IMPLEMENTASI ALGORITMA KRIPTOGRAFI RC4 UNTUK KEAMANAN DATABASE APLIKASI PENGGAJIAN KARYAWAN BERBASIS WEB PADA PT. TRANS INTRA ASIA

Andre Setiawan[1)], **Titin Fatimah**[2)]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : andrestwn.bl@gmail.com[1)] titin.fatimah@budiluhur.ac.id[2)]

Abstrak

PT. Trans Intra Asia adalah perusahaan yang bergerak di bidang consultant management yang mempuyai 70 karyawan. Setiap bulannya Perusahaan melakukan penggajian terhadap karyawan dimana data yang disimpan dalam database yang memiliki keamanan mudah dicuri karena hanya memakai keamanan database yang sewaktu–waktu bisa saja dicuri atau digunakan oleh pihak yang tidak bertanggung jawab. Jadi perlu dibuat aplikasi keamanan database untuk mengamankan data penggajian karyawan. Teknik kriptografi menjadi salah satu solusi yang perlu digunakan untuk pengamanan database. Adapun metode kriptografi yang digunakan algoritma RC4 (Rivest Code 4) yang termasuk kunci simetris, yaitu kriptografi yang menggunakan kunci enkripsi yang sama dengan dekripsinya. Kelebihan kriptografi kunci simetris adalah proses enkripsi dan dekripsi membutuhkan waktu yang cukup singkat, untuk ukuran kunci simetris relatif lebih pendek dan dapat dipergunakan untuk membangkitkan bilangan acak. Aplikasi ini menggunakan bahasa pemrograman PHP (Hypertext Prepocessor) dengan database MySQL. Hasil penelitian ini menunjukkan bahwa aplikasi penggajian berhasil dibangun dan telah diimplementasikan pada PT. Trans Intra Asia dalam mengamankan data penggajian dengan menggunakan RC4.

Kata kunci: Database, Kriptografi, RC4, Enkripsi, Dekripsi

1. PENDAHULUAN

Saat ini data menjadi sangat penting bagi perusahaan. Banyak perusahaan menggunakan teknologi *database* untuk menyimpan banyak data perusahaannya. Keamaanan data yang di simpan ke dalam database sudah menjadi hal yang dibutuhkan. Namun keamanan database tidak dapat menjamin keamanan data karena kemanan data yang kurang baik sehingga dapat digunakan oleh pihak-pihak yang berhubungan dengan database seperti data penggajian.

Kriptografi secara umum digunakan dalam keamananya data, teknik yang digunakan adalah mengubah data dalam bentuk yang sulit dipahami dengan menggunakan kunci asimetris dalam proses enkripsi dan dekripsinya. Kriptografi merupakan ilmu yang mempelajari membuat pesan yang dikirim oleh pengirim dapat disampaikan oleh penerima dengan aman [1].

Perkembangan penggunaan database berbarengan dengan keharusan pemahaman akan keamanan database. Masih banyak lembaga atau instansi yang mengabaikan keamanan database, sehingga data yang ada bisa diakses oleh orang yang tidak bertanggung jawab. Banyak cara yang dilakukan untuk bisa mengamankan data tersebut.

Penelitian dilakukan di PT. Trans Intra Asia, yang merupakan salah satu perusahaan konsultan terkemuka di Indonesia. Dalam lebih dari 35 tahun keberadaannya, ia telah membangun reputasi yang sangat baik terutama karena para spesialis yang luar biasa pada stafnya dan di antara rekanannya, kinerja yang secara konsisten baik dalam perencanaan dan pelaksanaan proyek, serta staf manajemen dan dukungan yang kuat dan berdedikasi tinggi. Sehingga data–data perusahaan disimpan kedalam database yang memiliki keamanan kurang baik,

PT. Trans Intra Asia menggunakan *database* yang keamanannya kurang aman. Pihak pihak yang tidak bertanggung jawab dengan dapat mengakses *database* dengan mudahnya karena tidak ada keamanan lebih. PT. Trans Intra Asia mempunyai data yang sangat penting jika data perusahaan mudah dicuri akan merugikan PT. Trans Intra Asia. Data perushaan berisi data karyawan, data penggajian dan data *client*. Data gaji karyawan adalah data yang sangat penting karena dalam data penggajian terdapat seperti data nik, data telefon, dan data pribadi lainnya, yang berbahaya adalah penggajian karyawan dimana jika data tersebut dicuri oleh pihak yang tidak bertanggung jawab yang dapat mengakibatkan banyak kerugian pada PT. Trans Intra Asia, karena kompetitor perusahaan PT. Trans Intra Asia dapat mengetahui data penggjiankaryawan dapat menarik karyawan dengan jumlah gaji yang mungkin melebihi gaji yang sebelumnya. Karena itu sangat di butuhkan untuk mengamankan database penggajian.

Algoritma RC4 termasuk kedalam kriptografi kunci simetris, yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Kelebihan kunci simetris adalah untuk proses enkripsi dan dekripsi dibutuhkan waktu yang cukup singkat, untuk ukuran kunci simetris relative lebih pendek dan dapat dipergunakan untuk membangunkan

bilangan acak, kunci simetris disusun untuk menghasilkan cipher yang lebih kuat.

1.1. Perumusan Masalah

Terdapat beberapa permasalahan yang menjadi titik utama dalam melakukan penelitian ini, sebagai berikut:

a. Bagaimana menerapkan algoritma RC4 dalam mengamankan data penggajian dalam database?
b. Bagaimana cara mengembalikan data yang sudah dienkripsi dengan tidak merubah data asli (dekripsi)?
c. Bagaimana cara membangun aplikasi sistem keamanan dengan menggunakan Algoritma RC4 berbasis web?

1.2. Batasan Masalah

Terdapat batasan-batasan masalah dalam penelitian ini, sebagai berikut:

a. Algoritma yang digunakan adalah RC4.
b. Aplikasi ini digunakan untuk enkripsi dan dekripsi data penggajian menggunakan RC4
c. Aplikasi ini berbasis web dan dijalankan mengunakan browser.
d. Bahasa pemograman yang digunakan adalah PHP (Hypertext Prepocessor)

1.3. Tujuan Penulisan

Adapun maksud dan tujuan dari penelitian ini, sebagai berikut:

a. Menerapkan Algoritma RC4 dalam mengamankan data penggajian pada database
b. Menengembalikan isi data di enkripsi tanpa merubah isi datanya.
c. Untuk mengetahui implementasi metode RC4 dalam pemangaman data.

2. Landasan Teori

2.1. Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu: "*cryptos*" adalah "*secret*" (rahasia) dan "graphein" adalah "*writing*" (tulisan). Jadi kriptografi yaitu ilmu dan seni untuk mengamanan pesan [2].

Kriptografi mempunyai dua konsep penting yaitu proses enkripsi dan proses dekripsi. Enkripsi adalah proses informasi atau data yang terkirim lalu diubah data menjadi bentuk yang sulit diketahui sebagai informasi dengan menggunakan algoritma tertentu. Dekripsi adalah mengubah informasi yang tersamar tersebut menjadi informasi awal. data yang asli dan belum melakukan perubahan dengan kriptografi dikenal sebagai *plaintext*. Kemudian setelah disamarkan oleh kriptografi, oleh *plaintext* disebut dengan *chipertext*. Proses perubahan *plaintext* menjadi *ciphertext* dapat disebut dengan enkripsi (*encryption*), dan proses dikembalikan ke *ciphertext* menjadi *plaintext* kembali dinamakan dekripsi (*decryption*).

kriptografi klasik biasanya menggunakan metode subtitusi atau transposisi yang telah digunakan sebelum adanya komputer ditemukan. Berisikan beberapa komponen utama dalam kriptografi. Secara umum, istilah kriptografi yang digunakan adalah sebagai berikut; [3]

a. Pesan
   Pesan adalah informasi yang dapat dengan mudah dibaca dan dimengerti maksudnya, pesan sering disebut juga dengan *plaintext*. Plaintext merupakan pesan yang bermakna akan langsung diproses menggunakan algoritma kriptografi.
b. *Ciphertext*
   Cipertext bisa disebut dengan *cryptosystem* adalah pesan yang telah berisi sandi. Pesan diubah bentuk *ciphertext* sulit dibaca karena berisi karakter-karekter yang tidak mempunyai makna setelah proses enkripsi
c. Enkripsi
   Enkripsi adalah penyandian plaintext diubah menjadi *ciphertext* atau bisa disebut dengan enciphering. Enkripsi dilakukan dengan maksud plaintext tersebut sulit dibaca oleh pihak yang tidak memiliki otoritas (wewenang).
d. Dekripsi
   Dekripsi adalah mengembalikan ciphertext diubah menjadi plaintext seperti awal atau bias disebut deciphering. Dekripsi akan dilakukan ketika pesan sampai kepada pihak tertentu.
e. Kunci (*key*).
   Kunci (*key*) merupakan parameter yang dapat digunakan untuk transformasi enkripsi dan dekripsi. Kunci merupakan string atau deretan bilangan. Keamanan kriptografi biasanya tergantung kerahasiaan dalam memberikan key.
f. Kriptosistem (*cryptosystem*)
   Cryptosystem merupakan implementasi perangkat lunak algoritma kriptografi yang dibutuhkan atau mentranformasi pesan asli yang menjadi ciphertext atau bisa sebaliknya.

2.2. Database

Database adalah sekumpulan file yang berhubungan dan terorganisasi atau sekumpulan record-record yang dapat menyimpan data dan hubungan diantaranya. [4]

Database memilki entitas, atribut, dan relasi. Entitas adalah objek yang berbeda yang terdapat pada sebuah database (orang, tempat, benda, konsep, atau peristiwa). Atribut adalah properti yang menjelaskan beberapa aspek dari sebuah objek yang ingin direkam. Relasi adalah hubungan antara suatu entitas dengan entitas lainnya.

2.3. Algoritma RC4

Algoritma RC4 (*Rivest code* 4) adalah jenis aliran kode yang merupakan operasi enkripsinya dilakukan karakter 1 byte bisa untuk sekali operasi. Algoritma Rivest Code 4 (RC4) yaitu kunci simetris yang dibuat *RSA Data Security Inc* (RSADSI) yang berupa stream cipher. Algoritma telah ditemukan pada tahun 1987 oleh Ronald Rivest dan merupakan simbol keamanan RSA (adalah singkatan dari tiga

nama penemu yaitu Rivest, Shamir, dan Adleman) [5].

Secara garis besar RC4 Stream Cipher dibedakan menjadi dua, adalah *Key Setup* atau *Key Schedulling* Algorithm (KSA) dan Stream Generation atau *Pseudo Random Generation Algorithm* (PRGA) dan proses XOR dengan stream data.

Dalam penggunaan metode RC4 untuk mengenkripsi tergolong cepat. Selain cepat, waktu yang digunakan RC4 tidak berpengaruh dengan panjang *keylength* yang dipakai. *Byte* K di-XOR-kan dengan *plaintext* dapat menghasilkan *ciphertext* atau di-XOR-kan dengan *ciphertext* untuk menghasilkan *plaintext*. Enkripsi sangat cepat kurang lebih 10 kali lebih cepat dari DES [6].

3. Analisa Masalah Dan Rancangan Program

3.1. Analisa Masalah

Kemajuan berpikir manusia membuat masyarakat sadar bahwa teknologi informasi adalah salah satu alat dalam kemajuan manusia untuk dapat mengatasi masalah penggunaan informasi. Teknologi informasi mempunyai potensi besar dalam mengubah data menjadi informasi, teknologi informasi dapat melakukan menyimpan data atau pesan dalam bentuk yang tidak dimengerti oleh pihak yang tidak bertanggung jawab. Hal ini dilakukan untuk menjaga informasi agar lebih aman dan terjaga dari pencurian. PT. Trans Intra Asia adalah perusahaan yang bergerak dibidang konsultan. Perusahaan meyimpannya data dalam *database*, memiliki keamanan yang kurang baik, sehingga data tersebut dapat digunakan pihak yang tidak bertanggung jawab. Maka dengan penggunaan aplikasi yang dapat mengamankan data yang ada di *database*. Dalam proses pembuatan keamanan *database* pada perusahaan PT. Trans Intra Asia menggunakan metode algoritma RC4.

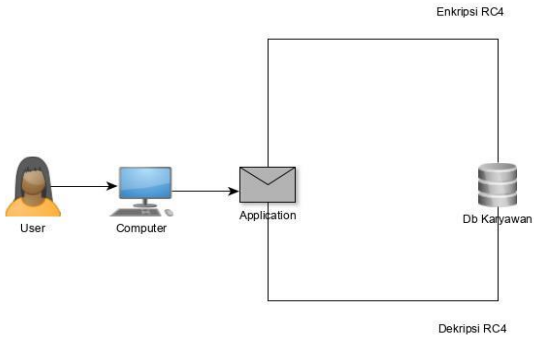
3.2. Penyelesaian Masalah

Permasalahan yang sudah dilakukan diatas maka, diperlukan adanya aplikasi yang dapat mengamankan isi data penggajian ke dalam *database* sehingga kerahasiaan data tersebut sulit untuk dibaca atau sulit diketahui oleh pihak-pihak yang tidak bertanggung jawab dalam keamanan database tersebut. Aplikasi tersebut nantinya akan mengubah data pengajian karyawan didalam database asli menjadi data karyawan yang isinya sulit untuk diketahui dan sulit untuk diketahui isi data tersebut sehingga terjaga kerahasiaan data. Kemudian menampilkan data penggajian menjadi data awal tanpa mengalami perubahan dalam isi data.

Dalam aplikasi ini, menggunakan algoritma RC4 sebagai metode kriptografi. Algoritma RC4 merupakan teknik kriptografi menggunakan kunci yang sama untuk mengekripsi atau mendekripsi pesan, data, ataupun informasi. Agar data penggajian didalam database bisa dienkripsi menjadi data *chipertext* dan mengembalikannya menjadi data semula, data dalam *database* terenkripsi terjadi jika saat enkripsi dan *text* dalam *database* menjadi *plaintext* setelah melakukan dekripsi. Untuk membangun aplikasi yang terkomputerisasi, digunakan bahasa pemrograman PHP dan menggunakana *database* Mysql sebagai pendukungnya.

3.3. Arsitektur Sistem

Untuk memudahkan dalam memahami cara kerja aplikasi yang akan dibuat maka bisa dilihat pada gambar arsitektur sistem yang menggambarkan konsep kerja aplikasi secara keseluruhan sistem



Gambar 1. Arsitektur Sistem

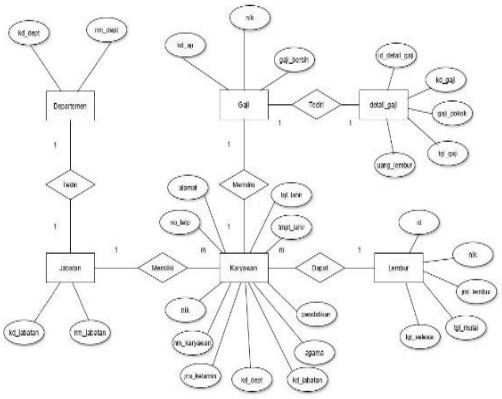
Berikut ini adalah tahapan proses enkripsi dan dekripsi aplikasi penggajian sebagai berikut:

a. *User* harus melakukan *login* ke web aplikasi penggajian
b. Jika berhasil *login*, user masuk kedalam halaman aplikasi penggajian
c. Entry dan update data yang sudah disediakan dalam aplikasi tersebut
d. Jika data berhasil diinput dan diupdate maka data akan terenkripsi kedalam database dan tampilan aplikasi penggajian akan terdekripsi.

3.4. Rancangan database

a. ERD (*Entity Relationship Diagram*)

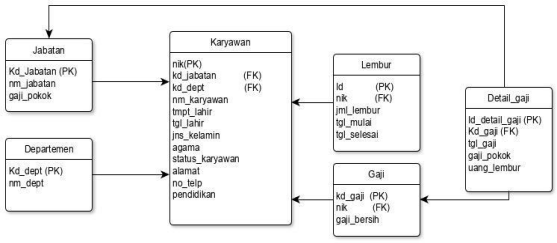
Berikut rancangan ERD (*Entity Relationship Diagram*) sebagai berikut:



Gambar 2. ERD (Entity Relationship Diagram)

b. LRS (*Logical Record Structured*)

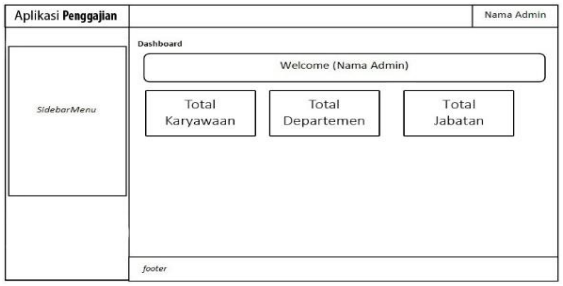
Bentuk diagram ERD (*Entity Relationship Diagram*) yang sudah menjadi LRS (*Logical Record Structured*) sebagai berikut:



Gambar 3. LRS (Logical Record Structured)

3.5. Rancangan Layar

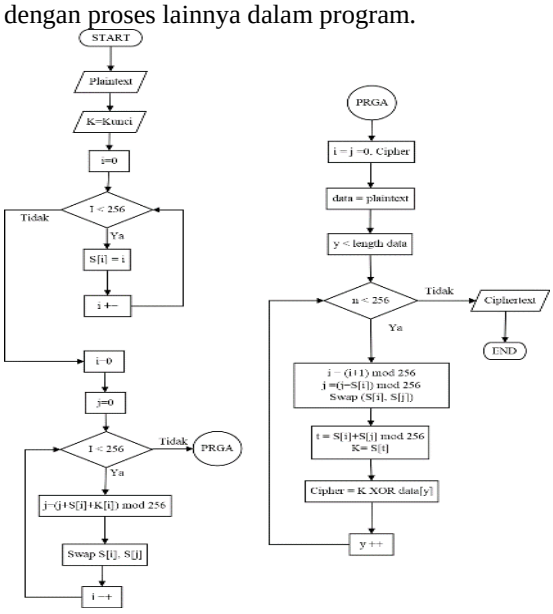
Sebelum memasuki tahap pembuatan haruslah dibentuk rancangan layar yang bertujuan untuk dapat memberikan yang mengambarkan tentang program yang dibuat. Agar dalam menggunakan merasa nyaman dalam mengoperasikannya sehingga rancangan layar tidak membingungkan pengguna dan tidak mengalami kesulitan dalam menggunakan atau mengoperasikan aplikasi ini.



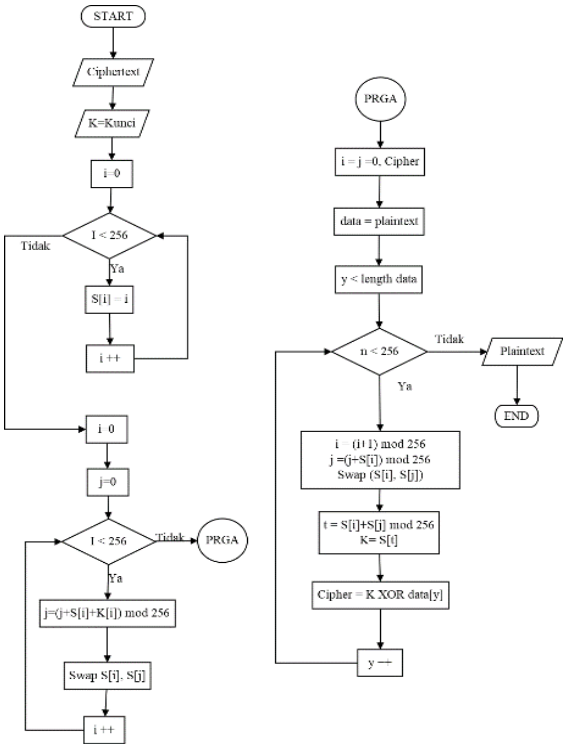
Gambar 4. Rancangan Halaman Utama

3.6. *Flowchart*

Suatu bagan dengan menggunakan simbol tertentu yang menggambarkan proses alur secara *detail* dan penghubung antara proses (instruksi) dengan proses lainnya dalam program.



Gambar 5. Flowchart Enkripsi RC4



Gambar 6. Flowchart Dekripsi RC4

Dalam *flowchart* ini dapat menggambarkan jalannya proses enkripsi dan dekripsi dimulai dari menambahkan data dan mengubah data, lalu diproses enkripsi dan dekripsi melalui RC4 (Rivest Code).

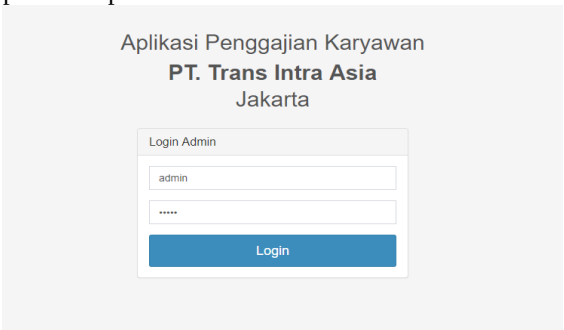
4. IMPLEMENTASI DAN UJI COBA PROGRAM

4.1 Tampilan Layar

Dalam tampilan layar, dapat diuraikan tentang tampilan layar mulai dari pertama kali aplikasi dijalankan hingga selesai. Berikut ini akan diberikan penjelasan gambar mengenai tampilan yang ada pada aplikasi penggajian ini.

a. Tampilan *Form Login*

Tampilan layar dari *from login* pada saat muncul pada saat pertama kali web diakses

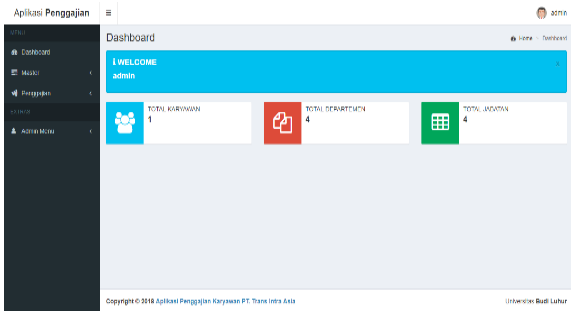


Gambar 7. Form Login

b. Tampilan Halaman *Dashboard*

Tampilan halaman dashboard keluar ketika *user login* mengisikan *username* dan *password* yang berisi sesuai data dengan yang ada di *database*. Pada halaman *dashboard*, admin diberikan akses untuk beberapa akses untuk beberapa menu yaitu akses ke

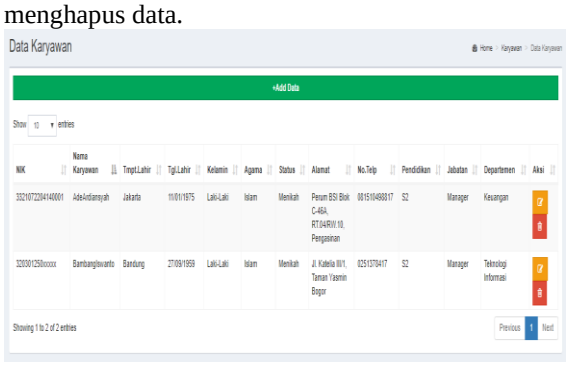
data master, mengelola departemen, mengelola jabatan, mengelola karyawan, mengelola lembur dan mengelola data gaji karyawan.



Gambar 8. Tampilan halaman dashboard

c. Tampilan Halaman Karyawan

Tampilan layar form data karyawan. Pada menu data karyawan dapat melakukan tambah data dengan menginput dan menggunakan menu add data. Untuk mengubah dan menghapus halaman data karyawan dengan melakukan pilih salah satu data yang ada didalam tabel dan menggunakan klik tombol ubah untuk mengubah isi data, tombol hapus digunakan untuk menghapus data dan tombol batal dilakukan untuk membatalkan apabila terjadi kesalahn input atau tidak jadi mengubah dan menghapus data.



Gambar 9. Tampilan Layar karyawan

4.2 Hasil Uji Coba Program

Data-data yang sudah dimasukan kedalam data uji coba untuk program keamanan database sudah dalam bentuk enkripsi. Berikut ini merupakan hasil data yang telah diuji sebagai data uji.

a. Hasil Pengujian Tabel Departemen

Hasil pengujian tabel departemen, data record yang berada pada nama departemen sudah dalam bentuk enkripsi

kd_dept	nm_dept
DEP0003	•œL
DEP0002	•Øt7í$‡¡?K
DEP0001	xjì¼(À•½

Gambar 10. Tampilan Database Departemen Terenkrip

b. Hasil Pengujian Tabel Jabatan

Hasil pengujian tabel jabatan, data record yang berada pada nama jabatan sudah dalam bentuk enkripsi

kd_jabatan	nm_jabatan	gaji_pokok
JTN0001	ûâƒº+p	‡»ÁXáRn
JTN0002	DÀQ¹ÚVï	?”è•-
JTN0003	W˜s¯ÒTÒ<	+Ý&íƒ•
JTN0004	“•&Ìd	áÌ{•:³Ñ
JTN0005	Ð·*	-Ð^âMŸ
JTN0006	Yú•ê‰{-Ù^×	>ºÝ¿Ë=Ï

Gambar 11. Tampilan Database Jabatan Terenkrip

4.3 Analisis Hasil Program

Bedasarkan pengujian program sistem keamanan *database* pada data penggajian yang sudah dilakukan, didapati kelebihan dan kekurangan program, yaitu sebagai berikut:

a. Kelebihan Program

Kelebihan yang dimiliki pada aplikasi ini adalah sebagai berikut:

1) Terdapat autentikasi *Username* dan *Password* pada *Form Login*.
2) Program yang *user friendly*, karena memilik tampilan yang sederhana dan jelas.
3) Data perusahaan akan aman jika menggunakan aplikasi ini, Karena aplikasi ini sudah menggunakan sistem keamanan database. Data yang dihasilkan didalam database dalam bentuk enkripsi sehingga data sulit dicuri

b. Kekurangan Program

Kekurangan yang dimiliki aplikasi ini adalah sebagai berikut:

1) Aplikasi ini hanya digunakan pada *database* yang sudah ditentukan database user.
2) Tidak semua *field* (kolom) dapat dienkripsi

5. PENUTUP

Berdasarkan hasil penelitian dan pembahasan penerapan sistem keamanan database dengan menggunakan metode Algoritma Rivest Code 4(RC4) untuk mengamankan database dari pencurian data atau memanipulasi data agar aman, dapat diambil kesimpulan dan saran.

5.1 Kesimpulan

Selesai dengan pembahasan mengenai Implementasi Algoritma Kriptografi RC4 Untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis Web Pada PT. Trans Intra Asia, maka kesimpulan yang dapat diambil sebagai berikut:

a. Aplikasi penggajian karyawan ini telah berhasil dibangun dan telah diimplementasikan pada PT. Trans Intra Asia dalam mengamankan data menggunakan RC4

b. akan lebih terjaga kerahasiaan data-data perusahaan karena melalui enkripsi lebih dahulu sehingga data penggajian terhindar dari pencurian data atau dapat diketahui oleh pihak yang tidak bertanggung jawab.
c. Aplikasi ini dibangun sebagai alat bantu bagi perusahaan untuk mengamankan data penggajian agar terjaga kerahasiaan data yang penting di PT. Trans Intra Asia

5.2 Saran

Selain menarik beberapa kesimpulan, ada beberapa saran yang bisa dijadikan pertimbangan dalam mengembangkan aplikasi sistem keamanan database sebagai berikut:

a. Karena dalam pembuatan program ini memiliki keterbatasan, sebaiknya program lebih disempurnakan, agar hasil tidak hanya dilihat didalam web saja, tetapi dapat dilihat melalui smartphone.
b. Perbaikan dalam proses enkripsi dapat lebih luas lagi yaitu pada bagian pilihan *field* (kolom) yang akan diproses untuk diterapkan dengan mengenkrip semua *field* (kolom) sesuai keinginan

6. DAFTAR PUSTAKA

[1] Schneier, B., 1996 Applied Cryptography Second edition: Protocol, Algorithm, and Source code in C, John Wiley and Son
[2] Munir, Rinaldi. 2008. Belajar Ilmu Kriptografi. Yogyakarta: Penerbit Andi
[3] Munir, Rinaldi. 2006. Diktat Kuliah Kriptografi. Bandung: Program Studi Tenik Informatika, Institut Teknologi Bandung
[4] Sutarman. 2012. Pengantar Teknologi Informasi. Jakarta: PT. Bumi Aksara.
[5] Ariyus, D. 2008. Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi. Yogyakarta; Andi
[6] Suryani, K.N., 2009, Algoritma RC4 Sebagai Metode Enkripsi, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika ITB, Bandung