login user. Proses ini dapat dilihat pada flowchart seperti yang terdapat dalam gambar 3.2.4 berikut :



Gambar 3,7 Flowchart verifikasi GOST hash

Berdasarkan gambar 3.7. untuk membuktikan password terenkripsi pada tabel database login user maka dilakukan proses perhitungan sebagai berkut:

Hitung nilai v,

Maka v =4321125 mod 127=85.

Hitung nilai Zi,

Maka Zi = (5*85) mod 127 = 44

Hitung nilai Z2 = ((127-103)*85) mod 127=8.

Dengan diperolehnya nilai Z1 dan Z2 selanjutnya dilakukan perhitungan dari nilai U.

Hitung nilai u,

Maka u = ((2344 *2938) mod 509) mod 127= 103

Dari hasil perhitungan tersebut diketahui bahwa nilai u = 103 dan r = 103, dimana u= r maka dapat disimpulkan bahwa nilai hash tidak berubah.

4. Hasil dan Pembahasan

4.1 Implementasi

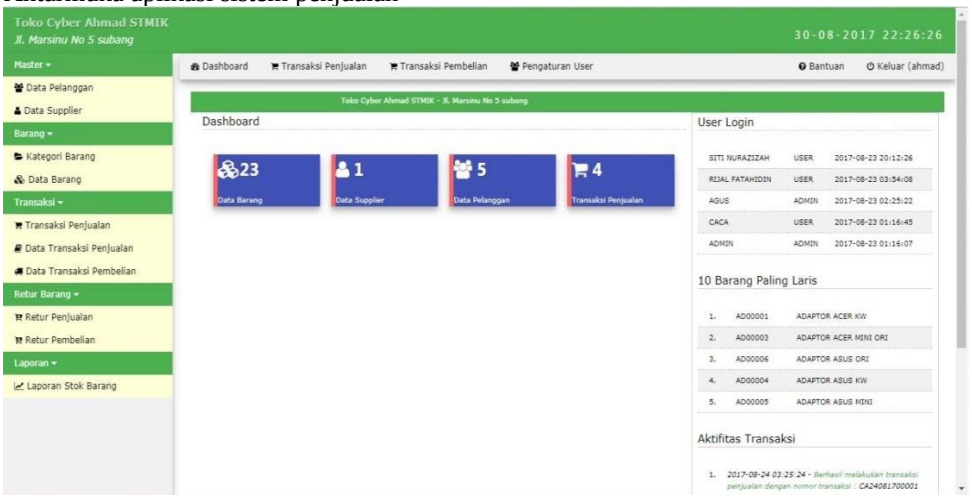
Implementasi antarmuka merupakan penerapan hasil perancangan atau design aplikasi kedalam bentuk interface aplikasi yang dibangun dengan menggunakan perangkat lunak.

1. Login admin

Antarmuka login admin ialah proses utama untuk memulai untuk menggunakan aplikasi untuk melihat isi didalamnya.

Gambar 4.1. Login Admin

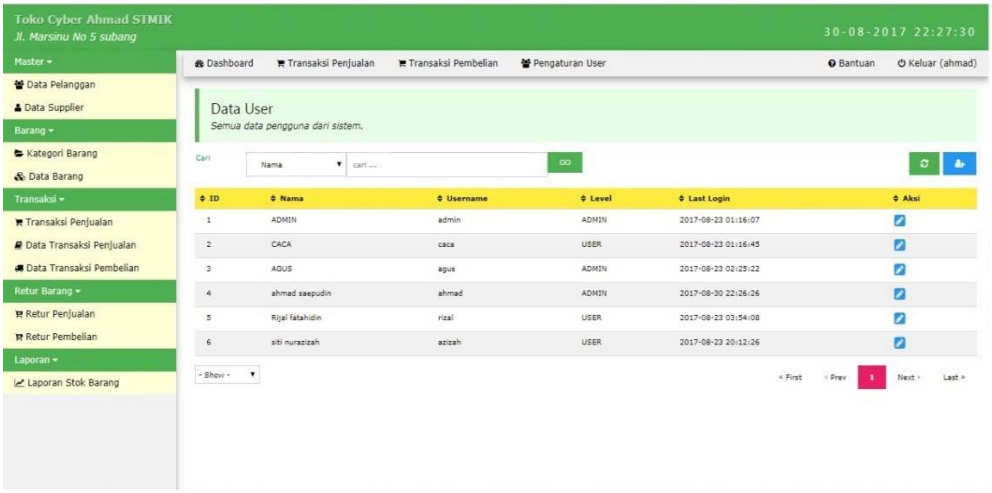
Antarmuka aplikasi sistem penjualan



Gambar 4.1 Antarmuka Aplikasi Sistem Penjualan

Berdasarkan pada gambar, halaman ini adalah antarmuka aplikasi sistem penjualan. Setelah melakukan login maka user dapat memilih dan barang yang di inginkan setelah terpilih barang bisa dimasukan ke keranjang penjualan untuk selanjutnya dilakukan transaksi pembayaran.

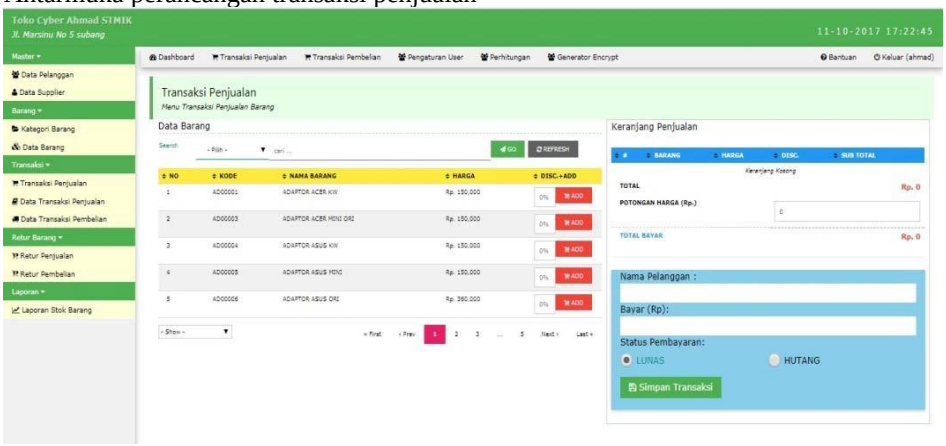
Antarmuka pengaturan user



Gambar4.2 Antarmuka Pengaturan User

Berdasarkan gambar diatas, halaman ini digunakan oleh admin untuk menambahkan user baru, mengedit password, menghapus user dan memperbaharui sistem penjualan.

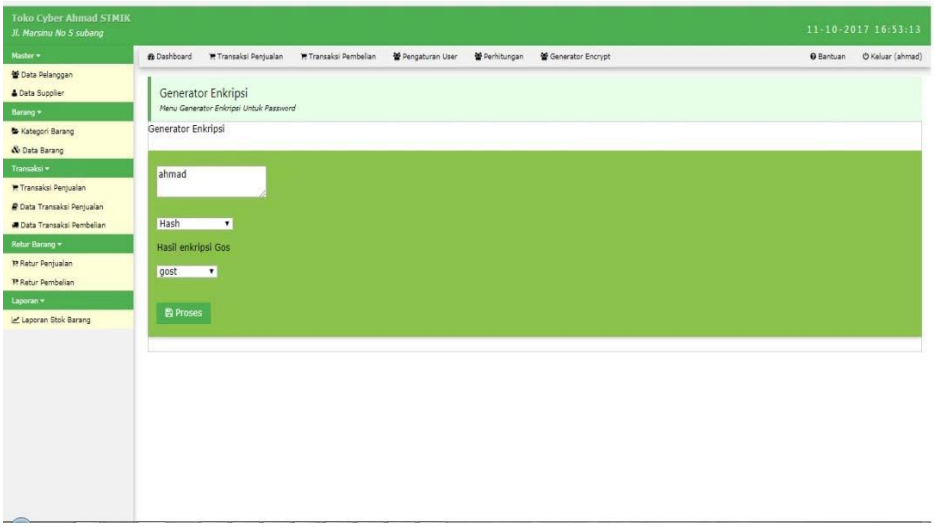
Antarmuka perancangan transaksi penjualan



Gambar 4.3 Antarmuka Perancangan Transaksi

Berdasarkan gambar diatas, halaman ini digunakan oleh user yang akan melakukan transaksi, user akan memilih dulu barang yang akan dibeli lalu dimasukan ke keranjang pembelian dan mendapatkan struk pembelian yang bisa di print langsung secara online oleh user yang sudah melakukan pembayaran.

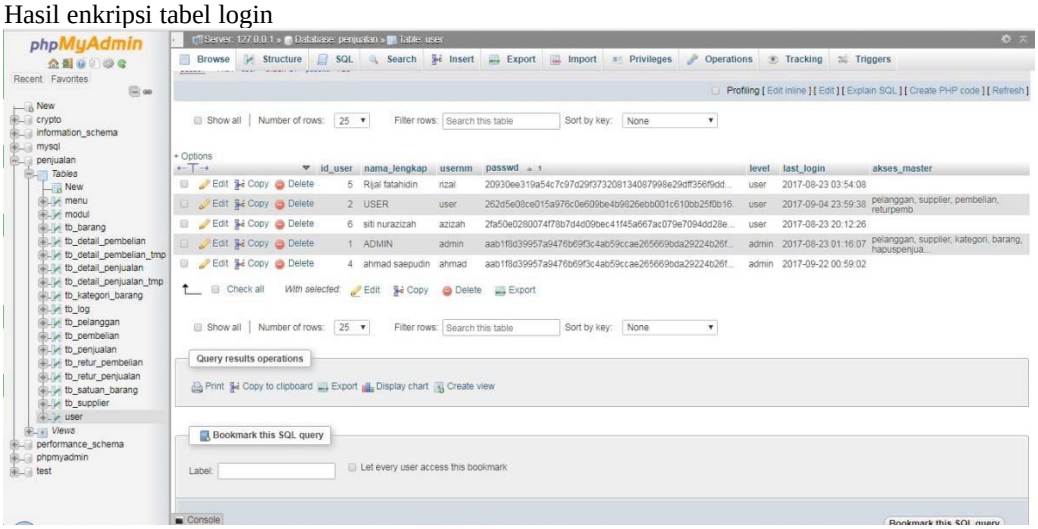
Perancangan antarmuka generator enkripsi



Gambar 4,5 Perancangan Antarmuka Generator Enkripsi

Berdasarkan gambar diatas, halaman ini digunakan untuk mengetahui ke akuratan password hashing yang tersimpan pada tabel database user dalam MYQL. Hasil hashing yang dihasilkan generator harus sama dengan hasil enkripsi yang tersimpan pada tabel database user.

Hasil enkripsi tabel login



Gambar 4.4 Hasil Enkripsi Tabel Database Login

Berdasarkan gambar diatas, gambar memperlihatkan hasil enkripsi pada tabel database login user

Pengujian Sistem

Untuk mengetahui kehandalan kriptografi GOST hash Function, maka dilakukan pengujian dengan beberapa data plainteks seperti pada tabel-tabel dibawah ini.

Tabel 41 Pengujian Sistem

NO	Pesan (Plainteks)	Message digest (64 Sting)
1	ahmad	aab1f8d39957a9476b69f3c4ab59ccae265669bda29224b26fd55002f76d6159
2	Ahmad	68ece293e2f78c80958b951f37684e6789794f9390746181e53f7d5f6cc6e3f0
3	Zuel	220e31f3ca316348a55448cd13c4ff4417d59586cf5fa25a3ac924e11bb9ab13
4	Drew	f1692f9fd5cc2741a27d783761bd856e883c34f647c359b9d9007aa7f4c294ed
5	Andrew	b13e13bd4ca84f6b90b224c53b2c8197a47dab5dfa62b7f74334678f1db527c8
6	Kos	ddc78c2517dafa1aaf4c7121841cef559e63640ae81153e8f475b121c2d0a997
7	Koswara	2e072748995a9438bcd1ce2bd5494fd268af97ff38901ddeabe6ecc30461e403
8	Ojiw	e846296efc42231276610b34ee3dc967ef6c30a7cbe6c9700407a356df7e36a3
9	Oji	c1b8cd7ae3112132f9d84965ae38c16e06ad95b85fbc36cefd208d95dfe7d8bd
10	Med	78593a1ee2d0dac9182e029f94ba2408f81a5eaa9cb12f18ab3e316c772e6096

Tabel4.2 Rekapitulasi Hasil Varifikasi

O	Plainteks		Nilai GOST hash		Nilai Hexa		Hasil Verifikasi
	S	ST	S	ST	S	ST	
	1	0	1	0	1	0	Valid
	1	0	1	0	0	1	Tidak valid
	1	0	0	1	1	0	Tidak valid
	1	0	0	1	1	0	Tidak valid
	0	1	1	0	1	0	Tidak valid
	0	1	1	0	0	1	Tidak valid
	0	1	0	1	1	0	Tidak valid
	0	1	0	1	0	1	Tidak valid

Keterangan: S=sah, ST= Tidak sah, 1= ya, 0= tidak.

Seperti yang terlihat pada tabel 4.2.2. dapat disimpulkan bahwa verifikasi akan valid jika plainteks, nilai GOST hash dan nilai HEXA-nya sah.

5. Kesimpulan

Kesimpulan dari penelitian ini adalah sebagai berikut:

1. Aplkasi ini telah dapat melakukan enkripsi hashing text password untuk melindungi database dari serangan hacker dan cracker yang mencoba untuk melakukan penetrasi pada aplikasi sistem penjualan.
2. Proses enkripsi pada login admin dan user sudah di uji dengan menggunakan generator enkripsi yang sudah dibuat dan terdapat pada aplikasi sistem penjualan.
3. Hasil hashing dan enkripsi pada password login admin dan user dengan GOST (govement standart) menghasilkan output HEXADECIMAL dengan panjang fexed 64 bit. Karakter pesan yang di inputkan dengan panjang maksimal 1024 bit dan akan menghasilkan nilai hashing dengan panjang pesan fixed 64 bit.

Pustaka

A Dmukh, A., M. Dygin, D., & B, G. M. (2017). a lightweight-friendly modifiocation of GOST block cipher. Math-Net.RU, All Russian mathematical portal, 5(2), 47-55.

Asmayunita. (2014). APLIKASI OTENTIKASI DOKUMEN MENGGUNAKAN ALGORITMA GOST DIGITAL SIGNATURE. Universitas Sumatera Utara, 1-63.

Hall, J. A. (2011). The Context-Level Data Flow Diagram (DFD). Dipetik 08 25, 2017, dari library.binus.ac.id: http://library.binus.ac.id/eColls/eThesisdoc/Bab2HTML/2012201245SIBab2001/page10.html

Herryawan, I Putu. (2010). Aplikasi Keamanan Data Menggunakan Metoda Kriptografi Gost. TSI, 1, 138.

Iqbal, M., & Siahaan, A. P. (2016, Oktober). The Understanding of GOST Cryptography Technique The Understanding of GOST Crytography Technique. International Journal of Engineering Trends and Technology (IJETT), 39, 1-6.

Juardi, D. (2013). PENGAMANAN DATA DENGAN PENGGABUNGAN METODE GOST DAN RC6. Politeknik Tri Mitra Karya Mandiri (TMKM), 2(2), 1-9.

Kazymyrov, O., & Kazymyrova, V. (2012). Algebraic Aspects of the Russian Hash Standard GOST R 34.11-2012. Algebraic, 1-18.

Kustian, N. (2014). SISTEM INFORMASI PENGAMANAN BASIS DATA MENGGUNAKAN TEKNIK ENKRIPSI BAGIAN TATA USAHA LEMBAGA SANDI NEGARA. Faktor Exacta, 7(2), 188-199.

Metrology, Federan Agency On Tecnical Regulation and. (2013). Information technology CRYPTOGRAPHIC DATA SECURITY. NATIONAL STANDARD OF THE RUSIAN FEDERATION, 1-38.

Raymond McLeord Jr, G. P. (2007). Management information system 10/e. Dipetik 08 28, 2017, dari whyphi.staff.telkomuniversity: http://whyphi.staff.telkomuniversity.ac.id/files/2015/10/McLeod_CH07p.pdf

Riswaya, A. R. (2001). Sistem Penjualan Tunai Dan Kredit Property Di PT Sanggraha Properti. Computech & Bisnis, 106-116.

Sylviani, Agung, T. B., & Wahyu, N. C. (2011). Pengembangan algoritma kriptografi gost (gosudarstvenny standart) untuk peningkatan keamanan dalam penyandian data. Dokumentasi, Teknik Informatika, Universitas Telkom, 1-6.

T. Courtois, N., & Mourouzis, T. (2013). Propagation of Truncated Differentials in GOST. SECURWARE(C), 156-161.

Widharta, W. P. (2013). Penyusunan strategi dan sistem penjualan dalam rangka meningkatkan penjualan toko damai. Jurnal Manajemen Pemasaran Petra(1), 1-15.