Implementasi Algoritma Hill Cipher Untuk Keamanan Rekam Medis Di Puskesmas Pematang Raya

Ronaldo Mardianson Sinaga*[1], Nice Rejoice Refisis[2]
[1,2]Program Studi Ilmu Komputer, Fakultas MIPA, Universitas Negeri Medan,
Jl. Willem Iskandar / Pasar V, Kota Medan, 6613319
e-mail: ***[1]ronaldomardianson@gmail.com**, [2]nicerejoicerefisis@gmail.com

Abstrak

Implementasi algoritma hill cipher untuk keamanan rekam medis di puskesmas Pematang Raya dilatarbelakangi karena kurangnya keamanan yang diterapkan pada data rekam medis, sehingga ada kemungkinan orang lain yang tidak berwenang mengakses data rekam medis. Tujuan penelitian ini untuk mengamankan data rekam medis dengan mengimplementasikanya pada algoritma Hill Cipher dan mempermudah dalam mencari data serta mentransimikan data dengan lebih efisien dan aman. Metode yang digunakan adalah Hill Cipher yang dapat diimplementasikan pada data gaji karyawan agar menjadi lebih aman dan data tidak jatuh ke pihak yang tidak berwenang. Pengumpulan data dilakukan dengan menggunakan intrumen penelitian, yaitu wawancara dan studi dokumen. Pada penelitian ini kunci enkripsi dan dekripsinya berupa perkalian matriks dan karakter yang digunakan sebanyak 93 karakter. Dalam penerapan terhadap sistem algoritma Hill Cipher diterapkan pada database, sehingga data tersimpan dengan aman. Hasil pengujian validasi enkripsi dan deskripsi diketahui bahwa sistem dapat mengenkripsi dan mendeskripsikan kembali data sesuai dengan ketentuan algoritma hill cipher. Dari pengujian fungsionalitas dan non fungsionalitas, sistem bekerja sebagaimana mestinya dan dapat menyesuaikan pada perangkat yang digunakan.

Kata kunci*— Kriptografi, Hill Cipher, Rekam Medis.*

Abstract

The implementation of the hill cipher algorithm for medical record security at the Pematang Raya health center is motivated by the lack of security applied to medical record data, so there is a possibility that other unauthorized people access medical record data. The purpose of this study is to secure medical record data by implementing it in the Hill Cipher algorithm and making it easier to search for data and transmit data more efficiently and safely. The method used is Hill Cipher which can be implemented on employee salary data to make it more secure and data does not fall to unauthorized parties. Data collection is carried out using research instruments, namely interviews and document studies. In this study, the encryption and decryption keys are in the form of matrix multiplication and the characters used are 93 characters. In the application of the Hill Cipher algorithm system is applied to the database, so that the data is stored safely. The results of encryption and description validation testing show that the system can encrypt and re-describe data in accordance with the provisions of the hill cipher algorithm. From testing functionality and non-functionality, the system works as it should and can adjust to the device used.

Keywords— *Cryptography, Hill Cipher, Medical Records.*

1. PENDAHULUAN

Kemudahan mendapatkan informasi tidak bisa dilepaskan dari dampak ilmu pengetahuan dan teknologi, salah satunya adalah dampak teknologi [1]. Penggunaan teknologi memang sangat diperlukan, namun masih ada juga hal yang tidak bisa dilupakan yaitu privasi data, karena pada dasarnya setiap informasi memiliki privasinya masing-masing [2].

Pada bidang kesehatan, data pasien baik berupa rekam medis adalah informasi yang bersifat rahasia atau hak milik karena informasi tersebut mencakup informasi pribadi tentang riwayat kesehatan pasien yang dimiliki baik oleh pasien maupun dokter [3]. Pasal 10 dari peraturan rekam medis yang berlaku saat ini yaitu Peraturan Menteri Kesehatan No. 269/MENKES/III/2008 menetapkan bahwa informasi atau data dalam rekam medis memiliki nilai kerahasiaan yang harus dijunjung tinggi karena rekam medis berisi riwayat kesehatan pasien [4].

Selain disimpan oleh puskesmas atau rumah sakit terkait, data rekam medis terkadang juga akan dikirimkan ke rumah sakit lain sebagai data rujukan pasien. Adanya transfer data tersebut tentunya meningkatkan kemungkinan penyebaran atau penyalahgunaan informasi. Melihat adanya kemungkinan tersebut, maka perlu dilakukan pencegahan berupa perlindungan dokumen guna mengurangi hal yang tidak semestinya [2]. Di puskesmas Pematang Raya kegiatan rekam medis belum terkomputerisasi sepenuhnya. Rekam medis di puskesmas ini masih dibuat menggunakan sistem manual dan untuk data rujukan petugas menyimpan data rekam medis di media komputer. Perlindungan data pada media komputer dan pada saat mengirim data perlu diperhatikan guna mengurangi hal yang tidak semestinya.

Kriptografi merupakan ilmu matematika yang juga bersangkutan dengan bidang keamanan informasi seperti integritas entitas, dan integritas data [5]. Kriptografi terdiri dari enkripsi dan deskripsi. Enkripsi mengubah informasi (data) menjadi bentuk yang tidak dapat dimengerti dengan menggunakan algoritma tertentu saat pengiriman sedangkan deskripsi adalah proses sebaliknya [6]. Banyak algoritma kriptografi yang digunakan untuk menjaga keamanan data, seperti *MD2, MD4, LOKI, RSA, GOST, Blowfish, Vigenere*, dll. Masing-masing metode kriptografi ini memiliki kekuatan dan kelemahan. Selain algoritma kriptografi diatas, masih ada algoritma kriptografi lainnya, disini penulis mencoba menggunakan algoritma *Hill Cipher* [7].

Hill Cipher adalah algoritma kriptografi yang menggunakan matriks sebagai kunci untuk melakukan enkripsi dan dekripsi, serta menggunakan aritmetika modulo. Dalam *Hill Cipher*, setiap karakter pada plainteks dan ciperteks dikonversi menjadi angka [8]. Matriks merupakan sekumpulan unsur yang tersusun dalam bentuk kotak persegi panjang dan dibagi jadi kolom dan baris [9]. Operator yang dipake dalam aritmatika modular adalah mod. Operasi modulus memulangkan r, yang ialah sisa dari operasi pembagian yang ditentukan $\alpha \bmod n = r$ [10].

Penelitian sebelumnya dilakukan oleh Aritonang et al., 2019 dalam penelitiannya berjudul "Implementasi Kriptografi Dengan Metode *Hill Cipher* Untuk Keamanan Data Gaji Karyawan Kasir Di PT. Matahari *Department Store Plaza* Medan Fair" [11]. Dari hasil penelitian tersebut diketahui bahwa Metode *Hill Cipher* dapat di implementasikan pada data gaji kariawan yang bertujuan untuk menjaga privasi data menjadi lebih aman sehingga data tidak jatuh ke pihak yang tidak bertanggung berwenang.

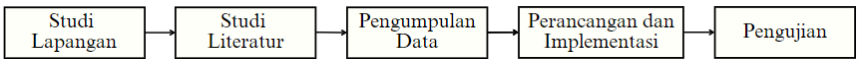
Dari latar belakang diatas diketahui algoritma *Hill Cipher* dapat mengamankan data dengan operasi perkalian matriks dalam proses enkripsi dan deskripsi. Karakter yang digunakan sebanyak 93 kode karakter, sihingga data akan semakin sulit dipecahkan dan *Hill Cipher* merupakan salah satu cipher *clasic* yang sangat susah untuk dipecahkan oleh *cryptanalyst* jika mereka hanya mengetahui file cipherteks [7]. Oleh karena itu penulis tertarik untuk mengimplementasikan algoritma *Hill Cipher* dalam rekam medis, dengan judul "Impementasi Algoritma *Hill Cipher* Untuk Kemanan Rekam Medis di Puskesmas Pematang Raya". Dimana data - data rekam medis dapat dikelola dengan lebih mudah dan ditransmisikan dengan lebih aman, sehingga dapat mengurangi risiko kehilangan atau pencurian data.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan menerapkan metode pengembangan. Penelitian pengembangan ini bertujuan merancang sebuah sistem keamanan data rekam medis yang diimplementasikan pada algoritma *Hill Cipher* di Puskesmas Pematang Raya

2.1 Tahapan Penelitian

Proses penelitian ini melibatkan serangkaian tahapan yang meliputi proses studi lapangan, studi literatur, pengumpulan data, perancangan dan implementasi, dan tahap pengujian. Adapun tahapan tersebut seperti ilustrasi pada Gambar 1 berikut.



Gambar 1 Alur Penelitian

2. 1.1 Studi Lapangan

Tujuan dilakukannya studi lapangan adalah untuk mengumpulkan data dengan mangamati secara langsung pada bagian elemen yang akan diteliti. Dengan proses studi lapangan, peneliti bisa mengetahui apakah permasalahan yang telah dirumuskan sebelumnya benar adanya sesuai dengan kondisi lapangan.

2. 1.2 Studi Literatur

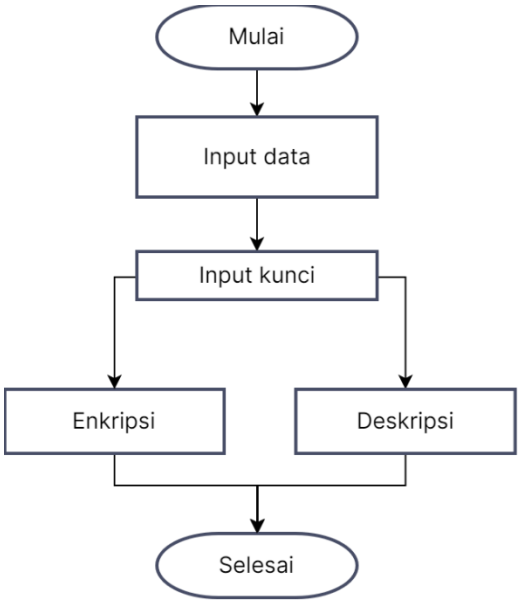
Sumber-sumber ilmiah yang digunakan untuk mendukung penggunaan *Hill Cipher* dalam melindungi data rekam medis diuraikan dalam bagian tinjauan pustaka dari penelitian ini. Kerangka teori yang mendasari penelitian ini mengacu pada literatur ilmiah yang bersumber dari jurnal, publikasi, situs web resmi, dan penelitian sebelumnya yang berkaitan dengan pokok bahasan atau terkait erat dengan masalah penelitian.

2. 1.3 Pengumpulan Data

Pengumpulan data pada penelitian ini dilakukan dengan mengumpulkan lembar formulir rekam medis di puskesmas Pematang Raya yang akan di implementasikan ke dalam sistem aplikasi kemamanan data rekam medis pasies dengan menggunakan algoritma *Hill Cipher*.

2. 1.4 Perancangan dan implementasi

Tahap ini dilakukan untuk merancang dan mendesain sistem implementasi algoritma *Hill Cipher* untuk kemanana data rekam medis yang dibutuhkan berdasarkan hasil dari analisis kebutuhan. Implementasi dimulai dengan menyusun data yang diterima dan menyesuaikannya dengan sistem yang dibuat. Informasi seperti nama, alamat, deskripsi rekam medis, dan gejala kemudian digunakan untuk mengenkripsi dan mendeskripsikan algoritma *Hill Cipher*. Pada tahap ini, aturan-aturan diimplementasikan ke dalam mesin inferensi menggunakan kriptografi, dan algoritma *Hill Cipher* diimplementasikan ke dalam bahasa pemrograman menggunakan kompiler kode Visual Studio. Berikut adalah gambar alur perancangan sistem enkripsi dan deskripsi



Gambar 2 Alur Perancangan Sistem Enkripsi dan Deskripsi

Proses enkripsi melibatkan penggunaan algoritma dan kunci. Proses enkipsi ini dilakukan dengan memasukkan data pasien dengan format nama, tanggal lahir, gender, alamat, agama, NIK, layanan, nomor BPJS, alergi, *vital sign*, *anamnensis*, diagnosa dan catatan dokter lalu memasukan kunci matriks sebagai implementasi algoritma Hill Cipher dalam keamanan data. Secara matematika, proses enkripsi pada *Hill Cipher* adalah sebagai berikut ini [12]:

$$C = K \,.\, P \quad (1)$$

Proses deskripsi dilakukan dengan memasukan kembali kunci yang sama pada saat enkripsi. Proses dekripsi pada *Hill Cipher* sama dengan proses enkripsi, tetapi dengan langkah tambahan yaitu membalik kunci matriks. Secara matematika, dekripsi *Hill Cipher* dapat diperoleh dari persamaan 2.1 yang disebutkan sebelumnya. Secara matematika, proses deskripsi pada *Hill Cipher* adalah sebagai berikut ini [12]:

$$P = K - 1 \,.\, P \quad (2)$$

2. 1.5 Pengujian

Pengujian yang dilakukan dalam penelitian ini mencakup beberapa aspek, seperti analisis vektor uji, pengujian keamanan, pengujian validasi enkripsi, pengujian fungsionalitas sistem, dan pengujian non-fungsionalitas sistem. Tujuan dari pengujian vektor uji adalah untuk memverifikasi bahwa cipherteks yang dihasilkan oleh algoritma *Hill Cipher* sesuai dengan hasil yang diharapkan berdasarkan kunci yang diberikan dan plainteks, seperti yang ditentukan melalui perhitungan matematis secara manual. Pengujian keamanan bertujuan untuk melihat apakah data yang tersimpan di sistem dan database terenkripsi atau tidak. Tujuan dari pengujian validasi enkripsi adalah untuk memastikan bahwa output dari proses enkripsi sesuai dengan deskripsi plainteks asli. Tujuan pengujian fungsionalitas adalah untuk memastikan bahwa sistem sesuai dengan tujuan yang dimaksudkan, sedangkan pengujian non-fungsional berfokus pada verifikasi kompatibilitas sistem dengan *browser web* yang berbeda, seperti Google Chrome, Mozilla Firefox, dan Microsoft Edge, dalam hal aksesibilitas yang memadai [3].

3. HASIL DAN PEMBAHASAN

Kode karakter yang digunakan pada sistem disesuaikan berdasarkan kebutuhan, yaitu berupa huruf, angka, tanda baca dan simbol sebanyak 93 karakter yang terdiri dari

"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!#$%&'( )*+,-./:;<=>?@[\]^_`{|}~ ". Selanjutya kode karakter tersebut di konversikan menjadi angka dari 0 – 92 secara berurutan seperti tabel berikut.

Tabel 1 Konversi Kode Karakter

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
V	W	X	Y	Z	a	b	c	d	e	f	g	h	i	j	k	l	M	n	o
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
q	r	s	t	u	v	w	X	y	z	0	1	2	3	4	5	6	7	8	9
42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61
#	$	%	&	‘	(	)	*	+	,	-	.	/	:	;	<	=	>	?	@
63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82
\	]	^	_	`	{	|	}	~											
84	85	86	87	88	89	90	91	92											

3.1 Perhitungan Hill Cipher

Untuk percobaan perhitungan manual *Hill Cipher* dengan menggunakan *plaintext* P yaitu HELLO WORLD, dan Kunci K =$\begin{pmatrix}2 & 1\\3 & 4\end{pmatrix}$, maka:

a. Bagi *plaintext* P menjadi matriks 2 x 1 dan konversi menjadi angka sesuai dengan tabel 1.

$\begin{pmatrix}H\\E\end{pmatrix} = \begin{pmatrix}7\\4\end{pmatrix}$
$\begin{pmatrix}L\\L\end{pmatrix} = \begin{pmatrix}11\\11\end{pmatrix}$
$\begin{pmatrix}O\\W\end{pmatrix} = \begin{pmatrix}14\\22\end{pmatrix}$
$\begin{pmatrix}O\\R\end{pmatrix} = \begin{pmatrix}14\\17\end{pmatrix}$
$\begin{pmatrix}L\\D\end{pmatrix} = \begin{pmatrix}11\\3\end{pmatrix}$

b. Kalikan setiap angka dengan matriks kunci.

$\begin{pmatrix}2 & 1\\3 & 4\end{pmatrix} \cdot \begin{pmatrix}7\\4\end{pmatrix} = \begin{pmatrix}14 + 4\\21 + 16\end{pmatrix} = \begin{pmatrix}18\\37\end{pmatrix}$
$\begin{pmatrix}2 & 1\\3 & 4\end{pmatrix} \cdot \begin{pmatrix}11\\11\end{pmatrix} = \begin{pmatrix}22 + 11\\33 + 44\end{pmatrix} = \begin{pmatrix}33\\77\end{pmatrix}$
$\begin{pmatrix}2 & 1\\3 & 4\end{pmatrix} \cdot \begin{pmatrix}14\\22\end{pmatrix} = \begin{pmatrix}28 + 22\\42 + 88\end{pmatrix} = \begin{pmatrix}50\\130\end{pmatrix}$
$\begin{pmatrix}2 & 1\\3 & 4\end{pmatrix} \cdot \begin{pmatrix}14\\17\end{pmatrix} = \begin{pmatrix}28 + 17\\42 + 68\end{pmatrix} = \begin{pmatrix}45\\110\end{pmatrix}$
$\begin{pmatrix}2 & 1\\3 & 4\end{pmatrix} \cdot \begin{pmatrix}11\\3\end{pmatrix} = \begin{pmatrix}22 + 3\\33 + 12\end{pmatrix} = \begin{pmatrix}25\\45\end{pmatrix}$

c. Selanjutnya melakukan proses Mod 93 pada setiap operasi matriks angka tersebut agar dapat dikonversi menggunakan tabel 1.

$\begin{pmatrix}18\\37\end{pmatrix}$ Mod 93 = = $\begin{pmatrix}18\\37\end{pmatrix}$
$\begin{pmatrix}33\\77\end{pmatrix}$ Mod 93 = $\begin{pmatrix}33\\77\end{pmatrix}$
$\begin{pmatrix}50\\130\end{pmatrix}$ Mod 93 = $\begin{pmatrix}50\\37\end{pmatrix}$
$\begin{pmatrix}45\\110\end{pmatrix}$ Mod 93 = $\begin{pmatrix}45\\17\end{pmatrix}$
$\begin{pmatrix}25\\45\end{pmatrix}$ Mod 93 = $\begin{pmatrix}25\\45\end{pmatrix}$

d. Mengubah seluruh matriks angka menjadi huruf dengan konversi seperti tabel 1.

$\begin{pmatrix}18\\37\end{pmatrix} = \begin{pmatrix}S\\l\end{pmatrix}$

$\binom{33}{77} = \binom{h}{;}$
$\binom{50}{37} = \binom{y}{l}$
$\binom{45}{17} = \binom{t}{R}$
$\binom{25}{45} = \binom{Z}{t}$

Dari proses enkripsi yang telah di lakukan di atas sehingga diperoleh pesan HELLOWORLD yang telah berhasil dienkripsi menjadi Slh;yltRZt.

Proses dekripsi pada *Hill Cipher* sama dengan proses enkripsi, tetapi dengan langkah tambahan yaitu membalik kunci matriks. Dengan kunci K =$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$, selanjutnya proses dekripsi yang pertama harus dilakukan adalah dengan mencari nilai *invers* matriks K. Nilai *invers* matriks bisa ditemukan menggunakan Operasi Baris Elementer (OBE) ataupun dengan prinsip determinan.

$K{-}1 = \begin{pmatrix} 4 & -1 \\ -3 & 2 \end{pmatrix}$
$K{-}1 = \begin{pmatrix} 224 & -56 \\ -168 & 112 \end{pmatrix}$
$-1 = \begin{pmatrix} 38 & 37 \\ 18 & 19 \end{pmatrix}$

Matriks K^{-1} menjadi kunci untuk deskripsi, maka:

a. Bagi *plaintext* P menjadi perkalian 2 x 1 dan konversi menjadi angka sesuai tabel 4.1.

$\binom{S}{l} = \binom{18}{37}$
$\binom{h}{;} = \binom{33}{77}$
$\binom{y}{l} = \binom{50}{37}$
$\binom{t}{R} = \binom{45}{17}$
$\binom{Z}{t} = \binom{25}{45}$

b. Melakukan perkalian pada setiap angka dengan matriks kunci:

$\begin{pmatrix} 38 & 37 \\ 18 & 19 \end{pmatrix} \cdot \binom{18}{37} = \binom{684 + 1369}{324 + 703} = \binom{2053}{1027}$
$\begin{pmatrix} 38 & 37 \\ 18 & 19 \end{pmatrix} \cdot \binom{33}{77} = \binom{1254 + 2849}{594 + 1463} = \binom{4103}{2057}$
$\begin{pmatrix} 38 & 37 \\ 18 & 19 \end{pmatrix} \cdot \binom{50}{37} = \binom{1900 + 1369}{900 + 703} = \binom{3269}{1603}$
$\begin{pmatrix} 38 & 37 \\ 18 & 19 \end{pmatrix} \cdot \binom{45}{17} = \binom{1710 + 629}{810 + 323} = \binom{2339}{1133}$
$\begin{pmatrix} 38 & 37 \\ 18 & 19 \end{pmatrix} \cdot \binom{25}{45} = \binom{950 + 1665}{450 + 855} = \binom{2615}{1305}$

c. Membuat operasi Modulo 93 ke matriks angka supaya dapat dikonversi kembali.

$\binom{2053}{1027}$ Modulo 93 = $\binom{7}{4}$

$\binom{4103}{2057}$ Modulo 93 = $\binom{11}{11}$

$\binom{3269}{1603}$ Modulo 93 = $\binom{14}{22}$

$\binom{2339}{1133}$ Modulo 93 = = $\binom{14}{17}$

$\binom{2615}{1305}$ Modulo 93 = = $\binom{11}{3}$

d. Mengubah setiap matriks angka jadi huruf dengan aturan konversi seperti tabel 1.

$$\begin{pmatrix}7\\4\end{pmatrix} = \begin{pmatrix}\mathrm{H}\\\mathrm{E}\end{pmatrix}$$

$$\begin{pmatrix}11\\11\end{pmatrix} = \begin{pmatrix}L\\L\end{pmatrix}$$

$$\begin{pmatrix}14\\22\end{pmatrix} = \begin{pmatrix}O\\W\end{pmatrix}$$

$$\begin{pmatrix}14\\17\end{pmatrix} = \begin{pmatrix}O\\R\end{pmatrix}$$

$$\begin{pmatrix}11\\3\end{pmatrix} = \begin{pmatrix}L\\D\end{pmatrix}$$

Sehingga diperoleh pesan Slh;yltRZt yang telah didekripsi kembali menjadi HELLOWORLD.

3.2 Tampilan Sistem

Penelitian ini menghasilkan sistem kemanan rekam medis pada puskesmas pematang raya yang di implementasikan dengan algoritma *Hill Cipher*. Berikut ini merupakan tampilan dan pembahasan dari aplikasi yang telah dibuat.

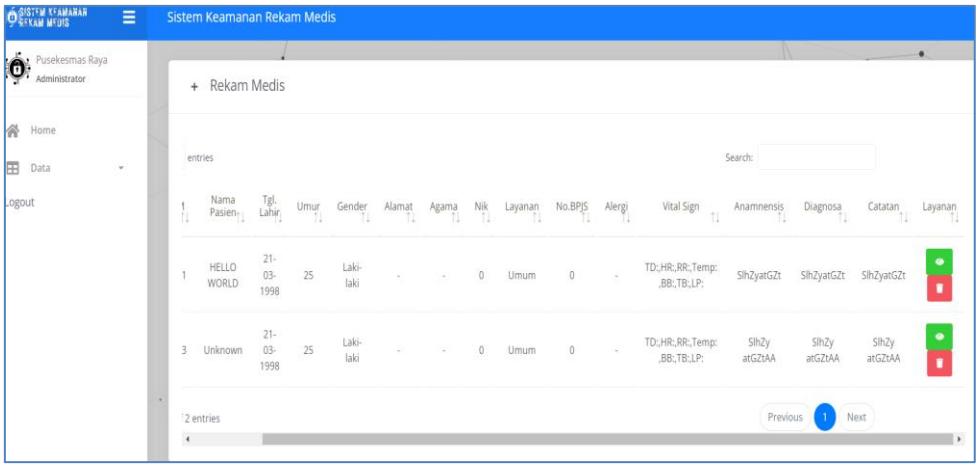
3.2.1 Halaman Home

Tampilan home merupakan tampilan setelah berhasil masuk ke sistem setelah halaman *login*. Tampilan halaman home dapat dilihat pada gambar di bawah ini.

Gambar 3 Halaman Home

3.2.2 Halaman Data Rekam Medis

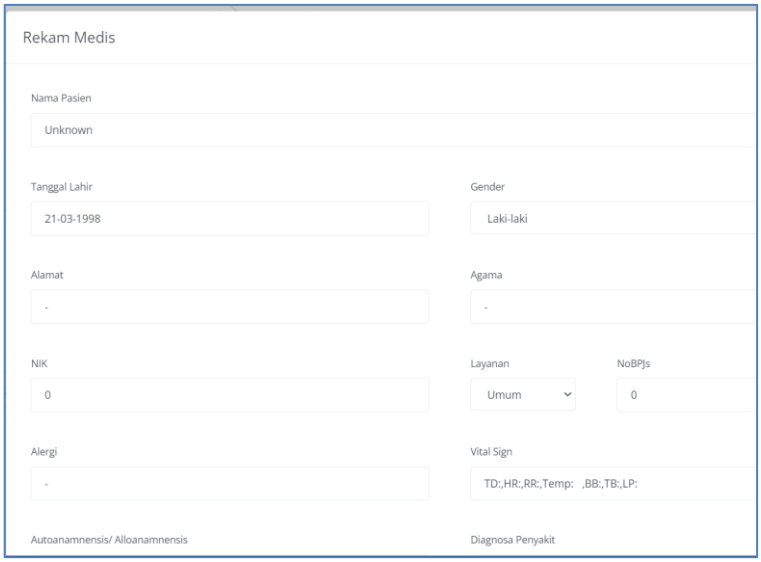
Pada halaman Data Rekam Medis pengguna dapat mengolah data yang ditampilkan pada aplikasi. Pada menu ini pengguna dapat menambahkan data dengan masuk ke menu + Rekam Medis, dan pada saat menambah data rekam medis, pengguna juga melakukan pembentukan kunci untuk proses enkripsi data. Di menu ini juga ada tombol hapus dengan icon keranjang sampah, dan icon mata untuk tombol menampilkan data yang akan di deskripsi.



Gambar 4 Halaman Data

3.2.3 Tambah Data (enkripsi)

Pada halaman tambah data rekam medis, pengguna dapat melakukan penambahan data dengan mengisi data rekam medis pasien sesuai format pengisian *form* yang sudah tersedia di sitem. Selanjutnya pengguna perlu menambahkan kunci matriks sebagai pengamanan data rekam medis yang nantinya bertujuan untuk enkripsi data diagnosa pasien. Untuk lebih jelasnya, tampilan halaman tambah data rekam medis dapat dilihat pada gambar dibawah ini:

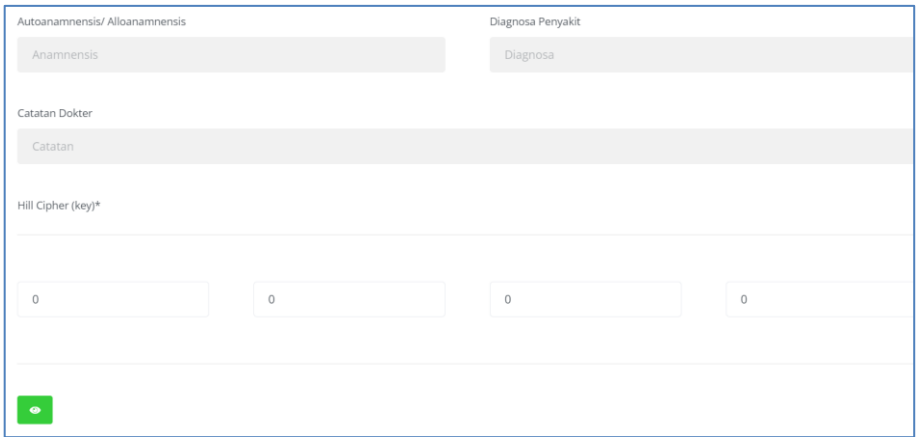


Gambar 5 Tambah Data

3.2.4 Lihat data (deskripsi)

Pada halaman ini menampilkan data yang sudah di tambahkan sebelumnya yang akan di deskripsi kembali pada data diagnosa dokter dengan menggunakan kunci yang sama pada proses tambah data (enkripsi) sebelumnya.

Tampilan data diagnosa dokter sebelum di deskripsi dapat di lihat pada gambar di bawah ini dengan contoh data anamnensis, diagnosa, dan cacatan dokter dengan kalimat “HELLOWORLD”



Gambar 6 Lihat Data

3.3 Pengujian Sistem

3.3.1 Test Vector

Pengujian *test vector* digunakan untuk memverifikasi bahwa implementasi algoritma *Hill Cipher* dalam sistem menghasilkan *ciphertext* yang sama dengan hasil yang diharapkan dari algoritma *Hill Cipher* yang telah ditentukan sebelumnya oleh penciptanya. Dengan menggunakan *test vector* yang telah ditentukan sebelumnya, dapat dipastikan bahwa sistem menghasilkan output *ciphertext* yang konsisten dan sesuai dengan algoritma yang diinginkan. Pengujian ini penting untuk memvalidasi kebenaran implementasi algoritma *Hill Cipher* pada sistem.

Tabel 2 Hasil Test Vector

Ket	Perhitungan Manual	Hasil Sistem
Key	$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$	$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$
Plaintext	HELLOWORLD	HELLOWORLD
Ciphertext	Slh;yltRZt	Slh;yltRZt

3.3.2 Pengujian Keamanan

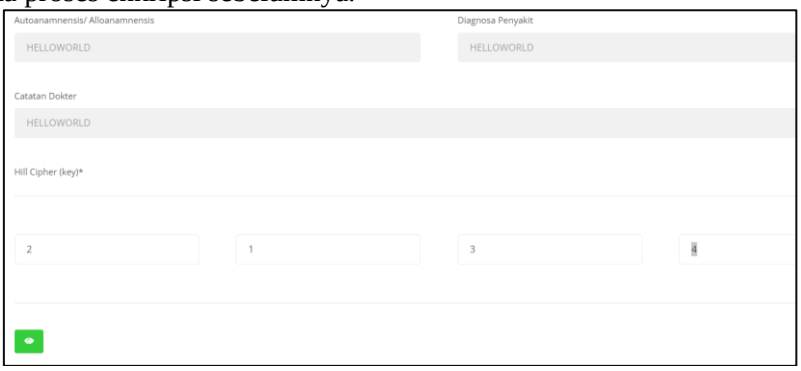
Proses tes keamanan pada kunci yang digunakan pada sistem, yaitu dengan menggunakan kunci yang tidak sama pada saat menyimpan data.

Gambar 7 Invalid Key

Dari gambar di atas dapat diketahui bahwa dengan kunci yang berbeda makan data sebelumnya yang di simpan tidak bisa di deskripsikan kembali atau *Invalid Key*. Yang seharusnya jika di deskripsi dengan kunci yang benar akan menampilkan kata "HELLOWORLD", yang sebelumnya yang sudah di input dengan kunci matriks 2, 1, 3, 4.

3.3.3 Validasi Enkripsi dan Deskripsi

Uji verifikasi enkripsi dan deskripsi digunakan untuk memastikan bahwa data dienkripsi sesuai dengan algoritma yang digunakan. Untuk mendapatkan hasil verifikasi, Anda dapat membuktikannya dengan membandingkan hasil deskripsi dengan *plaintext* sebelum melakukan proses enkripsi. Untuk melakukan proses enkripsi, Anda membutuhkan kunci yang telah digunakan pada proses enkripsi sebelumnya.



Gambar 8 Sesudah Deskripsi

Dari hasil deskirpsi pada gambar 8 dapat diketahui bahwa data yang sudah di enkripsi sebelumnya dapat di deskripsi kembali dari ciperteks "Slh;yltRZt" menjadi "HELLOWORLD".

3.3.4 Pengujian Fungsionalitas dan Non-Fungsionalitas

Tabel 3 Pengujian Fungsional tambah data (enkripsi)

Nama Uji Kasus	Insert Data
Prosedur	- Masuk ke halaman tambah data dengan menekan menu tambah - Memasukkan data rekam medik pasien dan kunci matriks yang valid. - Simpan data dengan tekan tombol "simpan"
Hasil yang di harapkan	Sistem akan memperlihatkan notifikasi pesan "berhasil" Lalu mengarahkan sistem ke menu data.
Hasil	Sistem akan memperlihatkan notifikasi pesan "berhasil" Lalu mengarahkan sistem ke menu data.
Status	Valid

Tabel 4 Pengujian Fungsional lihat data (deskripsi)

Nama Uji Kasus	Lihat Data
Prosedur	- Menekan tombol lihat "icon mata" - Masuk ke halaman lihat data - Masukan Kunci yang valid
Hasil Yang di Harapkan	Sistem akan menampilkan data yang di deskripsi kembali
Hasil	Sistem akan menampilkan data yang di deskripsi kembali
Status	Valid

Tabel 5 Pengujian Fungsional Portability

Nama Uji Kasus	*Portability*
Prosedur	Sistem ini berjalan di berbagai peramban web seperti Mozilla Firefox, Google Chrome, dan Microsoft Edge pada sistem operasi Windows.
Hasil Yang di Harapkan	Sistem dapat digunakan dengan lancar dan tampilan dapat menyesuaikan.
Hasil	Sistem dapat digunakan dengan lancar dan tampilan dapat menyesuaikan.
Status	Valid

Dari hasil pembahasan diatas implementasi sistem yang dibuat sesuai dengan ketentuan algortima *Hill Cipher* dimana hasil enkripsi dan deskripsi yang dihasilkan oleh sistem sama dengan enkripsi perhitungan manual *Hill Cipher*. Seperti pada pengujian sebelumnya, uji validasi enkripsi dan deskripsi membuktikan bahwa data yang dienkripsi sesuai dengan algoritma yang digunakan. Pada segi keamanan, data yang di enkripsi tidak dapat diketahui dengan kunci yang tidak sama pada saat menyimpan data. Untuk fungsional sistem berjalan sesuai fungsinya masing – masing, dan sistem dapat berjalan di berbagai peramban web dan sistem dapat menyesuaikan tampilan pada perangkat yang digunakan.

4. KESIMPULAN

Setelah melakukan berbagai macam tahapan-tahapan maka diperoleh suatu kesimpulan sebagai berikut:

1. Algoritma *Hill Cipher* dapat di implementasikan pada keamanan data rekam medis, sehingga data rekam medis yang di *input* ke dalam sistem menjadi lebih aman.
2. Algoritma *Hill Cipher* dapat digunakan untuk melindungi data rekam medis dengan proses enkripsi pada data diagnosa pasien dan mendeskripsikan kembali dengan kunci yang sama pada saat enkripsi yang di buktikan berdasarkan hasil *test vector*.
3. Di pengujian keamanan, data yang sudah di tambahkan dalam sistem dapat di amankan dengan baik dengan proses enkripsi algoritma *Hill Cipher* sehingga data yang ada pada database dan sistem tidak dapat dibaca.

Pada pengujian fungsional sistem dan non-fungsional sistem, sistem dapat berjalan dengan baik sesuai dengan fungsinya dan sistem dapat berjalan pada berbagai web browser.

5. SARAN

Kunci yang digunakan pada sistem Algoritma *Hill Cipher* ini menggunakan kunci matriks 2x2, sehingga untuk pengembangan selanjutnya dapat menggunakan kunci yang lebih banyak dan diharapkan sistem ini dikembangkan dengan filtur sistem yang lebih lengkap sehingga terus berkembang dalam mengamankan data

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak Puskesmas Pematang Raya yang telah memberi kesempatan untuk dijadikan objek dalam melakukan penelitian ini. Penulis juga menyampaikan terimakasih kepada tim reviewer dan pihak terkait dalam publikasi artikel ini.

DAFTAR PUSTAKA

[1] Y. P. Putra, T. Mufizar, and E. Alfiyani, "IMPLEMENTASI SUPER ENKRIPSI AES DAN RSA PADA PENGAMANAN DATA REKAM MEDIS PASIEN," 2022.

[2] O. G. Khoirunnisa and D. Djuniadi, "Implementasi Algoritma AES untuk Keamanan Data Rekam Medis," *Jurnal Pengkajian dan Penerapan Teknik Informatika*, vol. 15, no. 1, pp. 21–27, Dec. 2021, doi: 10.33322/petir.v15i1.1333.

[3] Kartika H, "Implementasi Algoritme Speck Dan Sha-3 Pada Database Rekam Medik," 2018.

[4] A. Tarigan and L. Herfiyanti, "Tinjauan Aspek Keamanan dan Kerahasian Rekam Medis di Ruang Filing RS BSA Bandung," *Cerdika: Jurnal Ilmiah Indonesia*, vol. 1, no. 11, pp. 1454–1460, Nov. 2021, doi: 10.36418/cerdika.v1i11.222.

[5] D. Calista, A. Farissi, and M. Diana Marieska, "Sistem Pengamanan Data Menggunakan Kriptografi AES dan Blockchain Berbasis Android," *Jurnal JUPITER*, vol. 13, no. 2, pp. 220–226, 2021.

[6] F. Muharram, "Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard," *Prosiding Seminar Nasional Ilmu Komputer dan Teknologi Informasi*, vol. 3, no. 2, 2018.

[7] I. Gunawan *et al.*, "FUNGSI ALGORITMA KRIPTOGRAFI HILL CIPHER UNTUK PENGAMANAN FILE GAMBAR DAN PESAN TEKS," *TECHSI*, vol. 10, no. 1, pp. 119–128, 2018, doi: 10.29103/techsi.v10i1.605.

[8] A. Hidayat and T. Alawiyah, "Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang," *Jurnal Matematika Integratif*, vol. 9, no. 1, pp. 39–51, 2013.

[9] A. Vega, "ENKRIPSI DAN DEKRIPSI PESAN MENGGUNAKAN POLINOMIAL GALOIS FIELDDENGAN ALGORITMA HILL CIPHER," Skripsi, Universitas Islam Negeri Maulana Malik Ibrahim, Malang, 2022.

[10] Fadlilah S, "Enkripsi dan Deskripsi Menggunakan Algoritma Hill Cipher dan Elgamal untuk Mengamankan Pesan Teks," Skripsi, Universitas Islam Negeri Maulana Malik Ibrahim, Malang, 2021.

[11] O. Gusti Awang Aritonang, B. Anwar, and F. Taufik, "'Implementasi Kriptografi Menggunakan Metode HILL CIPHER Untuk Keamanan Data Gaji Karyawan Kasir Di PT. Matahari Department Store Plaza Medan Fair,'" Medan , 2019.

[12] A. Rotal Yuliandaru -, "Teknik Kriptografi Hill Cipher Menggunakan Matriks," Bancung, 2016.