PENGAMANAN DATA REKAM MEDIS PASIEN MENGGUNAKAN KRIPTOGRAFI *VIGÈNERE CIPHER*

Erwin Gunadhi[1], Agung Sudrajat[2]

Jurnal Algoritma
Sekolah Tinggi Teknologi Garut
Jl. Mayor Syamsu No. 1 Jayaraga Garut 44151 Indonesia
Email : jurnal@sttgarut.ac.id

[1]erwin.gunadhi@sttgarut.ac.id
[2]1206007@sttgarut.ac.id

Abstrak – *Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Namun masalah keamanan ini seringkali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi, salah satu contohnya adalah sistem informasi rekam medis yang ada di puskesmas kersamenak.* R*ekam medis merupakan sebuah rekaman kesehatan yang memuat kumpulan data-data penting berkaitan dengan identitas, hasil anamnesis, hasil pemeriksaan fisik dan catatan segala kegiatan para tenaga kesehatan terhadap pasien yang telah diperiksa dan mendapat pelayanan kesehatan di fasilitas kesehatan pada waktu ke waktu. Data yang ada pada rekam medis ini bersifat rahasia sehingga perlu untuk dilakukan pengamanan terhadap data-data tersebut. Maka dari itu upaya yang dilakukan untuk melakukan pengamanan data tersebut yaitu dengan melakukan enkripsi. Metode yang digunakan dalam penelitian ini menggunakan Kriptografi Vigènere Cipher yang dikemukakan oleh Blaise de Vigènere. Dan untuk menggambarkan alur kerja serta tahapan proses penelitian dari awal sampai selesai menggunakan work breakdown structure yang dikemukakan oleh dawson. Dengan tahapan analisis, perancangan, dan penerapan keamanan data. Tools yang digunakan dalam pemodelan menggunakan Microsoft visio. Dari hasil penelitian ini, dapat disimpulkan bahwa proses pengamanan data rekam medis pasien menggunakan kriptografi Vigènere cipher dapat mengakomodasi kebutuhan pengguna sistem dalam meningkatkan keamanan data yang ada pada aplikasi rekam medis.*

Kata Kunci – *Keamanan Data, Kriptografi, Rekam Medis, Vigènere Cipher*.

I. PENDAHULUAN

Masalah keamanan data merupakan salah satu aspek penting dari sebuah sistem informasi. Sehingga masalah keamanan ini harus diperhatikan oleh para pemilik dan pengelola sistem informasi sebagai salah satu masalah yang dianggap penting dan harus dicari pemecahan masalahnya. Salah satu masalah keamanan data yang kurang mendapat perhatian adalah keamanan data pada aplikasi rekam medis pasien.

Sebelumnya sudah ada penelitian yang membahas mengenai masalah keamanan sistem informasi, kasus yang diangkat dalam penelitian sebelumnya mengenai pengamanan pada basis data keuangan koperasi dengan menggunakan kriptografi *advance encryption standard* yang dibahas oleh Novianty [1]. Penelitian tersebut bisa dijadikan sebagai sebuah bahan rujukan untuk melakukan pengamanan terhadap data-data yang ada pada aplikasi rekam medis dengan menggunakan metode pengamanan yang berbeda yaitu dengan menggunakan kriptografi *Vigènere Cipher*.

II. URAIAN PENELITIAN

A. Rekam Medis

Rekam medis merupakan sebuah rekaman kesehatan yang memuat kumpulan data-data penting berkaitan dengan identitas, hasil anamnesis, hasil pemeriksaan fisik dan catatan segala kegiatan para tenaga kesehatan terhadap pasien yang telah diperiksa dan mendapat pelayanan kesehatan di fasilitas kesehatan pada waktu ke waktu [2], Tujuan dibuatnya rekam medis adalah sebagai alat bukti utama yang bisa membenarkan adanya pasien dengan identitas yang jelas dan telah diperiksa serta telah mendapatkan berbagai pemeriksaan dan pengobatan di fasilitas kesehatan. Rekam medis juga memiliki tujuan untuk mendokumentasikan hasil pelayanan apasaja yang telah diberikan oleh para tenaga kesehatan, penunjang medis, dan tenaga lain yang bekerja di fasilitas kesehatan. Dengan demikian rekaman itu membantu dalam pengambilan keputusan mengenai terapi, tindakan, dan penentuan diagnosis pasien.

B. Keamanan

Perkembangan teknologi informasi pada saat ini membuat setiap pemilik dan pengelola sistem informasi harus dan wajib memikirkan bagaimana cara untuk melindungi keamanan sistem informasi yang dimilikinya agar terhindar dari berbagai resiko yang mungkin saja dapat menyebabkan kerugian. Keamanan sistem menurut Garfinkel yang dikutif oleh rahardjo mengemukakan bahawa keamanan komputer mencakup tiga aspek yang meliputi *Confidentiality*, *Integrity* dan *Availability* [3].

Berbagai resiko yang bisa saja menimbulkan dampak kerugian termasuk kedalam bagian dari *risk management* yang meliputi tiga komponen yang memiliki kontribusi terhadap resiko yang diantaranya *Asset*, *Threat*, dan *Vulnerabilities* [3].

C. Kriptografi

Menurut pendapat Stallings, mengartikan kriptografi sebagai (*Cryptography is the art and science of keeping messages secure*) atau dalam bahasa Indonesia arti bahwa kriptografi adalah ilmu dan seni untuk menjaga pesan supaya terjaga dalam hal keamanannya. Menurut Lee "*Crypto*" berarti "*secret*" (dalam bahasa Inggris) yakni rahasia dan "*graphy*" berarti "*writing*" (dalam bahasa Inggris) yang berarti tulisan. Para ahli kriptografi atau pengguna dikenal dengan istilah *cryptographers*. Algoritma kriptografi biasanya disebut dengan *cipher*. *Cipher* merupakan sebuah persamaan matematika yang digunakan untuk proses melakukan enkripsi dan dekripsi. Biasanya kedua persamaan matematika tersebut mempunyai hubungan matematis yang erat [4].

Sedangkan definisi kriptografi menurut Munir mengartikan Kriptografi (*cryptography*) berasal dari Bahasa Yunani kuno: "*cryptós*" yakni "*secret*" (rahasia), sedangkan "gráphein" yakni "*writing*" (tulisan) [5]. Jadi, kriptografi adalah "*secretwriting*" (tulisan rahasia). Terdapat beberapa definisi kriptografi yang telah diungkapkan dalam berbagai literatur. Definisi kriptografi yang digunakan dalam buku- buku yang lama yaitu sebelum tahun 1980-an, mengemukakan bahwa kriptografi merupakan seni dan ilmu yang digunakan untuk menjamin kerahasiaan sebuah pesan dengan menggunakan cara melakukan penyandian pesan tersebut ke dalam bentuk yang tidak dapat dipahami lagi maknanya oleh orang lain. Pendapat yang diutarakan di atas mengenai kriptografi yang digunakan untuk menjamin keamanan dalam sebuah komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata mungkin cocok pada masa dulu. Namun pada saat ini kriptografi bukan hanya sebuah privasi, tetapi juga bertujuan untuk data *Integrity*, *Authentication*, dan *non-repudiation*.

D. Algoritma Vigènere Cipher

Vigènere Cipher merupakan contoh terbaik dari *cipher* alfabet-majemuk (manual). *Vigènere Cipher* ini di publikasikan pada tahun 1586 oleh seorang diplomat (sekaligus seorang kriptologis) dari Perancis, Blaise de *Vigènere* pada abad 16 meskipun Giovan Batista Belaso pertama kali menggambarkannya pada tahun 1553 seperti ditulis di dalam isi bukunya *La Cifra del Sig*. *Vigènere Cipher* dipublikasikan pada tahun 1586 akan tetapi algoritma tersebut baru luas dikenal pada 200

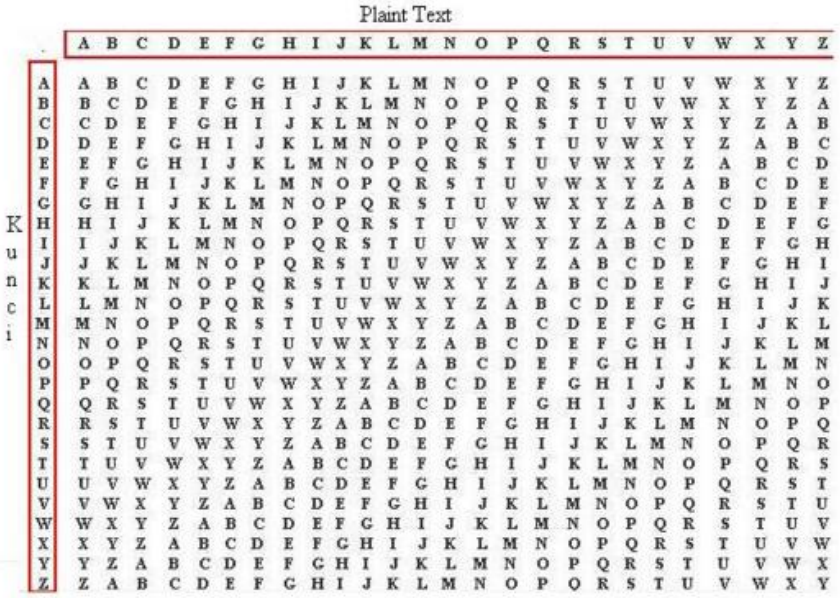
tahun kemudian lalu oleh penemunya *cipher* tersebut diberi nama *Vigènere cipher. Vigènere Cipher* digunakan oleh para tentara konfiderasi pada perang sipil Amerika (*American civil war*).

Vigènere Cipher dikenal luas karena mudah dipahami dan diimplementasikan. *Cipher* ini menggunakan bujursangkar *Vigènere* untuk melakukan enkripsi. Pada kolom paling kiri dari bujursangkar menyatakan huruf-huruf kunci sedangkan baris paling atas menyatakan huruf-huruf dari plainteks. Pada setiap baris di dalam bujursangkar *Vigènere* menyatakan huruf-huruf cipherteks yang diperoleh dengan *Caesar cipher*, dimana jumlah pergeseran huruf plainteks ditentukan nilai *numeric* huruf kunci tersebut (yaitu, a=0, b=1, c=2, d=3, e=5…, z=25). Sebagai contoh, huruf kunci c(=2) menyatakan huruf-huruf plainteks digeser sebanyak 2 huruf ke kanan (dari susunan alfabetnya), sehingga huruf-huruf cipherteks pada baris c adalah :

C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Bujursangkar *Vigènere* dipakai guna memperoleh cipherteks. Apabila panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang penggunaanya secara periodik. Sebagai contoh, jika plainteks adalah THIS PLAINTEKS dan kunci adalah AGUNG, maka penggunaan kunci periodik adalah sebagai berikut :

Plainteks	:	T	H	I	S	P	L	A	I	N	T	E	X	T
Kunci	:	A	G	U	N	G	A	G	U	N	G	A	G	U



Gambar 1: Bujursangkar *Vigènere*

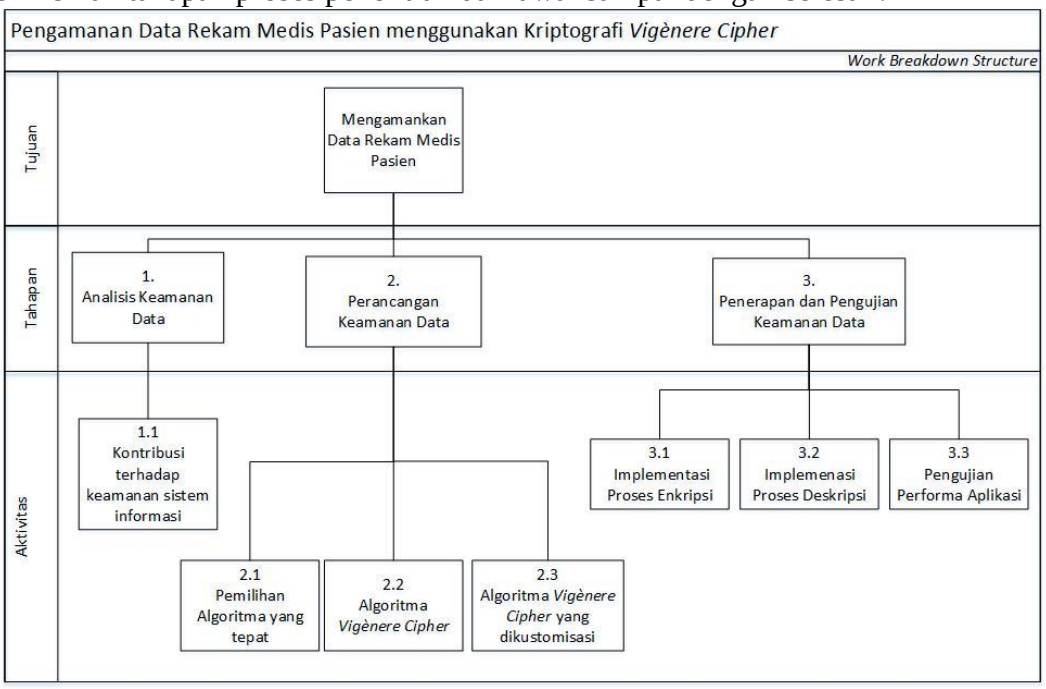
Setiap huruf *plainteks* dienkripsi dengan setiap huruf kunci dibawahnya. Untuk melakukan proses enkripsi tersebut, dilakukan dengan bujursangkar *Vigènere* sebagai berikut : tarik garis *vertical* dari huruf plainteks ke bawah, lalu tarik garis mendatar dari huruf kunci ke kanan. Titik temu dari kedua garis tersebut menyatakan huruf cipherteksnya. Munir [3]

E. Definisi PHP Hypertext Processor (PHP)

PHP merupakan *script* yang digunakan untuk pemrograman *script web server side*, dengan menggunakan PHP maka *maintenance* suatu situs *web* menjadi lebih mudah. Proses pengolahan data dapat dilakukan dengan menggunakan aplikasi yang dibuat dengan menggunakan *script* PHP. Peranginangin [5]

III. KERANGKA KERJA KONSEPTUAL

Dalam penelitian ini ada beberapa tahapan aktivitas dalam proses pencapaian tujuan penelitian yang digambarkan dengan menggunakan pemodelan work breakdown structure yang dijelaskan oleh dawson [1], berikut merupakan bagan yang digunakan untuk menggambarkan alur dari sebuah proyek untuk mendefinisikan tahapan proses penelitian dari awal sampai dengan selesai :



Gambar 2: *Work breakdown structure* Pengamanan rekam medis pasien

IV. HASIL DAN PEMBAHASAN

A. Analisis Keamanan Data

Pada zaman teknologi informasi seperti sekarang ini data menjadi sesuatu yang penting yang harus diperhatikan oleh para pengolah data informasi, sehingga data tersebut tidak disalahgunakan oleh pihak-pihak tertentu yang tidak bertanggung jawab. Oleh karena itu diperlukan suatu pengamanan data agar data-data yang bersifat penting dan rahasia dapat tetap terjaga keamanannya. Berikut ini merupakan analisis keamanan data dilihat dari aspek-aspek yang berkontribusi terhadap keamanan sistem informasi menurut Garfinkel yang dikutif oleh Rahardjo [6]:

lomor	Nomor kartu	Tanggal Pemeriksaan	Nama	Tanggal Lahir	Jenis Kelamin	Alamat	Tinggi Badan	Berat Badan	Keluhan	Tekanan Darah	Respiratory Rate	Nama Penyakit	Nama Obat	Nama Dokter
20	010001	2016-07-29	Agung Sudrajat	1993-06-18	laki-laki	Kp. Panawuan RT.03 Rw.11 Ds. Sukajaya Kec. Tarogong Kidul Kab. Garut	169	59	sakit kepala	120/80	120	Hipertensi primer (esensial)	Propanolol HCl tablet 40 mg	Dr.Suparman
23	010003	2016-07-30	lesty ASP	1993-09-12	Perempuan	Cikajang Garut	160	50	sakit gigi	100/70	120	Penyakit gusi, jaringan periodental dan tulang alv	Amoksisilin Kaplet 500 mg	Dr.
27	010002	2016-07-31	Nani	1986-06-18	Perempuan	Kp. Kersamenak RT.03 Rw.11 Ds.	155	50	sakit magh	100/70	100	Tukak lambung	Antasida DOEN I Tablet Kunyah	Dr.H.Rujito

Gambar 2: Data pada Aplikasi Rekam Medis

Dilihat dari data yang ada pada gambar diatas, maka analisis keamanan data dilihat dari aspek-aspek yang berkontribusi terhadap keamanan sistem informasi diantaranya :

1) *Privacy*/*Confidentiality*

Aspek *Privacy*/*Confidentiality* disini merupakan salah satu aspek keamanan sistem untuk menjaga agar informasi mengenai data-data penting dan rahasia tidak bisa diakses oleh orang-orang yang tidak memiliki kewenangan untuk mengakses informasi. Data-data penting dan rahasia yang berkaitan dengan rekam medis ini diantaranya adalah data nama, tanggal lahir, alamat, keluhan, tekanan darah, *respiatory rate*, penyakit yang pernah diderita dan nama obat yang diberikan. Data-data tersebut merupakan data yang sifatnya pribadi sehingga data tersebut harus dijaga penggunaanya serta penyebarannya.

2) *Integrity*

Aspek *Integrity* merupakan aspek yang menekankan bahwa sebuah informasi tidak boleh diubah tanpa seijin pemilik informasi. Untuk menjaga agar integritas dari informasi yang disampaikan tetap terjaga keasliannya maka peneliti menerapkan teknik enkripsi pada data-data penting dan rahasia yang ada pada aplikasi rekam medis Menggunakan Kriptografi *Vigènere Cipher* yang telah dikustomisasi.

3) *Availability*

Aspek availability merupakan aspek yang berhubungan dengan ketersediaan informasi ketika informasi tersebut dibutuhkan. Sehingga pada aspek ini harus bisa menjamin bahwa pengguna informasi yang sah selalu bisa mengakses informasi dan sumberdaya miliknya sendiri. Untuk dapat memastikan bahwa pengguna merupakan orang yang benar-benar berhak untuk menggunakan informasi tersebut maka implementasinya yaitu dengan menambahkan *password* pada data-data penting dan rahasia yang ada pada aplikasi rekam medis.

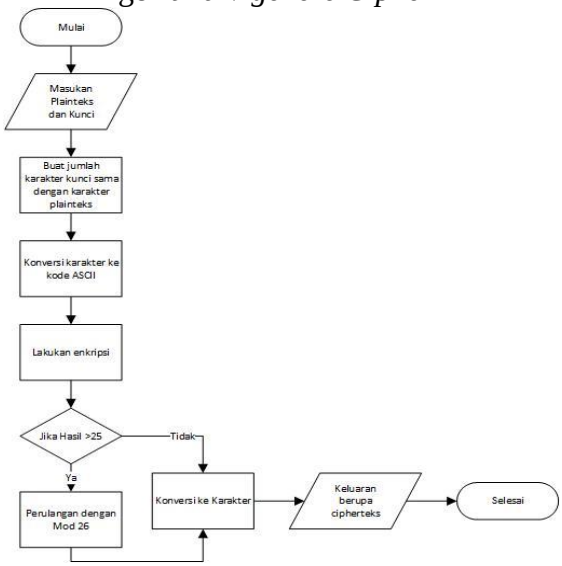
B.Perancangan Keamanan Data

Setelah diketahui alasan pentingnya melakukan pengamanan data yang terdapat pada aplikasi rekam medis, maka untuk tahap selanjutnya dibuat tahap perancangan dengan tahapan sebagai berikut :

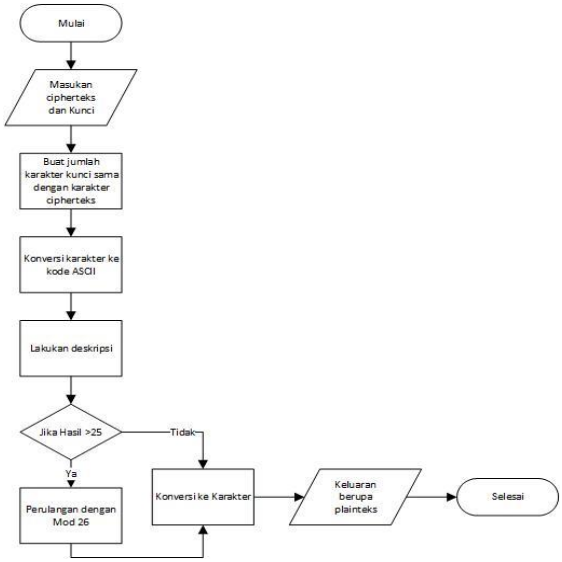
1) Pemilihan Kriptografi yang Tepat

Berdasarkan hasil analisis keamanan data yang dijelaskan sebelumnya maka perlu dipilih sebuah algoritma kriptografi yang tepat untuk dapat bekerja di dalam bahasa pemrograman PHP, kriptografi yang dipilih harus mudah dijalankan dan dikembangkan untuk proses pengembangan selanjutnya, dan kriptografi tersebut harus memiliki sandi yang tidak rentan terhadap pemecahan sandi atau yang biasa disebut analisis frekuensi. Berdasarkan kesimpulan penulis mempertimbangkan pembahasan sebelumnya penulis memilih kriptografi *Vigènere Cipher*.

2) Algoritma *Vigènere Cipher*

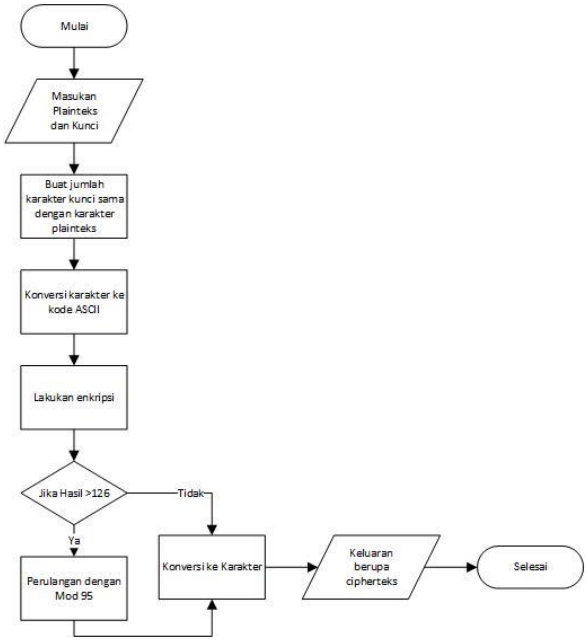


Gambar 3: *Flowchart* proses enkripsi

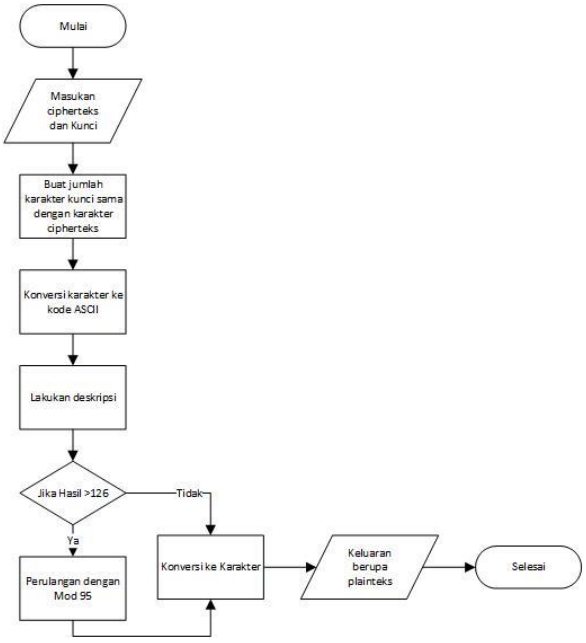


Gambar 4: *Flowchart* proses deskripsi

3) Algoritma *Vigènere Cipher* yang dikustomisasi



Gambar 5: Flowchart proses enkripsi

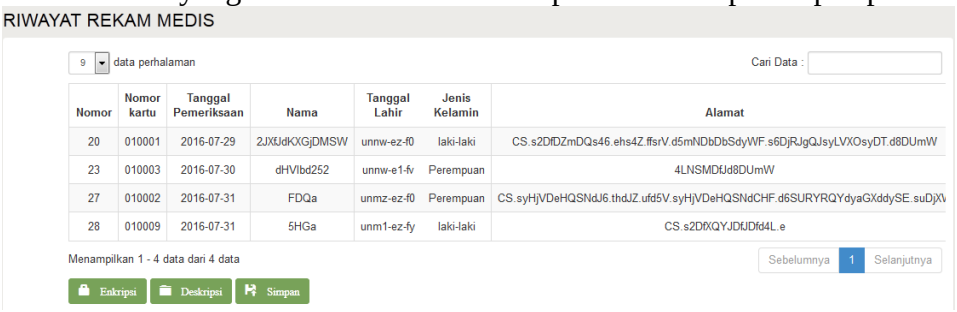


Gambar 6: Flowchart proses enkripsi

C. *Penerapan dan Pengujian*

1) Proses Enkripsi

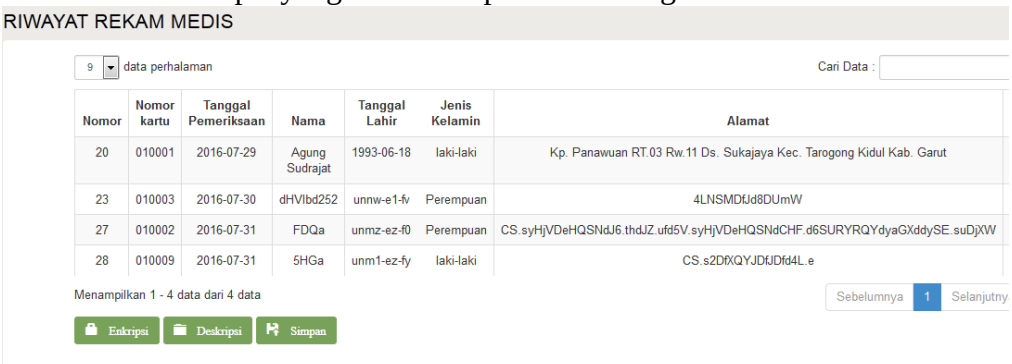
Contoh penerapan enkripsi pada aplikasi rekam medis pasien, yaitu dengan melakukan enkripsi pada data-data yang dianggap penting dan rahasia yaitu dilakukan enkripsi pada data nama, tanggal lahir, alamat, keluhan, tekanan darah, *respiatory rate*, penyakit yang pernah diderita dan nama obat yang diberikan. Berikut merupakan contoh penerapan proses enkripsi :



Gambar 7: Data riwayat rekam medis yang terenkripsi

2) Proses Deskripsi

Untuk melakukan deskripsi yaitu dengan cara memilih data manasaja yang ingin dilakukan deskripsi kemudian tekan tombol deskripsi lalu selanjutnya tekan tombol simpan. Berikut ini merupakan contoh deskripsi yang dilakukan pada data dengan nomor kartu 010001 :



Gambar 7: Data riwayat rekam medis hasil deskripsi

V. KESIMPULAN/RINGKASAN

Berdasarkan hasil kajian dan teori yang ada, kesimpulan dari hasil penelitian ini adalah sebagai berikut :

1. Kriptografi *Vigènere Cipher* ini dapat diterapkan untuk pengamanan aplikasi rekam medis pasien
2. Data yang ada pada rekam medis pasien menjadi lebih aman dari serangan para *kriptanalis* dengan algoritma *Vigènere Cipher* yang dikustomisasi.

DAFTAR PUSTAKA

[1] V. Novianty, "Pengamanan Basis Data Keuangan Koperasi Menggunakan Kriptografi Advance Encryption Standard," *Jurnal Algoritma,* 2015.

[2] E. Munawaroh, "Perancangan Aplikasi Rekam Medis Klinik Bersalin Baiturrahman Menggunakan Object Oriented," *Jurnal Algoritma,* 2013.

[3] B. Rahardjo, Keamanan Sistem Informasi Berbasis Internet, Jakarta: PT INDOCISC, 2005.

[4] A. T. Sholeh, "Pengamanan Skrip pada Bahasa Pemrograman PHP," *Jurnal Algoritma,* 2013.

[5] R. Munir, Kriptografi, Bandung: Informatika, 2006.

[6] K. Peranginangin, Aplikasi Web dengan PHP dan MySQL, Yogyakarta: Andi Offset, 2006.