PENGEMBANGAN SISTEM INFORMASI *SECURITY CLEARANCE IDENTIFICATION* BERBASIS RFID DI PT. ANGKASA PURA I JUANDA SURABAYA

Sandy Priyo Pambudi [1], Mungki Astiningrum [2]

Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Malang
JL. Soekarno-Hatta No. 9 Malang 65141, Indonesia
[1] sandypriyo@gmail.com, [2] mungki_astiningrum@polinema.ac.id

Abstrak

Banyaknya aktifitas dari luar maupun dari dalam lingkungan bandara memicu berbagai tindakan kriminal yang dapat terjadi sehingga dapat menghambat keamanan dan memberikan dampak yang buruk bagi lalu lintas bandara. Disini PT. Angkasa Pura I berperan penuh dalam mengatasi permasalahan di atas. Salah satunya yaitu masalah pemberian izin yang diberikan oleh perusahaan kepada pegawai eksternal yang akan memasuki area tertentu untuk bekerja. Mengingat area bandara tersebut bersifat *restricted area* yakni terbatas sehingga tidak semua orang dapat mengaksesnya. Maka dibuatlah Sistem Informasi *Security Clearance* untuk menyelesaikan masalah diatas. Sistem Informasi *Security Clearance* berguna menjadi sebuah alat bantu untuk pencatatan data-data *customer* atau pegawai eksternal yang akan melakukan aktifitas kerja di kawasan bandara. Sistem tersebut diintegrasikan dengan memanfaatkan RFID *Card* sebagai alat identifikasi atau pemberian pas bandara yang digunakan pegawai eksternal sebagai izin memasuki area tertentu. Dalam sistem ini juga dilakukan pengamanan pada data *customer* tertentu yang dirahasiakan. Pengamanan data dalam Sistem Informasi *Security Clearance* didukung dengan model algoritma RSA yang merupakan algoritma enkripsi maupun deskripsi dalam kriptografi. Teknik ini digunakan untuk mengkonversi data kedalam bentuk kode-kode tertentu, untuk tujuan agar informasi yang tersimpan tidak dapat terbaca oleh siapa pun kecuali orang-orang yang berhak. Terbukti dari hasil pengujian yang dilakukan, metode RSA ini berjalan dengan baik untuk mengamankan data *customer*. Sistem ini juga mampu meningkatkan performa kinerja petugas *security*, mudah dioperasikan, dapat dijadikan laporan pendataan *customer* yang masuk atau keluar di area bandara secara jelas dan terperinci serta memudahkan petugas dalam pencatatan dan manajemen data-data *customer*. Hasil dari perancangan sistem informasi berbasi RFID ini terbukti dapat mempermudah proses keamanan *gate* dan dapat di aplikasikan di kehidupan nyata.

Kata kunci: Sistem Informasi *Security Clearance*, RFID, RSA

1 Pendahuluan

Seiring dengan perkembangan zaman, manusia berusaha untuk menciptakan peralatan dan teknik yang dapat mempermudah serta menyempurnakan pengolahan dan penyampaian informasi, sehingga menghasilkan informaasi yang cepat dan akurat.

Pada sistem yang berjalan di PT Angkasa Pura I Bandar Udara Internasional Juanda Surabaya bagian *Security Clearance* sekarang ini belum sepenuhnya terkomputerisasi, adapun prosedur yang dilakukan adalah mula-mula petugas menyerahkan formulir yang harus diisi oleh calon *customer*, setelah terisi formulir tersebut disimpan pada lemari hal ini mempersulit pencarian data pegawai jika sewaktu-waktu data tersebut dibutuhkan misalkan apabila ada laporan tindak kriminal maka dokumen formulir harus disatukan dengan dokumen-dokumen tindakan kriminal. Maka penulis menyimpulkan lemahnya pengolahan data pada bagian *security clearance* dimana prosedur yang dilakukan belum sepenuhnya terkomputerisasi.

Kemudahan akses media komunikasi membawa pengaruh terhadap keamanan informasi yang menggunakan media komunikasi sebagai media penyimpanan. Informasi menjadi sangat renta untuk diketahiu, diambil atau bahkan dimanipulasi dan disalahgunakan oleh pihak lain yang tidak berhak. Terlebih lagi semua data yang ada di *database* sistem rentan terhadap pencurian dan manipulasi data. Untuk permasalahan keamanan tersebut diperlukan suatu metode untuk menjaga keamanan informasi. Salah satu metodenya adalah kriptografi.

Oleh sebab itu dibutuhkanya sistem aplikasi *Security Clearance*. Dimana sistem ini berguna menjadi sebuah alat bantu yang meringankan pekerjaan pegawai PT. Angkasa Pura I atau petugas dalam pencatatan data-data orang yang akan masuk dan bekerja di kawasan bandara Juanda dan juga mengeluarkan Surat Keterangan (SK). Selain itu kegunaan lainya adalah untuk memudahkan pengidentifikasian tiap orang yang telah terdaftar dengan memberikan ID seperti card RFID yang nantinya digunakan untuk pengganti surat keterangan

untuk masuk pada kawasan yang dikehendaki. Serta dapat mengamankan data-data pekerja yang ada.

Maka dengan adanya sistem informasi *Security Clearance* ini diharapkan dapat memperbaiki sistem yang ada sehingga dapat membuat pekerjaan yang dulunya dilakukan secara manual dan lambat akan dapat berubah menjadi cepat, tepat, aman dan akurat dan juga dapat mempermudah dalam penyajian informasi baik bagi pegawai atau petugas *Security Clearance* maupun penanggungjawab lapangan. Selain itu juga dapat memantau keluar masukknya *customer*.

2 Landasan Teori

2.1 RFID

Teknologi RFID merupakan bagian dari RF *(Radio Frequensi)* yang digunakan sebagai media identifikasi secara *wireless* yang terdiri dari dua komponen (Karigianes,2007) yaitu:

a) RFID tag (*tranfonder*) yang terdiri dari sebuah *device* yang kecil yang tertanam dalam sebuah buku seperti label, *smartcard* dan lainya yang memiliki identifikasi yang unik.

Gambar 2.1 RFID *Tag* (berbentuk *card*)

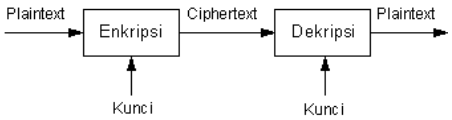
b) RFID *reader* merupakan sebuah *device* yang dapat berkomunikasi tanpa kontak langsung dengan suatu tag untuk mengidentifikasikanya (*wireless*) pada *radio frequensi* (Karigianes, 2007).

Gambar 2.2 RFID *Reader*

Gambar 2.3. Komunikasi Pada *Radio Frequence*

2.2 Kriptografi

Kriptografi merupakan suatu bidang ilmu yang mempelajari tentang bagaimana merahasiakan suatu informasi penting ke dalam suatu bentuk yang tidak dapat dibaca oleh siapapun serta mengembalikannya kembali menjadi informasi semula.



Gambar 2.4 Skema Enkripsi dan Dekripsi

2.3 RSA

Algoritma RSA, ditemukan oleh 3 orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1976, yaitu: Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Keamanan enkripsi dan dekripsi data model ini terletak pada kesulitan untuk memfaktorkan modulus n yang sangat besar. Sebuah operasi RSA, baik enkripsi, dekripsi, penandaan, atau verifikasi intinya adalah sebuah eksponensial terhadap modul. Saat ini kriptosistem RSA menggunakan digit minimum sebesar 154 digit (512 bit), hal ini dilakukan untuk menjaga data agar lebih terjaga keamanannya. (Triorizka, 2010)

Secara garis besar, proses kriptografi pada algoritma RSA terdiri dari 3 tahapan yaitu:

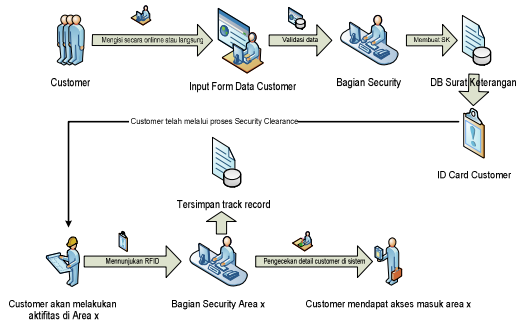
1. Pembangkitan Kunci
   - Pilih bilangan prima sembarang *p* dan *q*.
   - Hitung $n = p.q$,
   - Kemudian dicari nilai φ yang digunakan untuk mencari kunci publik dan privat menggunakan rumus:
     $\varphi = (p-1)(q-1)$
   - Selanjutnya dicari nilai *e* yang mana diperoleh dari relatif prima antara φ dan bilangan yang dicari(*e*) dirutkan menggunakan perulangan yang dimulai dari 2 hingga menemukan relatif prima. Dengan kata lain *e* dan *m* tidak mempunyai faktor prima bersama.
   - Setelah itu dilakukan perhitungan untuk memperoleh nilai *d* untuk dekripsi dengan cara dilakukan perulangan sebanyak 1000 kali untuk mencoba nilai *d* agar memenuhi syarat : e*d mod φ hasilnya harus 1.
   - Maka akan didapatkan kunci publik adalah (*n, e*) dan kunci private (*n, d*).
2. Proses Enkripsi
   - Ambil kunci *public* (*n,e*)
   - Ambil plaintext kemudian pecah menjadi beberapa bagian tiap karakternya dan beri batasan "+".
   - Kemudian tiap karakter tersebut dirubah kedalam format ASCII.
   - Setelah terbentuk dengan format kode ASCII maka dihitung tiap bagian tersebut dengan rumus:
     $ci = mi^e \bmod n$
   - Setelah tiap bagian tersebut terhitung, maka dilakukan penggabungan setiap bagian (*ci*) sehingga memperoleh kesatuan ciphertext c
3. Proses Dekripsi
   - Ambil kunci *privat* (*n,d*)
   - Ambil ciphertext kemudian pecah menjadi beberapa bagian sesuai dengan batasan pengelompokan dengan simbol "+".
   - Kemudian dilakukan perhitungan untuk dekripsi dengan rumus:
     $mi = ci^d \bmod n$

- Pada tahap ini *mi* dikembalikan dari kode ASCII menjadi karakter biasa.
- Setelah tiap bagian tersebut terhitung, maka dilakukan penggabungan setiap bagian (*mi*) sehingga memperoleh kesatuan plaintext m.

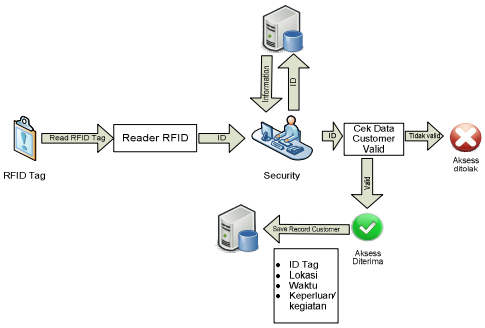
3 Perancangan Sistem

3.1 Gambara Umum Sistem

Sistem Informasi *Security Clearance* adalah sistem informasi yang dibangun untuk meningkatkan keamanan di kawasan bandara PT. Angkasa Pura I. Sistem ini berguna menjadi sebuah alat bantu yang meringankan pekerjaan pegawai atau petugas PT. Angkasa Pura I dalam pencatatan data-data *customer* atau pegawai *outsourcing* yang akan melakukan aktifitas kerja di kawasan bandara Juanda. Sistem tersebut mencatat data-data *customer* serta dilakukan intergrasi dengan memanfaatkan RFID *Card* sebagai alat identifikasinya dan juga dilakukan pengamanan pada data *customer* tertentu yang dirahasiakan.



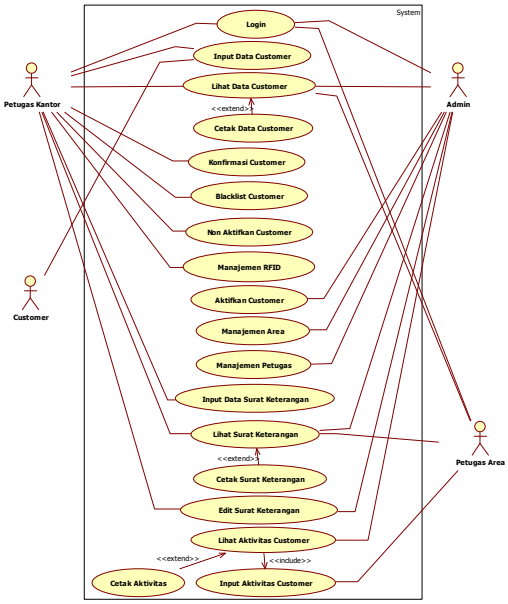
Gambar 3.1 Sistem Security yangakan dibangun di PT. Angkasa Pura I



Gambar 3.2 Gambar Implementasi RFID Pada Sistem Security Clearance

3.2 Use Case Diagram

Use case diagram merupakan pemodelan untuk kelakuan (*behavior*) sistem yang akan dibuat (Rosa A.S., 2013).



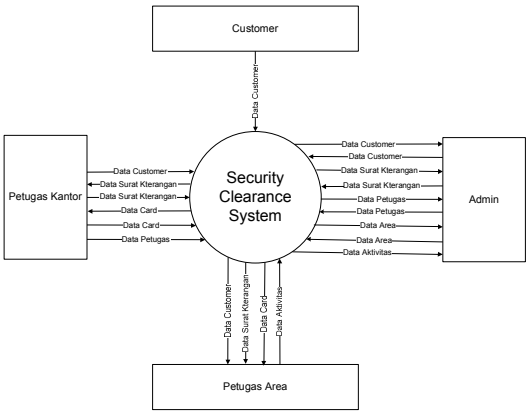
Gambar 3.3 *Use Case* Sistem *Security Clearance*

Pada gambar di atas terdapat 4 aktor yang terdiri dari Customer, Petugas Kantor, Petugas Area, Admin

Serta terdapat 18 kelakuan/aktivitas *use case* yang dapat dilakukan oleh aktor yang ada seperti pada gambar 3.3.

3.3 Context Diagram

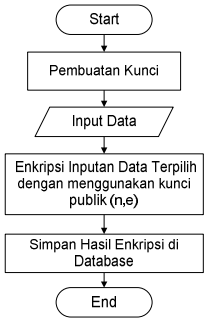
DFD Level 0 atau context diagram biasa disebut sebagai diagram sistem inti (fundamental system model) atau biasa model konteks (context model). Arah panah dari aliran data menunjukkan aliran data berupa masukan (input) dan keluaran (output) ke dalam proses perangkat lunak yang dirancang sebagai berikut :



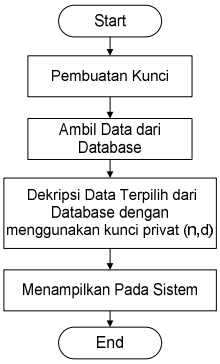
Gambar 3.4 *Context Diagram* Sistem *Security Clearance*

3.4 Penerapan RSA

Pada bagian ini akan membahas perancangan untuk pengimplementasian metode ini ke dalam sistem sebagai berikut:



Gambar 3.20 Tahapan Enkripsi Input Data pada RSA



Gambar 3.21 Tahapan Dekripsi Input Data pada RSA

Pada gambar 3.20 dijelaskan bahwa ada pemilihan data yang dilakukan enkripsi. Yang mana data tersebut dianggap pentinga dan diperlukan adanya pengamanan untuk data-data yang dipilih yaitu pada tabel data_customer, data saudara, data_p_lama, data_p_baru, data_tambahan, dan data_petugas.

Selanjutnya data yang telah terenkripsi akan disimpan pada database, sehingga nantinya hanya petugas yang berwenang yang dapat membaca data yang ada di database dengan proses dekripsi seperti pada gambar 3.21. Apabila petugas tersebut valid sesuai yang ada di database, maka proses dekripsi akan dieksekusi untuk menampilkan data yang telah terenkripsi

4 Implementasi

4.1 Implementasi Basis Data

Implementasi basis data dilakukan sesuai dengan perancangan yang telah dibuat.

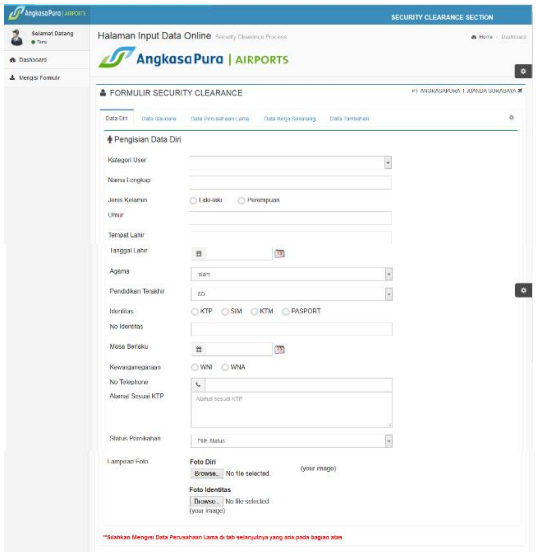
Pada basis data aplikasi ini terdapat 17 tabel, antara lain admin, aktivitas_customer, area, asurat_ket, card, data_customer, data_pernyataan, data_p_baru, data_p_lama, data_saudara, data_tambahan, dsurat_ket, lampiran, laporan, log, petugas, surat_ket.

4.2 Implementasi Program

Implementasi program yaitu tampilan hasil dari penerapan sistem yang telah dibuat, sesuai dengan perancangan yang telah dilakukan dengan hasil berupa tampilan aplikasi sebagi berikut:

Implementasi Sistem Informasi *Security Clearance* ini dilakukan dengan bahasa pemrograman PHP. Sedangkan untuk tampilannya menggunakan bootstrap adminLTE template.

Gambar 4.1 Halaman *Dashboard*



Gambar 4.2 Halaman Pengisian Data *Customer*

Gambar 4.39 Hasil Enkripsi di Database

Gambar 4.1 adalah halaman tampilan awal (*dashboard*) Sistem Security Clearance PT. Angkasa Pura I Juanda Surabaya. Pilih menu *Login Page* untuk u*ser* yang akan melakukan *login* sesuai dengan hak aksesnya.

User yang dapat mengakses aplikasi ini ada 3 yaitu admin sebagai supervisor, petugas kantor, dan petugas area. Sedangkan 1 user lagi sebagai *customer* yang hanya bisa melakukan insert data diri *customer* seperti pada gambar 4.2. Masing-masing user akan

diarahkan ke halaman yang fungsinya berbeda-beda sesuai dengan tugas masing-masing user sebagaimana dijelaskan pada bagian Context Diagram

5 Pengujian dan Pembahasan

Pengujian pada sistem ini meliputi beberapa jenis pengujian, yaitu pengujian fungsional, pengujian metode den pengujian teknis

5.1 Pengujian Fungsional

Untuk menguji kinerja aplikasi dibutuhkan suatu pengujian sistem, yaitu pengujian fungsionalitas aplikasi. Pengujian ini dilakukan dengan cara menjalankan setiap fitur dalam aplikasi dan melihat apakah hasilnya sudah sesuai dengan yang seharusnya. Menurut pengujian sistem yang telah dilakukan, fungsi-fungsi dalam sistem ini telah berjalan sesuai perencanaan

5.2 Pengujian Metode

Pada pengujian ini dilakukan dengan cara melakukan percobaan enkripsi dan dekripsi yang dilakukan secara manual dan juga di sistem. Dari hasil pngujian didapati bahwa hasil enkripsi dan dekripsi baik secara manual ataupun di aplikasi sesuai atau sama. Kemudian dilakukan pengujian lebih lanjut untuk mengetahui tingkat kesuksesan penerapan metode dengan mengambil dari 10 sampel inputan, sehingga menghasilkan grafik sebagai berikut :

Gambar 4.1 Grafik Perbandingan Tiap Nilai

Penjelasan dari gambar diatas yaitu "*Nilai Seharusnya*" yang isinya adalah jumlah karakter awal atau karakter yang akan dilakukan proses enkripsi. Juga terdapat "*Nilai Terukur*" yang isinya adalah jumlah karakter yang sukses setelah karakter awal melalui proses enkripsi dan juga dekripsi oleh sistem. Dalam artian jumlah karakter kembalian setelah melalui enkripsi dan juga dekripsi sesuai dengan karakter awal. Adapula "*Jumlah Karakter Terenkripsi*" meupakan jumlah karakter dari hasil enkripsi yang disimpan ke dalam *database*.

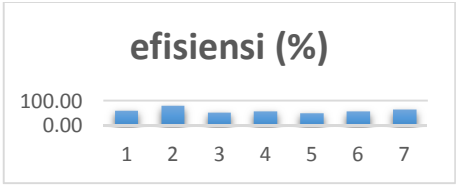
Jadi dapat disimpulkan bahwa penerapan metode kriptografi algoritma RSA untuk proses enkripsi dan dekripsi berhasil diimplementasikan pada sistem dengan tingkat keberhasilan enkripsi dan dekripsi 100% akan tetapi dari hasil uji coba dihasilkan jumlah karakter setelah dilakukan enkripsi mengalami peningkatan. Dibuktikan dari rata-rata peningkatan jumlah karakter setelah dilakukan enkripsi yaitu 3,75 kali dari *text* awal

5.3 Pengujian Teknis

5.3.1 Efisiensi Waktu

Dari Percobaan yang dliakukan sebanyak 7 kali didapati rata-rata peningkatan efisiensi dari segi waktu bertambah 60,02 % dibandingkan dengan kinerja tanpa sistem. Untuk grafik perbandingan kinerja dan juga kenaikan efisiensinya dapat dilihat pada gambar 4.2 dan gambar 4.3.

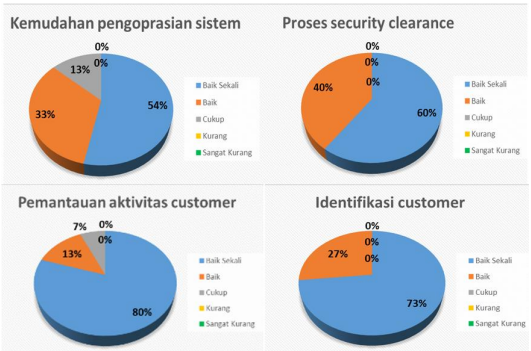
Gambar 4.2 Grafik Perbandingan Kinerja Dari Segi Waktu



Gambar 4.3 Grafik Kenaikan Efisiensi Dari Segi Waktu

5.3.2 Peningkatan Performa Kinerja Pegawai *Security*

Dari data kuisioner yang telah dianalisa dari responden yang berjumlah 15 orang kemudian dibuatkan tampilan grafik dalam bentuk diagram *pie* untuk mengetahui prosentase hasil analisa sebagai berikut:



Gambar 4.4 Grafik Analisa Kuisiener Pengujian Performa Sistem

Dari Gambar Grafik 4.4 dapat disimpulkan dari pemberian nilai 15 responden didapati bahwa sistem ini sudah terbukti memenuhi syarat dari pihak

PT. Angkasa Pura 1 Juanda Surabaya yang berimbas pada peningkatan performa kinerja pegawai *security*

6 Kesimpulan dan Saran

6.1 Kesimpulan

Berdasarkan pembahasan sebelumnya dapat ditarik beberapa kesimpulan, yaitu:

a) Hasil pengujian menunjukkan bahwa perancangan sistem telah menghasilkan sistem yang dapat membantu serta memudahkan petugas dalam pencatatan dan manajemen data-data *customer* yang akan masuk dan bekerja di kawasan bandara Juanda Surabaya, sehingga dapat membuat pekerjaan yang dulunya dilakukan secara manual dan lambat akan dapat berubah menjadi cepat, tepat dan akurat dan juga dapat mempermudah dalam penyajian informasi baik bagi pegawai atau petugas *Security Clearance* maupun penanggungjawab lapangan.

b) Sistem ini telah berhasil menerapkan metode kriptografi menggunakan algoritma RSA untuk pengamanan data-data *customer*.

c) Hasil pengujian menunjukkan bahwa performansi sistem dengan memanfaatkan teknologi RFID ini sudah baik dari hasil uji coba pada bab V. Dilihat dari segi teknis diantaranya adalah kemudahan pengoprasian sistem, proses *security clearance*, pemantaua aktivitas customer, dan identifikasi customer dijelaskan bahwa sistem ini dapat diterima dengan baik oleh pihak-pihak yang berkepentingan di PT Angkasa Pura 1 Juanda Surabaya.

6.2 Saran

Berdasarkan penelitian ini, ada beberapa hal yang disarankan, yaitu:

a) Dari proses pengujian didapati bahwa karakter yang disimpan mengalami kenaikan dari segi jumlah karakter yang berimbas pada size untuk penyimpananya. Maka bisa dikombinasikan dengan metode kriptografi ainya untuk membuat agar jumlah karakter hasil enkripsi sama dengan teks awal.

b) Sistem ini bisa dikembangkan lagi dengan memanfaatkan kartu RFID selain berfungsi untuk masuk area, juga dimanfaatkan untuk memfasilitasi customer untuk hal lainya, misalkan absensi pemberian jatah makan.

Daftar Pustaka:

Adiprana, Brahmasta. (2010): *Penerapan Business Process Management Dalam Service Oriented Architecture*, Institut Teknologi Bandung, Bandung.

Arifin, Zainal. (2009): *Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman*. Samarinda: Jurnal Informatika Mulawarman.

Alief, Ridwan. (2014): *Pemanfaatan Teknologi Rfid Melalui Kartu Identitas Dosen Pada Prototipe Sistem Ruang Kelas Cerdas*. [Online] Tersedia: http://download.portalgaruda.org/article.php?article=159393&val=1255. [14 Januari 2015].

Fathansyah. (2012): *Basis Data*. Bandung: Informatika Bandung.

Kadir, Abdur. (2009): *Membuat Aplikasi Web dengan PHP dan Database MySQL*. Yogyakarta: Penerbit ANDI.

Kromodimoeljo, Sentot. (2010): *Teori dan Aplikasi Kriptografi*. Jakarta: SPK IT Consulting.

Wicaksono, Prasetyo Andy. (2006): *Studi Pemakaian Algoritma RSA dalam Proses Enkripsi dan Aplikasinya*, Institut Teknologi Bandung, Bandung.

Gondohanindijo, Jutono. (2010): *Pemanfaatan Teknologi RFID (Radio Frequency Identification)*. Majalah Ilmiah Informatika. [Online] Tersedia: www.unaki.ac.id/ejournal/index.php/jurnal -informatika/article/download/26/25. [14 Januari 2015].

Lubis, Husni. 2012. *Metode Enkripsi Menggunakan Algoritma RSA pada Sistem Login. Prosiding Snastikom*. [Online] Tersedia: http://prosiding-snastikomti.stth-medan.ac.id/index.php/doc_download/52-metode-enkripsi-menggunakan-algoritma-rsa-pada-sistem-login. [11 Januari 2015].

Rachendu, Satma, Agung Budi Prasetijo dan Kodrat. 2012. *Aplikasi Proses Enkripsi-Dekripsi Algoritma Rsa (Rivest Shamir Adleman) Menggunakan Bahasa Pemrograman Java*. [Online] Tersedia: http://www.elektro.undip.ac.id/el_kpta/wp-content/uploads/2012/05/L2F097673_MTA.pdf. [7 Februari 2015].

S.A., Rosa, dan Shakahudin, M. (2013): *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*. Bandung: Informatika

Triorizka, Andrianus. (2010). *Penerapan Algoritma Rsa Untuk Pengamanan Data Dan Digital Signature Dengan . Net*. [Online] Tersedia: www.repository.amikom.ac.id/files/Publikasi_06.12.1748.pdf. [25 Februari 2015]

http://digilib.tes.telkomuniversity.ac.id/index.php?option=com_content&view=article&id=271:php&catid=6:internet&Itemid=14 waktu akses: 28 Mei 2015, 09:29