KEAMANAN DATA PASIEN BARU POLIKLINIK UMUM dengan ALGORITMA SANDI CAESAR (Studi Kasus:RS Sentra Medika Cibinong)

Safitri Jaya,[1)] Yane Arliana Kurniawati [2)]

Safitri Jaya,[1)]
Sekolah Tinggi Teknologi Informasi NIIT I-Tech
Jl. Asem 2 No. 22, Cipete – Jakarta Selatan
http://www.i-tech.ac.id

Yane Arliana Kurniawati [2)]
Sekolah Tinggi Teknologi Informasi NIIT I-Tech
Jl. Asem 2 No. 22, Cipete – Jakarta Selatan
http://www.i-tech.ac.id

ABSTRAK

Keamanan data merupakan sesuatu yang sangat penting, terlebih lagi apabila perusahaan atau instansi sudah terkomputerisasi dalam melakukan pengolahan data. Salah satu cara yang dapat dilakukan untuk pengamanan data adalah dengan mengenkripsi data tersebut agar tidak dapat terbaca oleh pihak yang tidak diharapkan. Algoritma yang digunakan dalam perancangan program aplikasi ini menggunakan Algoritma Sandi Caesar yang akan menghasilkan pesan acak sesuai dengan function yang dibuat.Dalam perancangan aplikasi ini, metode yang digunakan adalah dengan pengembangan waterfall dan pengujian dengan menggunakan black box dan white box testing. Program aplikasi ini dibuat dengan menggunakan MySql (sebagai database) dan Visual Studio 2010 yang dilengkapi dengan function algoritma Sandi Caesar untuk mengenkripsi dan dekripsi data. Setiap data yang sudah dienkripsi hanya dapat didekripsi oleh pihak yang memiliki akses untuk melakukan hal tersebut.

Kata kunci : Keamanan Data, Algoritma Sandi Caesar

1. PENDAHULUAN

Berkembangnya dunia teknologi dapat mendukung perkembangan bisnis yang dapat memberikan dampak positif dan juga dampak negatif atau tindakan – tindakan yang dapat merugikan pihak tertentu, seperti pencurian data. Pencurian data menjadi hal yang sangat merugikan dari segi finansial (keuangan) maupun produktivitas bagi perorangan terlebih lagi instansi, sehingga diperlukan solusi yang dapat mencegah atau memberikan keamanan terhadap data yang bersifat rahasia. Faktor keamanan sangat diperlukan untuk mengamankan data-data.

Begitupun dalam usaha di bidang medis, sudah kewajiban rumah sakit untuk menjaga keamanan data tersebut pada setiap pelayanan yang diberikan kepada pasien. Salah satu cara yang dilakukan untuk mencegah pencurian data pasien adalah dengan melakukan pengamanan pada database mengenai data pasien.

Keamanan pada database dapat dilakukan, misalnya dengan memberikan hak akses pada setiap pengguna sesuai dengan kebutuhannya dan melakukan enkripsi terhadap data yang tesimpan dalam database.

2. LANDASAN TEORI

Menurut Kamus Besar Bahasa Indonesia, Algoritma adalah prosedur sistematis untuk memecahkan masalah matematis dalam langkah-langkah terbatas. Salah satu cara yang dapat digunakan untuk mengamankan data adalah dengan menggunakan algoritma kriptografi yang terdiri dari algoritma enkripsi dan dekripsi.

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari cara menyembunyikan pesan. Pada pengertian modern, kriptografi adalah ilmu yang bersandarkan pada teknik matematika yang digunakan untuk keamanan informasi, seperti kerahasiaan, keutuhan data dan otentikasi entitas.

Enkripsi berasal dari Bahasa Yunani yaitu Kryptos yang artinya tersembunyi atau rahasia. Awal tahun 1900 SM, seorang juru tulis Mesir menggunakan hieroglif non-standar untuk menyembunyikan arti dari sebuah prasasti. Kebanyakan orang hanya dapat menulis pesan tersembunyi tanpa bisa membacanya, sampai skema enkripsi berkembang sehingga dapat mengkonversi pesan dengan transposisi atau subsitusi. Tahun 700 SM, Spartan menulis pesan pada strip dari kulit yang melilit tongkat. Abad pertengahan muncul subsitusi polyalphabetic yang menggunakan beberapa huruf subsitusi untuk membatasi penggunaan analisis frekuensi dalam memecahkan cipher. Penerapannya adalah mesin Enigma yang digunakan selama Perang Dunia kedua oleh Jerman. Enkripsi terus mengalami perkembangan, tahun 1976 B.Whitfield Diffie dan Martin Hellman memecahkan permasalahan dalam mendistribusikan kunci enkripsi secara aman.

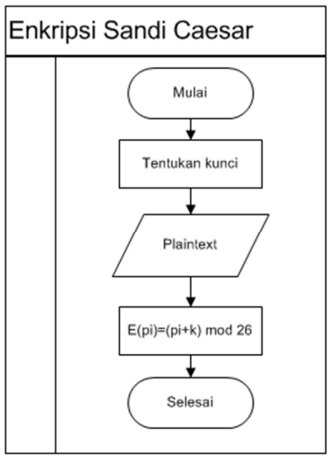
Gambar 1. Algoritma Sandi Caesar

Algoritma sandi caesar merupakan kriptografi klasik, dimana dalam menyembunyikan pesan dengan menggunakan metode subsitusi (pergantian huruf) dan atau transposisi (pertukaran tempat). Enkripsi dan dekripsi pada sistem persandian Caesar menggunakan operasi *shift*. Operasi *shift* adalah mensubsitusi suatu huruf menjadi huruf pada daftar alphabet berada di – k, sebelah kanan atau sebelah kiri huruf tersebut. Untuk dapat mengolah teks asli yang merupakan deretan simbol huruf diperlukan pemetaan dari huruf menjadi angka, sehingga dapat diaplikasikan operasi matematika. Misalnya huruf A-Z dipetakan ke angka integer 0-25 dan apabila

pergeseran melebihi 26, gunakan sisa bagi 26, oleh karena itu aritmatika modular yang digunakan pada sistem persandian Caesar adalah Z_{26}.

3. ANALISIS dan PERANCANGAN SISTEM

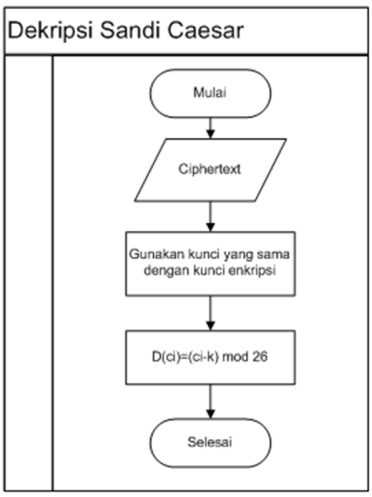
Enkripsi dengan menggunakan Sandi Caesar, setiap karakter yang diiput akan disubsitusikan ke karakter yang lain, sehingga akan menghasilkan karakter yang acak, sedangkan pada saat dekripsi karakter acak tersebut (*chipertext*) akan dikembalikan ke karakter semula sesuai dengan kuncinya sehingga akan ditampilkan karakter yang dapat dibaca *user* (*plaintext*).



Gambar 2. Enkripsi Sandi Caesar

Rumus enkripsi algoritma Sandi Caesar, yaitu E(pi)=(pi+k) mod 26

Contoh diberikan kunci (k)=3, apabila diberikan inputan atau *plaintext* (pi)=5→ E, maka didapat E(5)=(5+3) mod 26 = 8. Berdasarkan perhitungan tersebut didapat keluran atau *ciphertext* E(5) = 8 → huruf H.



Gambar 3. Dekripsi Sandi Caesar

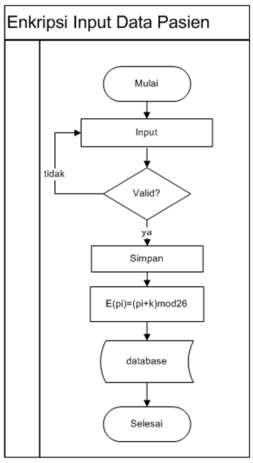
Rumus enkripsi algoritma sandi caesar, yaitu D(ci)=(ci-k) mod 26

Contoh diberikan kunci (k) = 3, apabila diberikan *ciphertext* (ci) = 8 → H, maka didapat D(8)=(8-3) mod 26 = 5. Berdasarkan perhitungan tersebut didapat keluran atau *plaintext* D(8) = 5 → huruf E.

Berdasarkan gambaran umum mengenai enkripsi dan dekripsi algoritma sandi Caesar, akan digambarkan juga proses enkripsi dan dekripsi yang terjadi pada aplikasi yang akan dibangun sebagai berikut :

1. Enkripsi Input Data Pasien

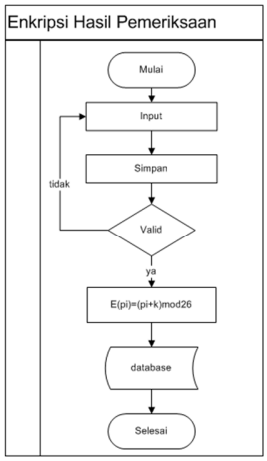
   Terjadi proses enkripsi untuk data pasien yang diinput oleh Petugas Pendaftaran.



Gambar 4. Enkripsi Input Data Pasien

2. Enkripsi Hasil Pemeriksaan

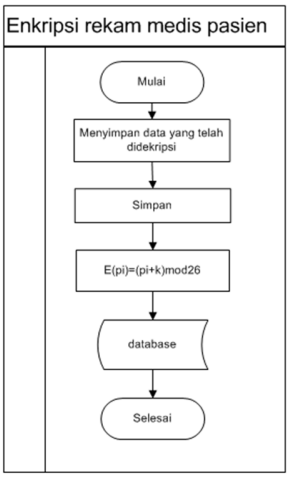
Terjadi proses enkripsi untuk data hasil pemeriksaan pasien yang diinput oleh Petugas Rekam Medis.



Gambar 5. Enkripsi Hasil Pemeriksaan

3. Enkripsi Rekam Medis Pasien

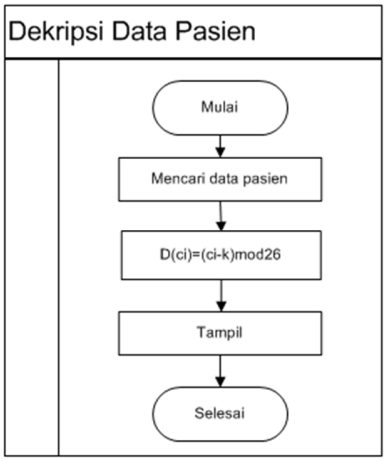
Terjadi proses enkripsi untuk data rekam medis pasien. Proses enkripsi dilakukan setelah proses pencetakan berkas rekam medis.



Gambar 6. Enkripsi Rekam Medis Pasien

4. Dekripsi Data Pasien

Terjadi proses dekripsi untuk data pasien. Proses dekripsi ini dilakukan pada saat pencarian data pasien karena akan ditambahkan / diinputkan data hasil pemeriksaan oleh Petugas Rekam Medis.

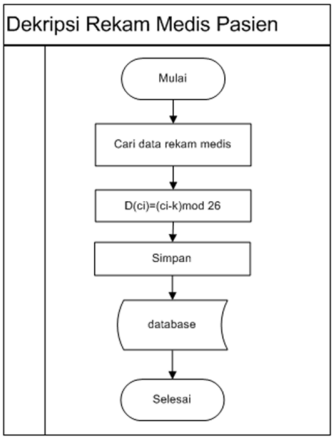


Gambar 7. Dekripsi Data Pasien

5. Dekripsi Rekam Medis Pasien

Terjadi proses dekripsi untuk rekam medis pasien. Proses dekripsi ini dilakukan untuk mencetak rekam medis

pasien. Data akan dikembalikan ke data asli (*plaintext*) pada saat pencetakan.

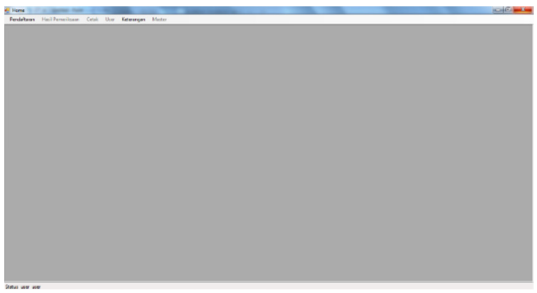


Gambar 8. Dekripsi Rekam Medis Pasien

4. IMPLEMENTASI

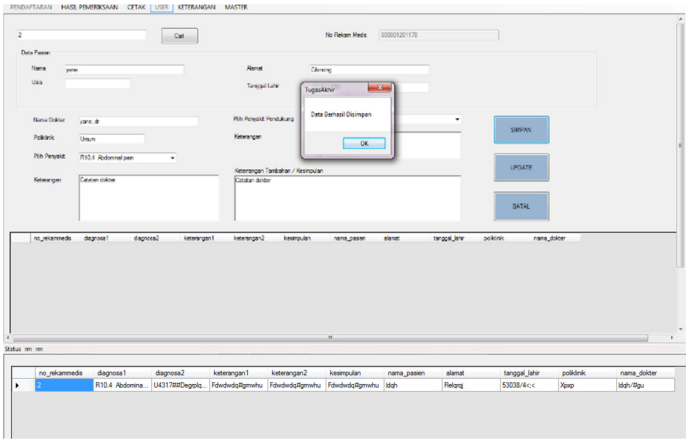
Terdapat 3 hak akses dalam program ini, yaitu pendaftaran, rekam medis dan administrator. Setiap *user*name yang diberikan hak aksesnya masing – masing dapat melakukan login dan menuju ke halaman yang sesuai dengan hak aksesnya.

setiap *user* akan diarahkan ke halaman utama, dimana terdapat menu yang aktif sesuai dengan hak aksesnya masing–masing pada saat login.



Gambar 9. Tampilan Halaman Utama / *MDI Parent*

Menu yang tidak aktif akan berwarna abu-abu dan tidak dapat diklik.



Gambar 10. Pesan Berhasil dan Enkripsi Input Hasil Pemeriksaan

Pengujian yang digunakan untuk menguji aplikasi sistem penerimaan pasien baru ini dengan menggunakan teknik pengujian *black box dan white box testing*.

Black Box Testing pada Aplikasi

Dalam melakukan *black box testing* terhadap aplikasi ini perlu dilakukan penginputan dengan login terlebih dahulu sesuai dengan hak aksesnya masing-masing

Tabel 1. Hasil Uji *Black Box Testing*

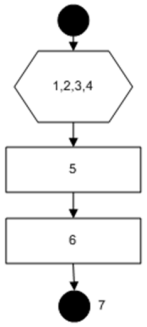
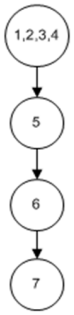
Aktor	**Kelas Uji**	**Butir Uji**	**Hasil Uji**
Administrator, Petugas Pendaftaran dan Petugas Rekam Medis	Login	Verifikasi username dan password	Pesan gagal (bila login gagal) Masuk ke Halaman Utama / MDI Parent sesuai hak akses (bila login berhasil)
Administrator	Input, cari, update, hapus data master user, dokter dan penjamin	Validasi data	Pesan gagal apabila terdapat field yang belum diisi / tidak sesuai dengan pattern Pesan berhasil apabila field diisi dan sesuai dengan pattern
Petugas Pendaftaran	Input data pasien	Validasi data	Pesan gagal apabila terdapat field yang belum diisi / tidak sesuai dengan pattern Pesan berhasil apabila field diisi dan sesuai dengan pattern

Rekam Medis	Input, cari, update, hapus data master *ICD*	Validasi data	Pesan gagal apabila terdapat field yang belum diisi / tidak sesuai dengan pattern Pesan berhasil apabila field diisi dan sesuai dengan pattern
		Tampilan sesuai dengan data asli (*plaintext*)	
	Pencarian data	Validasi data	Dekripsi data oleh sistem tampil sesuai fields nya
	Input, update hasil pemeriksaan	Enkripsi data	Pesan gagal apabila terdapat field yang belum diisi / tidak sesuai dengan pattern Pesan berhasil apabila field diisi dan sesuai dengan pattern Enkripsi data oleh sistem tampil di grid view Dekripsi data oleh sistem tampil di gried view
		Berkas rekam medis sesuai dengan data asli (*plaintext*)	
	Cetak berkas rekam medis		

White Box Testing pada Aplikasi

White box testing pada aplikasi difokuskan pada data yang akan dienkripsi dan dekripsi. Pengujian ini digambarkan dengan menggunakan diagram alir untuk menentukan *path* / jalur yang harus dilalui untuk proses enkripsi dan dekripsi

Tabel 2. Hasil Uji White Box Testing " Proses Enkripsi"

Diagram Alir	Grafik Alir
	

Keterangan :

```
        Function ENCCaesar(ByVal Plain As
        String) As String
           Dim x As String = ""
           Dim xkalimat As String = ""
1       For i = 1 To Len(Plain)
2          x = Mid(Plain, i, i)
3          x = Chr(Asc(x) + 3)
4          xkalimat = xkalimat + x
5            Next
6                 ENCCaesar = xkalimat
7       End Function
```

Berdasarkan grafik alir diatas dapat dihitung dan ditentukan banyaknya *path* / jalur untuk proses enkripsi yang digunakan

V(G) = E – N + 2

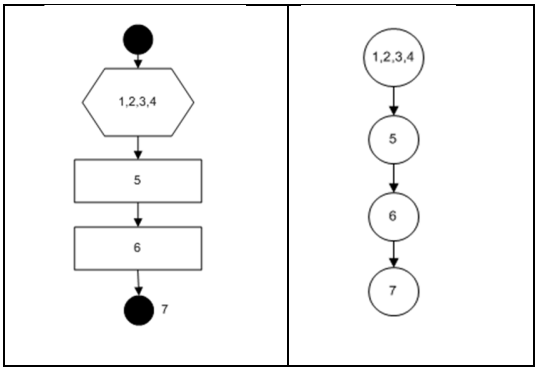
V(G) = 3 – 4 + 2

V(G) = 1

Path / jalur I = 1,2,3,4 - 5 - 6 - 7

Tabel 3. Hasil Uji White Box Testing " Proses Dekripsi"

Diagram Alir	Grafik Alir



Keterangan :

```
        Function DECCaesar(ByVal Plain As
        String) As String
           Dim x As String = ""
           Dim xkalimat As String = ""
1       For i = 1 To Len(Plain)
2          x = Mid(Plain, i, i)
3          x = Chr(Asc(x) - 3)
4          xkalimat = xkalimat + x
5            Next
6                 DECCaesar = xkalimat
7       End Function
```

Berdasarkan grafik alir diatas dapat dihitung dan ditentukan banyaknya *path* / jalur untuk proses enkripsi yang digunakan

V(G) = E – N + 2

V(G) = 3 – 4 + 2

V(G) = 1

Path / jalur I = 1,2,3,4 - 5 - 6 - 7

5. KESIMPULAN dan SARAN

Kesimpulan

Berdasarkan uraian yang telah dijabarkan sebelumnya, maka dapat ditarik kesimpulan sebagai berikut :

1. Dengan algoritma sandi caesar dapat dihasilkan hasil enkripsi dari data yang diinput.

2. Sistem Aplikasi yang dibangun dapat melakukan enkripsi dan dekripsi data secara otomatis.

Saran

Dari kesimpulan tersebut, penyusun menyadari bahwa aplikasi yang dibangun masih jauh dari sempurna dan masih terdapat kekurangan. Oleh sebab itu penyusun memberikan beberapa saran yang mungkin dapat digunakan di kemudian hari dalam pengembangan aplikasi ini, diantaranya :

1. Dalam proses pencetakan laporan data secara otomatis terdekripsi oleh sistem, agar *user* tidak lagi melakukan dekripsi sebelum mencetak laporan dan enkripsi setelah melakukan pencetakan laporan.
2. Diharapkan kedepannya algoritma yang digunakan lebih kompleks, sehingga dapat mempersulit jika ada penyusup yang mungkin sudah mendapatkan akses untuk masuk ke sistem.

6. DAFTAR PUSTAKA

Ardianto. (2011). Implementasi Algoritma Kriptografi Caesar Cipher Pada Aplikasi SMS Telepon Selular Berbasis J2ME. Naskah Publikasi : Amikom Yogyakarta.

Basbeth, Ferryal. Rekam Medis. Diakses pada : http://medicalrecord.webs.com/isirekammedis.htm

Kamus Besar Bahasa Indonesia. Diakses pada : http://kbbi.web.id/algoritme

S.Pressman, Roger, Ph.D. Rekayasa Perangkat Lunak. (2012). Yogyakarta : Andi.

Sadikin, Rifki.(2012). Kriptografi Untuk Keamanan Jaringan. Yogyakarta : Andi.

Seftyanto, Donny, dkk. (2012, P-94). Peran Algoritma Caesar Cipher Dalam Membangun Karakter Akan Kesadaran Keamanan Informasi Prosiding, ISBN: 978-979-16353-8-7. Seminar Nasional Matematika dan Pendidikan Matematika FMIPA UNY, Yogyakarta 10 November 2012.

Suprianto, Dodit. (2010). Membuat Aplikasi Desktop Menggunakan Mysql & Vb.Net Secara Operasional. Malang : Media Kita.

Sutabri, Tata (2012). Analisis Sistem Informasi. Yogyakarta.: Andi.

UML Tutorial, diakses pada World Wide Web : http://www.tutorialspoint.com/uml/umltutorial.pdf

Wahyuni, Ana. (2016). Kriptografi Dengan Algoritma Grass Caesar. Jurnal Teknologi Informasi dan Komunikasi, ISSN : 2087 – 0868, Volume 7 Nomor 1 Maret 2016.

Penulis adalah

1. Dosen pada Sekolah Tinggi Teknologi Informasi NIIT I-Tech
2. Alumni Program Studi Teknologi Informasi pada Sekolah Tinggi Teknologi Informasi NIIT I-Tech