Pengamanan Database Pada Aplikasi Test Masuk Karyawan Baru Berbasis Web Menggunakan Algoritma Kriptografi AES-128 Dan RC4

Geri Grehasen [1)], Sri Mulyati [2)]
[1,2]Program studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl Raya Ciledug, Petukangan Utara Jak- Sel, 12260
E-mail : gerigrehasen@gmail.com[1)], sri.mulyati@budiluhur.ac.id[2)]

Abstract

PT. Daliny Cipta Karya is a company engaged in the retail sector. The company has several stores scattered in various parts of the city. Because it has stores in various parts of the city then the company needs more employees, especially for the position SPG (sales promotion girl), cashier and admin. This makes the selection of the company held a sign test new employees almost every week. Selection of new employees in the company is done conventionally, ie prospective employees follow the written test at the time and place specified in advance. Thus the selection test is required online application that can simplify the selection process of new employees. To maintain the security of test questions can use cryptographic methods to encrypt the matter so as not to be seen by those who are not responsible. Applications built using the AES algorithm (Advanced Encryption Standard) 128 and the RC4 algorithm to encrypt the matter. Problem will be encrypted with AES-128 method beforehand after it is encrypted again with RC4 method. Ciphertext encrypted form that can not be read by people who are not responsible. To return to form of all, the matter must be at RC4 decryption method, only then decrypt with AES-128 method. The results of the implementation of the AES-128 algorithm and the RC4 on the company can help the selection process of new employees of PT. Daliny Cipta Karya became more assured because of security.

***Keywords**: AES-128, RC4, encryption, decryption.*

Abstrak

PT. Daliny Cipta Karya merupakan perusahaan yang bergerak di bidang retail. Perusahaan ini memiliki beberapa toko yang tersebar di berbagai penjuru kota. Karena memiliki toko di berbagai penjuru kota maka perusahaan tersebut membutuhkan banyak karyawan, khususnya untuk posisi SPG (sales promotion girl), kasir dan admin. Hal ini membuat perusahaan mengadakan seleksi test masuk karyawan baru hampir setiap minggu. Seleksi karyawan baru pada perusahaan tersebut dilakukan secara konvensional, yaitu calon karyawan mengikuti test tertulis pada waktu dan tempat yang telah ditentukan sebelumnya. Maka dari itu diperlukan aplikasi seleksi test online yang dapat mempermudah proses seleksi karyawan baru. Untuk menjaga keamanan soal test dapat menggunakan metode kriptografi untuk mengenkripsi soal tersebut sehingga tidak dilihat oleh pihak yang tidak bertanggungjawab. Aplikasi yang dibangun ini menggunakan algoritma AES (Advanced Encryption Standard) 128 dan algoritma RC4 untuk mengenkripsi soal tersebut. Soal akan di enkripsi dengan metode AES-128 terlebih dahulu setelah itu di enkripsi kembali dengan metode RC4. Hasil enkripsi berupa ciphertext yang tidak bisa dibaca oleh orang yang tidak bertanggung jawab. Untuk mengembalikan ke bentuk semua, soal harus di dekripsi dengan metode RC4, setelah itu baru di dekripsi dengan metode AES-128. Hasil dari implementasi algoritma AES-128 dan RC4 pada perusahaan dapat membantu proses seleksi karyawan baru PT. Daliny Cipta Karya menjadi lebih terjamin keamanannya.

***Kata kunci** : AES-128, RC4, enkripsi, dekripsi.*

1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi saat ini sangat membantu dalam menyelesaikan banyak pekerjaan dengan cepat, akurat, dan efisien. Salah satu aspek yang paling penting dalam dunia teknologi informasi adalah keamanan data. Salah satu ilmu pengamanan data yang terkenal adalah kriptografi. Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan, data, atau informasi dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna.

PT. Daliny Cipta Karya merupakan perusahaan yang bergerak dibidang *retail*. Perusahaan ini hampir setiap minggu mengadakan seleksi test masuk karyawan baru. Seleksi karyawan baru pada perusahaan tersebut dilakukan secara konvensional, yaitu calon karyawan mengikuti test tertulis pada waktu dan tempat yang telah ditentukan sebelumnya. Proses test yang dilakukan dengan

cara seperti itu tentu saja masih mengalami beberapa masalah diantaranya, lamanya proses pengolahan hasil test, memungkinkan terjadinya kesalahan ketika melakukan proses pengolahan hasil test, dan adanya kemungkinan manipulasi hasil test oleh pihak yang tidak bertanggung jawab. Untuk itu dibutuhkan aplikasi penunjang yang dapat membantu mengatasi masalah tersebut.

Berdasarkan pernyataan diatas dibutuhkan aplikasi yang dapat membantu seleksi test masuk yang bersifat tertulis menjadi bersifat *online*. Namun perlu diperhatikan pula keamanan soal test agar tidak sembarang pihak bisa mengetahui isi soal tersebut.

Dari uraian latar belakang masalah di atas, maka dapat dikemukakan beberapa identifikasi masalah :

a. Bagaimana mengubah cara seleksi test masuk PT. Daliny Cipta Karya dengan tidak menggunakan cara konvensional?
b. Bagaimana cara mengamankan soal pada seleksi test online agar tidak sembarang pihak mengetahui isi dari soal tersebut?

Dari permasalahan yang ada pada rumusan masalah, maka penulis bertujuan:

a. Mengembangkan sistem seleksi test masuk menjadi bersifat *online.*
b. Menambahkan keamanan sistem seleksi test masuk dengan menggunakan algoritma AES-128 dan RC4.

Untuk melakukan pengembangan sistem dilakukan hal-hal berikut ini :

a. Studi Literatur
   Melalui studi literatur diperoleh data atau informasi dengan mengumpulkan, mempelajari dan membaca berbagai referensi baik itu dari buku-buku, jurnal, makalah, *internet* dan berbagai sumber lainnya yang menunjang dalam penulisan ini.
b. Analisis Masalah
   Merupakan tahap dimana proses pengumpulan data dilakukan, identifikasi masalah, dan analisis kebutuhan sistem. Tahap ini bertujuan untuk menentukan solusi yang didapat dari aktivitas-aktivitas tersebut.
c. Perancangan Sistem
   Pada tahap ini dilakukan pemodelan perangkat lunak. Tujuan dari pembuatan model ini adalah untuk dapat menjamin keamanan data dan memberi gambaran seperti apa tampilan aplikasi yang akan dibuat.
d. Pemrograman (pengkodean)
   Dalam tahap ini penulis melakukan proses implementasi dari tahapan desain sistem ke dalam bahasa pemrograman PHP. Pada tahap *coding* penulis menggunakan *editor* notepad++, dan *localhost* menggunakan XAMPP serta MySQL untuk basis data nya.
e. Pengujian Sistem
   Pengujian dilakukan dengan melakukan beberapa tes pengujian aplikasi dan mencari kesalahan atau kekurangan dari aplikasi yang dibuat sehingga aplikasi tersebut dapat berjalan sesuai yang diinginkan.

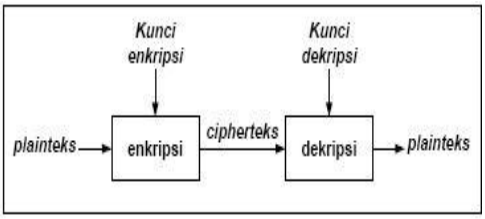
2. LANDASAN TEORI

2.1. Pengertian Kriptografi

Kata *cryptography* berasal dari bahasa Yunani: *"crypto"* artinya tersembunyi atau rahasia (*hidden* atau *secret*) dan *"graphia"* artinya tulisan (*writing*). Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (*message*)[1]. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi [2].

Sistem kriptografi (*cryptosystem*) terdiri dari algoritma kriptografi, *plaintext*, *ciphertext*, dan kunci. Algoritma kriptografi (*cipher*) adalah aturan untuk *enciphering* dan *deciphering*, atau fungsi matematika yang digunakan untuk *encrypt* dan *decrypt* pesan. *Plaintext* adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. *Ciphertext* adalah pesan yang telah disandikan sehingga tidak dapat dibaca oleh pihak yang tidak berhak [3].

Sistem kriptografi (*cryptosystem*) terdiri dari algoritma kriptografi, *plaintext*, *ciphertext*, dan kunci. Algoritma kriptografi (*cipher*) adalah aturan



untuk *enciphering* dan *deciphering*, atau fungsi matematika yang digunakan untuk *encrypt* dan *decrypt* pesan. *Plaintext* adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. *Ciphertext* adalah pesan yang telah disandikan sehingga tidak dapat dibaca oleh pihak yang tidak berhak [4].

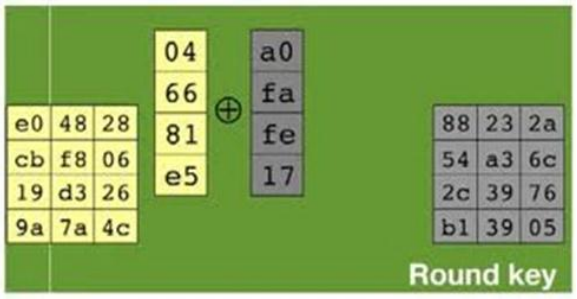
Gambar 1 : Proses encrypt dan decrypt

2.2. Algoritma AES-128

AES-128 (Advanced Encryption Standard) adalah lanjutan dari algoritma DES (Data Encryption Standard) yang masa berlakunya dianggap telah usai karena faktor keamanan. *AES-128* ini merupakan algoritma block *cipher* dengan menggunakan sistem permutasi dan substitusi (P-*Box* dan *S-Box*) bukan dengan jaringan Feistel sebagaimana *block cipher* pada umumnya. Pengelompokkan jenis *AES-128* ini adalah berdasarkan panjang kunci yang digunakan. Angka-angka di belakang kata *AES* menggambarkan panjang kunci yang digunakan pada tipa-tiap *AES*. Selain itu, hal yang membedakan dari masing-masing *AES* ini adalah banyaknya *round* yang dipakai. *AES*-128 menggunakan 10 *round*, *AES*-192 sebanyak 12 *round*, dan *AES*-256 sebanyak 14 *round*. [5].

a. AddRoundKey

AddRoundKey pada dasarnya adalah mengkombinasikan *ciphertext* yang sudah ada dengan *cipherkey* dengan operasi XOR.

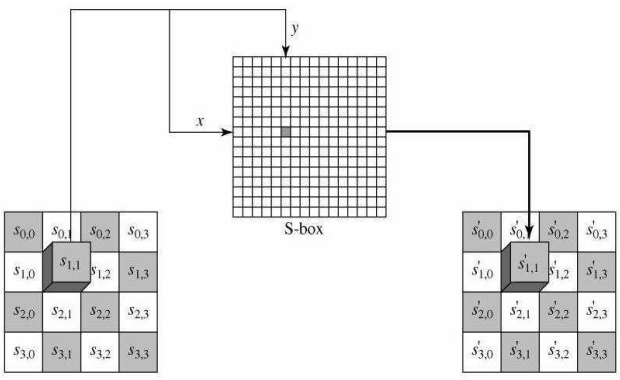


Gambar 2: Skema AddRoundKey

Pada gambar tersebut di sebelah kiri adalah ciphertext dan sebelah kanan adalah roundkeynya. XOR dilakukan perkolom yaitu kolom-1 ciphertext diXOR dengan kolom-1 roundkey dan seterusnya.

b. SubBytes

Prinsip dari *SubBytes* adalah menukar isi matriks/tabel yang ada dengan matriks/tabel lain yang disebut dengan *Rijndael S-Box*. Di bawah ini adalah contoh ilustrasi *SubBytes*.

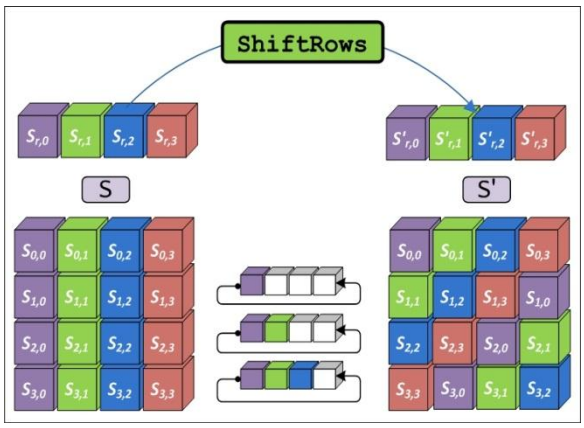


Gambar 3: Ilustrasi SubBytes

Pada setiap *s-box* terdapat nomor kolom dan nomor baris. Seperti yang telah disebutkan sebelumnya, tiap isi kotak dari blok *cipher* berisi informasi dalam bentuk heksadesimal yang terdiri dari dua digit, bisa angka-angka, angka-huruf, ataupun huruf-angka yang semuanya tercantum dalam *Rijndael S-Box*. Langkahnya adalah mengambil salah satu isi kotak matriks, mencocokkannya dengan digit kiri sebagai baris dan digit kanan sebagai kolom. Kemudian dengan mengetahui kolom dan baris, kita dapat mengambil sebuah isi tabel dari *Rijndael S-Box*. Langkah terakhir adalah mengubah keseluruhan blok *cipher* menjadi blok yang baru yang isinya adalah hasil penukaran semua isi blok dengan isi langkah yang disebutkan sebelumnya.

c. ShiftRows

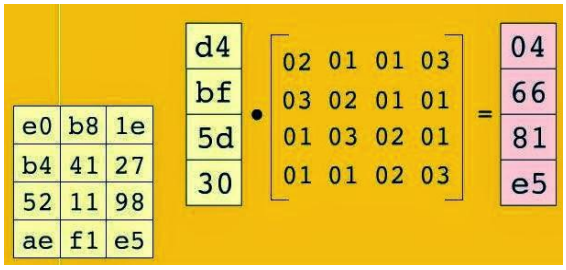
ShiftRows adalah sebuah proses yang melakukan *shift* atau pergeseran pada setiap elemen blok/tabel yang dilakukan per barisnya. Yaitu baris pertama tidak dilakukan pergeseran, baris kedua dilakukan pergeseran 1 byte, baris ketiga dilakukan pergeseran 2 byte, dan baris keempat dilakukan pergeseran 3 byte. Pergeseran tersebut terlihat dalam sebuah blok adalah sebuah pergeseran tiap elemen ke kiri tergantung berapa byte tergesernya, tiap pergeseran 1 byte berarti bergeser ke kiri sebanyak satu kali. Ilustrasi dari Tahap ini diperlihatkan oleh gambar di bawah ini.



Gambar 4: Ilustrasi dari ShiftRows

d. Mix Columns

Mix Column adalah mengalikan tiap elemen dari blok *cipher* dengan matriks pada gambar 4 dibawah ini. Perkalian dilakukan seperti perkalian matriks biasa yaitu menggunakan *dot product* lalu perkalian keduanya dimasukkan ke dalam sebuah blok *cipher* baru.



Gambar 5: Matriks Mix Coloumns

2.3. Algoritma RC4

RC4 adalah *stream cipher* yang dirancang di RSA Security oleh Ron Rivest tahun 1987. Pada mulanya cara kerja RC4 dirahasiakan oleh RSA Security, akan tetapi ini dibocorkan di internet tahun 1994 di milis Cypherpunks. RSA Security tidak pernah merilis RC4 secara resmi, akibatnya banyak yang menyebutnya sebagai ARC4 (alleged RC4 atau tersangka RC4) untuk menghindari masalah *trademark* [6].

Berbeda dengan mayoritas *stream cipher* sebelumnya yang implementasinya dioptimalkan untuk *hardware* menggunakan *linear feedback shift registers*, RC4 dirancang agar dapat diimplementasikan di *software* secara sangat efsien. Ini membuat RC4 sangat populer untuk aplikasi *internet*, antara lain RC4 digunakan dalam standard TLS (*transport layer security*) dan WEP (*wireless equivalent privacy*) [6].

Langkah algoritma enkripsi RC4 diilustrasikan sebagai berikut:

a. Inisialisasi *array* S-*box* pertama, S[0],S[1],…,S[255]. S-*box* tersebut diisi dengan bilangan 0 sampai dengan 255, sehingga *array* S-*box* berbentuk:
   S[0]=0, S[1]=1,…, S[255]=255
   For i = 0 to 255
   S[i] = i
b. Inisialisasi *array* kunci (S-*box* lain), missal *array* kunci K dengan panjang 256. Jika panjang kunci K < 256, maka dilakukan *padding* yaitu penambahan *byte* semua sehingga panjang kunci menjadi 256 *byte*. Misalnya K = "abc" yang hanya terdiri 3 *byte* (3 huruf), maka lakukan *padding* dengan penambahan *byte* (huruf) semu, misalnya K = "abcabc…" sampai panjang K mencapai 256 *byte*, sehingga S-*box array* kunci K berbentuk :
   K[0], K[1],…,K[255]
   For i = 0 to 255
   K[i] = Kunci [I mod length]
c. Permutasi terhadap nilai-nilai di dalam *array* S dengan cara menukarkan isi *array* S[i] dengan S[j], prosesnya sebagai berikut:
   j = 0
   for i = 0 to 255
   j = (j + S[i] + K[i]) mod 256
   isi S[i] dan isi S[j] ditukar
d. Membangkitkan aliran kunci *(keystream)* selanjutnya digunakan untuk enkripsi.
   i = j = 0
   i = (i + 1) mod 256
   j = (j + S[i]) mod 256
   isi S[i] dan S[j] ditukar
   t = (S[i] + S[j]) mod 256
   K = S [t]
   Proses pembangkitan aliran kunci K dipilih dengan mengambil nilai penjumlahan S[i] dan S[j] kemudian operasikan modulus 256. Hasil penjumlahan adalah nilai indeks t sehingga S[t] menjadi kunci aliran K.
e. Kunci aliran K kemudian digunakan untuk mengenkripsi *plaintext* ke *ciphertext*. Sedangkan untuk mendapatkan *plaintext* dengan cara *ciphertext* di-XOR-kan dengan kunci yang sama dengan proses enkripsi

3. RANCANGAN SISTEM DAN APLIKASI

3.1 Analisa Masalah

Data atau informasi merupakan aset yang berharga dan sangat penting untuk di jaga, terutama apabila data tersebut bersifat rahasia dimana tidak sembarang orang diperkenankan untuk mengetahui isi data tersebut, sehingga masalah keamanan data

menjadi salah satu aspek yang sangat penting untuk diperhatikan agar suatu data dapat dijamin kerahasiaannya. PT. Daliny Cipta Karya merupakan perusahaan yang bergerak di bidang *retail*. Perusahaan ini memiliki beberapa toko yang tersebar di berbagai penjuru kota. Karena memiliki toko di berbagai penjuru kota maka perusahaan tersebut membutuhkan banyak karyawan, khususnya untuk posisi SPG *(sales promotion girl)* dan kasir dan admin. Maka dari itu hampir setiap minggu diadakan seleksi test masuk karyawan baru. Seleksi karyawan baru pada perusahaan tersebut dilakukan secara konvensional, yaitu calon karyawan mengikuti test tertulis pada waktu dan tempat yang telah ditentukan sebelumnya. Kemudian beberapa hari berselang HRD (*Human Resources Development*) akan mengumumkan siapa yang lolos untuk kemudian mengikuti tahap selanjutnya. Proses test yang demikian tentu saja mengalami beberapa masalah diantaranya; membutuhkan waktu yang lebih lama untuk mengolah hasil test, memungkinkan terjadinya kesalahan ketika melakukan proses pengolahan hasil test, dan adanya kemungkinan manipulasi hasil test oleh pihak yang tidak bertanggung jawab.

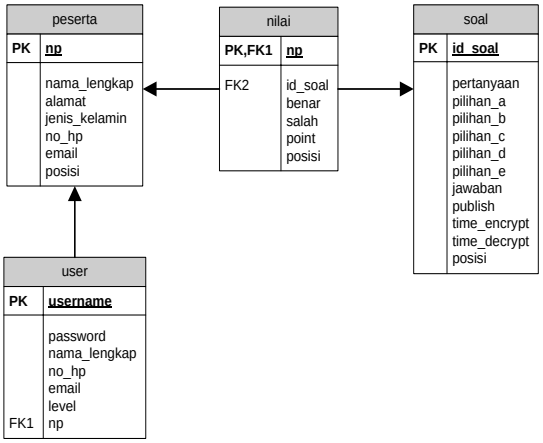
3.2 Penyelesaian Masalah

Dari permasalahan yang telah diuraikan diatas, diperlukan adanya sebuah aplikasi yang dapat membantu proses seleksi masuk PT. Daliny Cipta Karya. Selain itu perlu diperhatikan pula aspek keamanannya agar soal-soal seleksi masuk tersebut terjaga kerahasiannya. Dalam aplikasi tersebut, soal-soal yang disimpan didalam database dalam bentuk *chipertext* sehingga tidak bisa dibaca oleh sembarang pihak. Soal akan kembali ke bentuk *plaintext* ketika soal ditampilkan pada aplikasi.

Pada aplikasi ini, penulis menggunakan algoritma AES-128 (*Advance Encryption Standard*) dan RC4. Soal test akan di enkripsi dengan algoritma AES terlebih dahulu, setelah itu di enkripsi kembali dengan algoritma RC4. Untuk proses dekripsinya, soal yang berbentuk *chipertext* akan di dekripsi dengan algoritma RC4, kemudian di dekripsi kembali dengan algorima AES-128.

Dengan adanya aplikasi ini diharapkan dapat membantu proses seleksi masuk karyawan baru PT. Daliny Cipta Karya menjadi lebih mudah, efisien dan lebih terjamin keamanannya.

3.3 Rancangan Basis Data

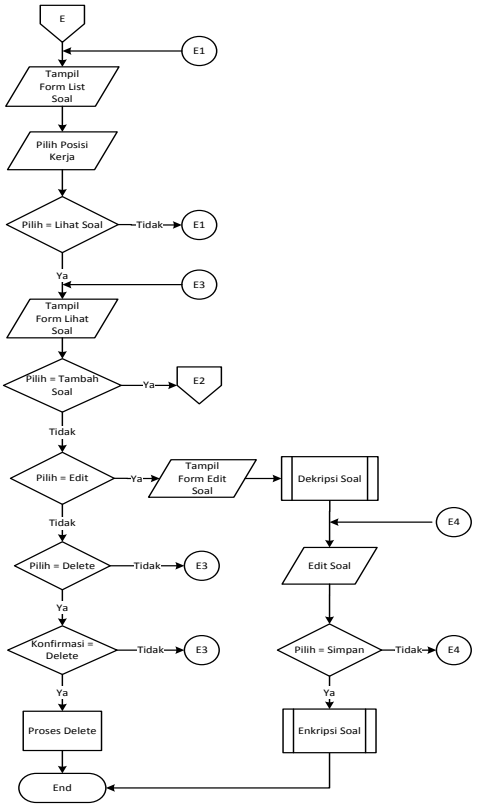


Gambar 6: Logical Relational Structure

3.4 *Flowchart* dan Algoritma Aplikasi

a. *Flowchart* Halaman Lihat Soal

Berikut ini adalah *flowchart* halaman lihat soal dimana admin dapat melihat soal ujian, menambah soal baru dan mengubah soal ujian dan menghapus soal ujian.



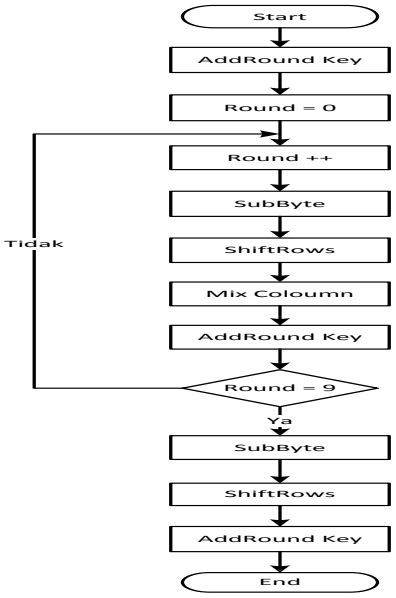
Gambar 7 : Flowchart Halaman Lihat Soal

Algoritma halaman lihat soal menjelaskan proses tampil data soal ujian, *edit* soal ujian dan hapus soal ujian.

1. Tampilkan *Form List* Soal
2. Pilih Posisi Kerja
3. *If* Pilih = Lihat Soal *Then*
4. Tampilkan *Form* Lihat Soal
5. *Else Then*
6. Kembali ke baris 1
7. *End If*
8. *If* Pilih = Tambah Soal *Then*
9. Tampilkan *Form Input* Soal
10. *End If*
11. *If* Pilih = *Edit* Soal *Then*
12. Tampilkan *Form Edit* Soal
13. Proses Dekripsi Soal
14. *Edit* Soal
15. *If* Pilih = Simpan *Then*
16. Proses Enkripsi Soal
17. *Else Then*
18. Kembali ke baris 12
19. *Else If* Pilih = *Delete* dan Konfirmasi = Ya *Then*
20. Proses *Delete*
21. *Else Then*
22. Kembali ke baris 4
23. Selesai

b. *Flowchart* dan Algoritma Proses Enkripsi AES-128

Berikut ini adalah *flowchart* proses enkripsi AES-



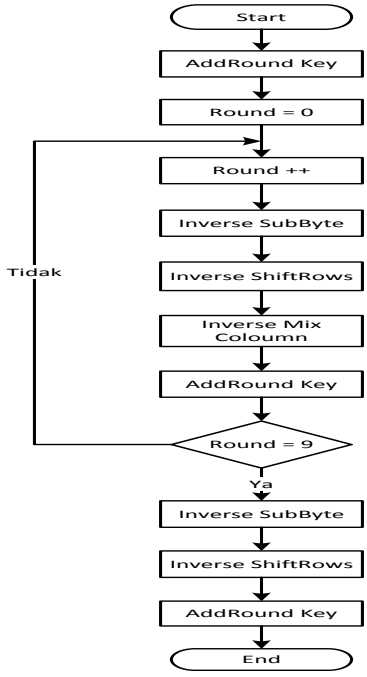
Gambar 8 : Flowchart Proses Enkripsi AES-128

Berikut adalah algoritma proses enkripsi AES-128.

1. Mulai
2. Lakukan XOR antara *plaintext* dan *cipher key*
3. *For Round* 0 to 9
4. Substitusi byte dengan menggunakan table substitusi (S-box)
5. Lakukan pergeseran baris-baris *array state* dari kanan ke kiri
6. Lakukan acak data di masing-masing kolom *array state*
7. Lakukan XOR antara *state* sekarang dengan *round key*
8. *EndFor*
9. Substitusi byte dengan menggunakan table substitusi (S-box)
10. Lakukan pergeseran baris-baris *array state* dari kanan ke kiri
11. Lakukan XOR antara *state* sekarang dengan *roundkey*
12. Selesai

c. *Flowchart* dan Algoritma Poses Dekripsi AES-128

Berikut ini adalah flowchart proses dekripsi AES-128



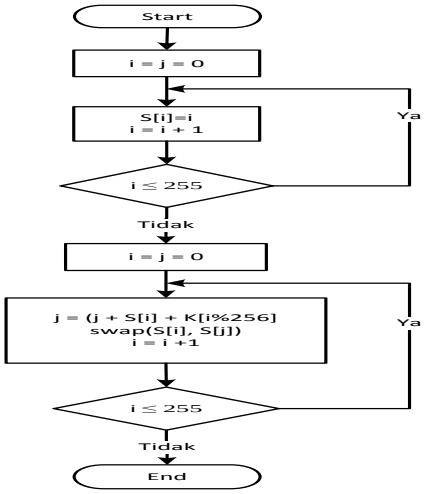
Gambar 9 : Flowchart Proses Dekripsi AES-128

Berikut ini adalah algoritma proses enkripsi AES-128.

1. Mulai
2. Lakukan XOR antara *ciphertext* dan *cipher key*
3. *For Round* 0 to 9
4. Petakan tiap elemen pada *state* dengan dengan menggunakan tabel *Inverse S-Box*
5. Lakukan pergeseran baris-baris *array state* dari kiri ke kanan
6. Kalikan setiap kolom dalam *state* dengan matrik perkalian dalam AES
7. Lakukan XOR antara *state* sekarang dengan *roundkey*
8. *EndFor*
9. Petakan tiap elemen pada *state* dengan dengan menggunakan tabel *Inverse S-Box*
10. Lakukan pergeseran baris-baris *array state* dari kiri ke kanan
11. Lakukan XOR antara *state* sekarang dengan *roundkey*
12. Selesai

d. *Flowchart* dan Algoritma Proses Enkripsi RC4

Berikut adalah *flowchart* proses enkripsi RC4.



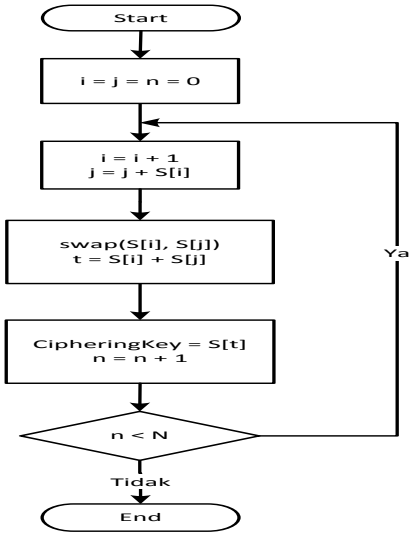
Gambar 10 : Flowchart Proses Enkripsi RC4

Berikut adalah algoritma proses enkripsi RC4

1. Mulai
2. Inisialisasi *array i* dan *array j* = 0
3. *For i* 0 to 255
4. Isi nilai i ke dalam *S-Box*
5. *EndFor*
6. Inisialisasi *array i* dan *array j* = 0
7. *For i* 0 to 255
8. Array j = j + S[i] + K[i mod 256]
9. Tukar nilai S[i] dengan nilai S[j]
10. *EndFor*
11. Selesai

e. *Flowchart* dan Algoritma Proses Dekripsi RC4

Berikut adalah *flowchart* proses dekripsi RC4



Gambar 11 : Flowchart Proses Dekripsi RC4

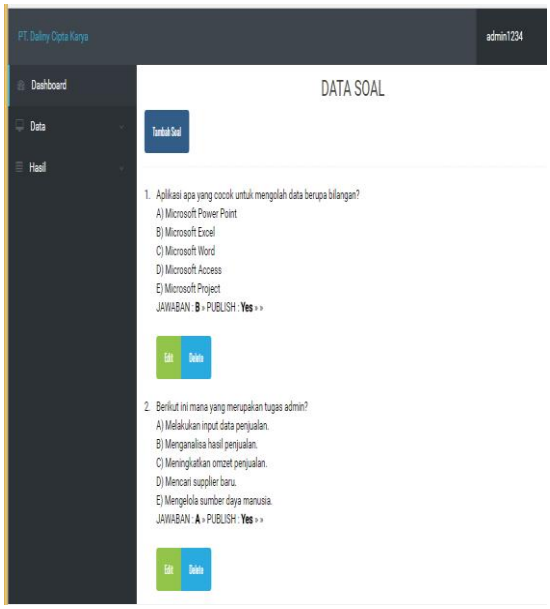
Berikut adalah algoritma proses dekripsi RC4

1. Mulai
2. Inisialisasi *array i* , *array j* dan *array n*= 0
3. *For* n < N
4. Nilai *array* j = j + S[i]
5. Tukar nilai S[i] dengan nilai S[j]
6. Nilai t = nilai S[i] + S[j]
7. Kunci Enkripsi = S[t]
8. *EndFor*
9. Selesai

4. HASIL DAN PEMBAHASAN

4.1 Tampilan Halaman Lihat Soal

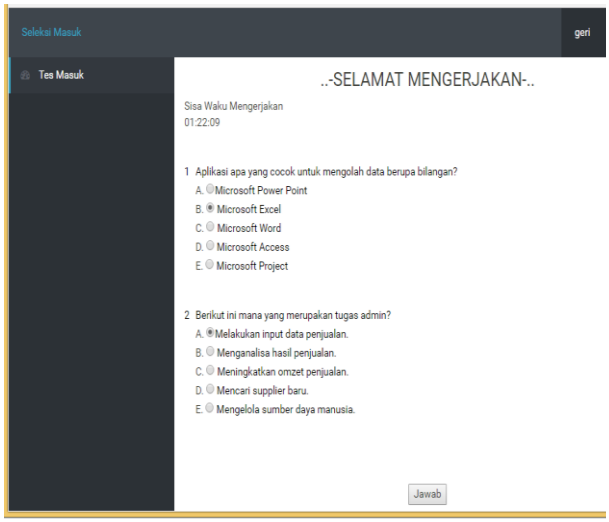
Pada halaman lihat soal terdapat tombol *edit* untuk mengubah soal dan *delete* untuk menghapus soal. Selain itu ada tombol Tambah Soal untuk menambah soal baru. Tampilan halaman lihat soal dapat dilihat pada gambar dibawah ini.



Gambar 12: Tampilan Halaman Lihat Soal

4.2 Tampilan Halaman Ujian Masuk

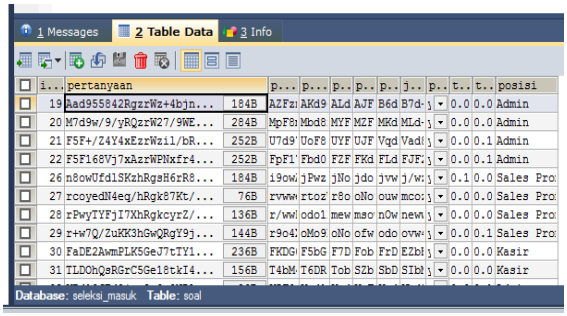
Pada halaman ini peserta dapat mengerjakan soal ujian yang mana soal berbentuk pilihan ganda dan dibatasi waktu pengerjaannya. Ketika selesai melakukan ujian dapat menekan tombol jawab.



Gambar 12: Tampilan Halaman Ujian Masuk

4.3 Tampilan Soal Hasil Enkripsi

Gambar dibawah ini tampilan soal hasil enkripsi yang tersimpan di database.



Gambar 14: Soal Hasil Enkripsi

4.4 Tabel Pengujian

Berikut merupakan tabel hasil dari percobaan enkripsi dan dekripsi dengan menggunakan algoritma AES-128 dan RC4.

a. Tabel Percobaan Enkripsi

Tabel 1 : Hasil Enkripsi

No	Plaintext	Posisi	Ciphertext	Waktu Proses Enkripsi
1	Kerjasama tim	Admin	AKd9+9Ao2RgzrW3008mB01vdj5NnBQcnK0ZW6Q==	0.016 detik
2	Universitas Budi Luhur	Sales Promotion Girl	zvw2bdxiZdbhbAsE749gnyl04ysnHdLL6UeCKbtyPs853FJxKTJ+Ng==	0.014 detik

b. Tabel Percobaan Dekripsi

Tabel 2 : Hasil Dekripsi

No	Ciphertext	Posisi	Plaintext	Waktu Proses Dekripsi
1	AKd9+9Ao2RgzrW3008mB01vdj5NnBQcnK0Z	Admin	Kerjasama tim	0.032 detik

	W6Q==			
2	zvw2bdxiZdbhbAsE749gnyl04ysnHdLL6UeCKbtyPs853FJxKTJ+Ng==	Sales Promotion Girl	Universitas Budi Luhur	0.012 detik

Evaluasi Sistem

Setelah dilakukan analisa dari hasil pengujian aplikasi ini dapat ditemukan beberapa kelebihan dan kekurangan dari aplikasi ini, yaitu sebagai berikut:

f. Kelebihan Aplikasi

a. Tampilan aplikasi *user friendly* sehingga mudah digunakan.
b. Soal test seleksi masuk menjadi lebih aman karena sudah melalui proses enkripsi.
c. Soal yang ditampilkan akan diacak untuk peserta yang berbeda.
d. Hasil seleksi masuk bisa langsung diketahui oleh admin ketika peserta selesai mengerjakan soal.
e. Peserta hanya dapat mengikuti test seleksi masuk sekali saja.

Kekurangan Aplikasi

a. Soal hanya berbentuk teks, tidak bisa berupa gambar.
b. Banyaknya soal yang tampil adalah sesuai yang admin *input*.

2. 5. Kesimpulan Dan Saran

Berdasarkan pengkajian aplikasi yang telah dilakukan terhadap masalah dan penyelesaian yang telah dilakukan, maka ditarik kesimpulan dan saran yang akan diperlukan untuk pengembangan aplikasi ini ke tahap lebih lanjut. Hal ini untuk menjadikan aplikasi yang dibuat lebih sempurna.

Kesimpulan

Dari hasil perancangan dan implementasi aplikasi ini dapat diambil kesimpulan sebagai berikut :

a. Dengan adanya aplikasi ini dapat membantu PT. Daliny Cipta Karya untuk melakukan seleksi masuk karyawan secara *online*.
b. Dengan adanya aplikasi ini dapat membantu pengolahan data hasil ujian menjadi lebih cepat.
c. Meminimalisir kemungkinan kebocoran soal seleksi masuk oleh pihak yang tidak bertanggung jawab.
d. Algoritma kriptografi AES-128 dapat diimplementasikan dengan algoritma kriptografi RC4 pada aplikasi ujian *online*.

Saran

Aplikasi seleksi masuk karyawan baru PT. Daliny Cipta Karya ini masih memiliki beberapa kekurangan, sehingga diperlukan saran demi membangun aplikasi ini agar menjadi lebih baik :

a. Soal test tidak hanya sebatas teks, diharapkan dapat berupa gambar atau ilustrasi yang lain.
a. Aplikasi dapat memberikan batasan soal yang akan ditampilkan..

DAFTAR PUSTAKA

[1] Jogianto. *Sistem Teknologi Informasi : Pendekatan Terintegrasi: Konsep Dasar, Teknologi, aplikasi, Pengembangan dan Pengelolaan*. Edisi Ke-3. Yogyakarta : Penerbit Andi, 2009

[2] Mulyanto, Agus. *Sistem Informasi Konsep dan Aplikasi /PPL*. Yogyakarta : Pustaka Pelajar, 2009.

[3] Jogiyanto,HM, MBA, Akt, Ph.D. *Metodologi Penelitian Sistem Informasi*. Yogyakarta : Andi Yogyakarta, 2008.

[4] Kadir, Abdul. *BelajarDatabase menggunakan Mysql*. Yogyakarta : Andi , 2009.

[5] Fikriansyah Rahmat. *Dasar Pemrograman VB.NET 2008* : Restu Agung, 2008.

[6] Shelly, B. Gary., Thomas J. Cashman., *Misty E. Vermaat. Discovering Computers 2007 A Gateway to Information*. USA: Thomson Course Technology, 2007.

[7] Gaol, Jimmy L. *Sistem Informasi Manajemen : Pemahaman dan Aplikasi* .Jakarta : Grasindo, 2008.