Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 2, September 2022, pp. 740-753
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Implementasi Super Enkripsi Menggunakan Metode *Rail Fence Cipher* dan Metode *Caesar Cipher* Pada Data Pasien Klinik Eka Karigas

Fery Fernando[1*], Magdalena A. Ineke Pakereng[2]
[1,2]Jurusan Teknik Informatika, FTI UKSW, Salatiga, Indonesia
e-mail: [1]672018116@student.uksw.edu, [2]ineke.pakereng@uksw.edu

Abstract

Data security is considered very important in nowadays information technology era to minimize data theft. To achieve data security, an encoding process for the data is needed. The encryption process can use a super encryption scheme by combining two or more cryptographic techniques to provide double security. In this research intend to implement the Rail Fence Cipher and Caesar Cipher cryptographic algorithms by using a super encryption scheme on patient data at the Eka Karigas Clinic. The combination of these two cryptographic algorithms is able to provide security by using encryption techniques on patient data at the Eka Karigas Clinic and returning it using a decryption technique to its original form so as not to cause data integrity loss.

Keywords*: Plaintext, Ciphertext, Super Encryption, Rail Fence Cipher, Caesar Cipher*

Abstrak

Keamanan data dinilai sangat penting pada masa teknologi informasi sekarang untuk meminimalkan pencurian data. Untuk mencapai keamanan data dibutuhkan proses penyandian terhadap data tersebut. Proses penyandian dapat menggunakan skema super enkripsi dengan menggabungkan dua atau lebih teknik kriptografi untuk memberikan keamanan ganda. Pada penelitian ini bertujuan mengimplementasikan algoritma kriptografi Rail Fence Cipher dan Caesar Cipher dengan menggunakan skema super enkripsi pada data pasien Klinik Eka Karigas. Kombinasi dua algoritma kriptografi ini dapat memberikan keamanan dengan menggunakan teknik enkripsi pada data pasien Klinik Eka Karigas dan dikembalikan kembali menggunakan teknik dekripsi ke bentuk aslinya sehingga tidak menyebabkan kehilangan integritas data.

Kata kunci*: Plaintext, Ciphertext, Super Enkripsi, Rail Fence Cipher, Caesar Cipher*

1. PENDAHULUAN

Keamanan data dinilai cukup penting dalam teknologi informasi zaman sekarang. Keamanan data diperlukan agar meminimalkan pencurian data. Untuk mencapai keamanan data tersebut, dilakukan proses penyandian terhadap data tersebut. Proses penyandian yang dilakukan adalah dengan menggunakan kriptografi. Kriptografi adalah ilmu dan seni yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta autentikasi. Enkripsi adalah proses pengaman pesan asli menjadi kode-kode yang tidak dimengerti. Sedangkan proses pembalikan kode-kode yang tidak dimengerti menjadi pesan kedalam bentuk asalnya disebut deskripsi [1,2]. Dalam pengamanan data untuk mendapatkan keamanan yang lebih baik diperlukan metode kriptografi yang lebih kuat. Super enkripsi adalah suatu konsep yang

menggabungkan dua atau lebih teknik substitusi dan transposisi untuk mendapatkan metode yang lebih andal [3,4].

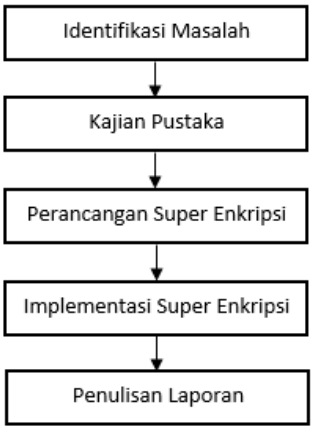
Rail Fence cipher merupakan salah satu kriptografi klasik yang termasuk dalam kriptografi transposisi. *Rail Fence cipher* membentuk suatu lintasan dengan menggubah posisi dan susunan karakter *plaintext* kedalam bentuk diagonal ke bawah dan ke atas untuk menghasilkan *ciphertext* dari *Rail Fence cipher* [5]. Caesar *cipher* merupakan salah satu kriptografi klasik yang termasuk dalam kriptografi subtitusi. Caesar *cipher* memiliki cara kerja menggeser setiap huruf dengan huruf lain dengan selisih tertentu sehingga menjadi algoritma standar dari Caesar *cipher*. Algoritma standar tersebut digunakan dalam pengaakan *plaintext* ke dalam bentuk *ciphertext* [1].

Dengan alasan keamanan data yang dinilai sangat penting pada zaman sekarang sehingga keamanan data pasien pada Klinik Eka Karigas dinilai sangat perlu agar menghindari pencurian data pribadi pasien maupun data *medical check* dari pasien-pasien yang melakukan kunjungan pada Klinik Eka Karigas. Penelitian ini mengimplementasi algoritma kriptografi menggunakan skema super enkripsi pada data pasien Klinik Eka Karigas dengan menggunakan dua teknik algoritma klasik yaitu *Rail Fence cipher* yang termasuk dalam teknik kriptografi transposisi dan Caesar *cipher* yang termasuk dalam teknik kriptografi substitusi.

2. METODOLOGI PENELITIAN

2.1. Tahapan Penelitian

Tahapan yang dilakukan dalam penelitian ini terdiri dari 5 (lima) tahap yaitu: Identifikasi Masalah, Kajian Pustaka, Perancangan Super enkripsi, Implementasi Super enkripsi, Penulisan Laporan.



Gambar 1. Tahapan Penelitian

a) Identifikasi Masalah
   Identifikasi Masalah, dilakukan untuk mengidentifikasi masalah yang berhubungan dengan keamanan data. Selain itu menentukan batasan masalah dalam penelitian ini yaitu; menggunakan metode super enkripsi pada data teks.

b) Kajian Pustaka
Kajian Pustaka, mempelajari literatur yang berkaitan dengan super enkripsi lebih terkhusus pada penelitian terdahulu sebagai acuan dalam penelitian ini.
c) Perancangan Super Enkripsi
Perancangan Super Enkripsi, merancang program proses enkripsi-dekripsi dengan metode super enkripsi menggunakan metode *Rail Fence cipher* dan Caesar *cipher*.
d) Implementasi Super Enkripsi
Implementasi Super Enkripsi, mengimplementasikan hasil rancangan super enkripsi pada data pasien Klinik Eka Karigas dalam bentuk *plaintext* untuk menghasilkan *ciphertext*.
e) Penulisan Laporan
Penulisan Laporan, hasil penelitian yang selesai dilakukan kemudian ditulis dalam laporan penelitian.

2.2. Tinjauan Pustaka

Pada penelitian berjudul Teknik Super Enkripsi Teks Kriptografi Menggunakan Algoritma *Hill Cipher* Dan Transposisi Kolom membahas tentang perancangan super enkripsi dengan menggunakan dua algoritma yaitu algoritma *Hill cipher* dan Transposisi Kolom. Penulis mengungkapkan bahwa teknik super enkripsi sangatlah baik digunakan dalam keamanan berganda tepatnya pada menanggulangi kebocoran data karena dapat menambah keamanan yang lebih. Dengan menggabungkan algoritma *Hill cipher* dan transposisi kolom, peretas lebih sulit memecahkan sandi daripada hanya menggunakan salah satu *cipher* substitusi atau *cipher* transposisi saja [6].

Pada penelitian berjudul Teknik Analisa Algoritma *Ciphers Transposition*: *Study Literature* membahas tentang penelitian terdahulu yang berkaitan dengan algoritma transposisi *cipher*. Penulis mengungkapkan masing-masing transposisi *cipher* memiliki kelebihan, kekurangan dan cara kerjanya tersendiri. Menurut penulis, kelebihan dari *Rail Fence cipher* adalah bentuk lintasan '*zig-zag*' yang dihasilkan untuk mengubah *plaintext* ke dalam bentuk *ciphertext* sehingga menambah kerumitan pada proses enkripsi pesan maupun dekripsi pesan. Kekurangan dari *Rail Fence cipher* adalah tidak ada perubahan karakter menjadi karakter lainnya, hanya mengubah posisi plaintext. Sehingga dirasa *ciphertext* masih dapat dipecahkan [7].

Pada Penelitian berjudul Implementasi Kombinasi Caesar dan *Affine Cipher* untuk Keamanan Data teks membahas tentang pengamanan data teks menggunakan teknik enkripsi super dengan mengkombinasikan dua kriptografi klasik subtitusi yaitu Caesar *cipher* dengan *Affine cipher*. Penulis menyimpulkan bahwa menggabungkan Caesar *cipher* dengan *Affine cipher* dapat membantu meningkatkan keamanan data daripada hanya menggunakan satu teknik kriptografi saja [8].

Pada Penelitian berjudul Perancangan Aplikasi Pengamanan Pesan Dengan Algoritma Caesar *Chiper* membahas tentang pengimplementasian algoritma Caesar *cipher* pada aplikasi pengamanan pesan. Penulis menyimpulkan bahwa keamanan pengiriman pesan dapat diimplementasikan dalam bentuk aplikasi dengan menggunakan metode enkripsi salah satunya adalah dengan menggunakan algoritma Caesar *cipher* [9].

Pada Penelitian berjudul Pengamanan Data Teks Melalui Perpaduan Algoritma *Beaufort* dan Caesar *Cipher* membahas tentang pengamanan data teks menggunakan teknik enkripsi super dengan mengkombinasikan dua kriptografi klasik yaitu *Beaufort cipher* dengan Caesar *cipher*. Penelitian ini bertujuan untuk mengoptimalkan penggunaan algoritma Caesar *cipher* dalam pengaman data dengan menggabungkannya dengan algoritma *Beaufort cipher* yang merupakan turunan dari *Vigenere cipher.* Penulis menyimpulkan bahwa konsep keamanan data dengan menggunakan perpaduan algoritma *Beaufort cipher* dan Caesar *cipher* berhasil dan dapat digunakan dalam melakukan pengamanan terhadap data teks [10].

Berdasarkan penelitian-penelitian sebelumnya maka dilakukan penelitian tentang perancangan super enkripsi dengan menggunakan metode *Rail Fence cipher* dan metode Caesar *Cipher* untuk mendapatkan metode enkripsi baru dengan keamanan ganda dan diimplementasikan dalam pengamanan data pasien Klinik Eka Karigas.

Selanjutnya akan dibahas dasar-dasar teori yang digunakan dalam perancangan super enkripsi pada penelitian ini. Kriptografi adalah ilmu yang mempelajari teknik matematis yang berhubungan dengan aspek keamanan informasi seperti tingkat keyakinan, integritas data, autentikasi entitas dan autentikasi keaslian data. Dapat disebut juga bahwa kriptografi menggunakan teknik matematika dan seni untuk menyandikan pesan agar tidak dapat dipahami oleh orang yang ingin mencuri informasi dari pesan tersebut. Dalam kriptografi, pesan atau informasi yang dapat dibaca disebut sebagai *plaintext* atau teks terang. Proses yang dilakukan untuk mengubah teks asli atau pengkodean pesan (*plaintext*) ke dalam teks rahasia (*chipertext*) disebut enkripsi. Pesan yang tidak terbaca disebut teks rahasia (*chipertext*). Proses kebalikan dari enkripsi disebut dekripsi. Dekripsi akan mengembalikan teks rahasia (*chipertext*) menjadi teks asli (*plaintext*). Kedua proses enkripsi dan dekripsi membutuhkan penggunaan sejumlah informasi rahasia, yang sering disebut kunci (*key*) [1,2].

Super enkripsi merupakan suatu konsep yang menggabungkan dua atau lebih teknik subtitusi dan teknik transposisi untuk mendapatkan algoritma yang lebih kuat. Pertama dilakukan enkripsi pesan menggunakan teknik subtitusi dan hasil teks-kode yang didapatkan dienkripsikan kembali menggunakan teknik transposisi [3,4].

Rail Fence cipher yang juga dikenal sebagai *zig-zag cipher* adalah salah satu kriptografi klasik transposisi. *Rail Fence cipher* menggunakan huruf pada *plaintext* dan mengubah posisi karakter *plaintext* menjadi bentuk diagonal ke

bawah dan ke atas dan membentuk jalur *zig-zag* sehingga menghasilkan *ciphertext* [5].

Sebagai contoh, melakukan enkripsi dengan pesan "RYAN APRILYADI" dengan menggunakan kunci *zig-zag* sebanyak 2. *Plaintext* dibentuk ke dalam pola *zig-zag* dalam dua baris. Kemudian *ciphertext* dapat dibaca dari baris pertama dan diikuti dengan baris-baris selanjutnya dengan hasil sebagai berikut.

Plaintext : RYAN APRILYADI
Kunci *Rail Fence* : 2

R		A				P		I		Y		D	
	Y		N		A		R		L		A		I

Ciphetext : RA PIYDYNARLAI

Sedangkan proses dekripsi, *ciphertext* dimasukkan ke dalam bentuk matrik dengan baris sesuai dengan jumlah nilai kunci dan kolom sesuai dengan jumlah karakter dari *ciphertext* tersebut, kemudian dibaca secara *zig-zag* sehingga menghasilkan *plaintext* kembali. Sebagai contoh melakukan dekripsi dengan pesan "FR ENNOEYFRAD" dengan menggunakan kunci *zig-zag* sebanyak 2 dengan hasil sebagai berikut.

Ciphertext : FR ENNOEYFRAD
Kunci *Rail Fence* : 2
Jumlah Karakter *Ciphertext* : 13

F		R				E		N		N		O
	E		Y		F		R		A		D	

Plaintext : FERY FERNANDO

Caesar *cipher* yang juga dikenal sebagai *shift cipher* merupakan salah satu kriptografi klasik subtitusi pertama. Caesar *cipher* digunakan oleh Julius Caesar untuk melakukan komunikasi kepada tentara pada garis depan. Agar pesan yang diberikan oleh Julius Caesar terlindungi kerahasian pesannya maka dilakukan pergeseran setiap huruf yang digunakan dalam pesan yang kemudian menjadi algoritma standar[1],

Sebagai contoh, melakukan enkripsi pesan "BRILIAN PUTRI CHRITIANI" dengan kunci Caesar *cipher* sebanyak 4 kali penggeseran. Setiap huruf dari *plaintext* diselaraskan dengan huruf sandi yang ada agar menghasilkan *ciphertext*. Dengan hasil sebagai berikut.

Plaintext : BRILIAN PUTRI CHRITIANI
Kunci Caesar *cipher* : 4

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 2, September 2022, pp. 740-753
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

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

Ciphertext : FVMPMER TYXVM GLVMWXMERM

Sedangkan proses dekripsi dengan Caesar *Cipher* sama saja dengan proses enkripsi, setiap huruf dari *chipertext* diselaraskan dengan huruf sandi yang ada agar menghasilkan *plaintext*, dengan contoh melakukan dekripsi pesan "YDNEOPEWJ ZSE LQPNW" dengan kunci Caesar *cipher* sebanyak 3 kali penggeseran dengan hasil sebagai berikut.

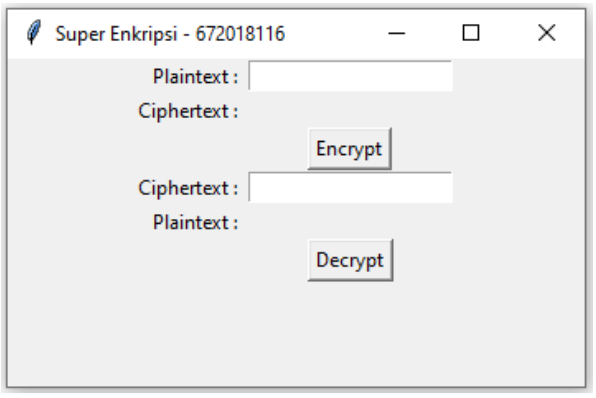
Ciphertext : YDNEOPEWJ ZSE LQPNW
Kunci Caesar *cipher* : 3

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

Plaintext : CHRISTIAN DWI PUTRA

3. HASIL DAN PEMBAHASAN

Aplikasi super enkripsi menggunakan metode *Rail Fence cipher* dan Caesar *cipher* terdiri dari dari dua proses yaitu proses enkripsi dan proses dekripsi. Implementasi super enkripsi pada penelitian ini hanya melakukan proses pengkodean pesan dan mengembalikan pengkodean pesan menjadi pesan biasa pada data teks. Hasil implementasi super enkripsi ini dijelaskan sebagai berikut.



Gambar 2. Aplikasi Super Enkripsi Menggunakan Metode *Rail Fence Cipher* dan Caesar *Cipher*

Adapun hasil implementasi super enkripsi yang akan dibahas adalah proses enkripsi dan proses dekripsi data teks. Untuk proses enkripsi super enkripsi dapat dilihat pada Kode Program 1, sedangkan untuk proses dekripsi super enkripsi dapat dilihat pada Kode Program 2.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 2, September 2022, pp. 740-753
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Kode Program 1. Perintah Untuk Melakukan Enkripsi Pada Data Teks

```
1   key1 = 4
2   rail = [['\n' for i in range(len(text))]
3             for j in range(key1)]
4
5   dir_down = False
6   row, col = 0, 0
7
8   for i in range(len(text)):
9    if (row == 0) or (row == key1 - 1):
10      dir_down = not dir_down
11
12   rail[row][col] = text[i]
13   col += 1
14
15   if dir_down:
16      row += 1
17   else:
18      row -= 1
19
20  txtc = ""
21  result = []
22  for i in range(key1):
23   for j in range(len(text)):
24      if rail[i][j] != '\n':
25         result.append(rail[i][j])
26         txtc = "" . join(result)
27  txt2 = txtc
28
29  key2 = 8
30  alpha = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
31  alpha1 = "abcdefghijklmnopqrstuvwxyz"
32  result = ""
33
34  for letter in txtc:
35   if letter in alpha:
36    letter_index = (alpha.find(letter) + key2) % len(alpha)
37    result = result + alpha[letter_index]
38   elif letter in alpha1:
39    letter_index = (alpha1.find(letter) + key2) % len(alpha1)
40    result = result + alpha1[letter_index]
41   else:
42    result = result + letter
43  return result
```

Kode Program 1 dapat dijelaskan sebagai berikut. Perintah pada baris 1-27 merupakan proses pengkodean pesan atau enkripsi dengan menggunakan metode *Rail Fence cipher* dengan memproses pesan biasa dalam bentuk *plaintext* dan menghasilkan *ciphertext* pertama. Perintah pada baris 29-43 merupakan proses enkripsi dengan menggunakan metode Caesar *cipher* dengan memproses *ciphertext* pertama dan menghasilkan *ciphertext* kedua yang merupakan hasil akhir *ciphertext* pada proses enkripsi implementasi super enkripsi ini.

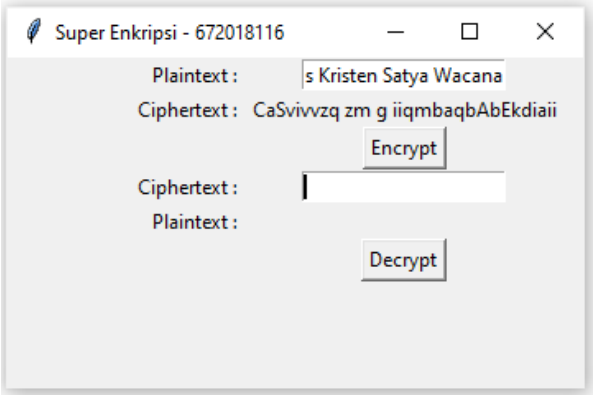
Kode Program 2. Perintah Untuk Melakukan Dekripsi Pada Data Teks

```
1   key4 = 4
2   key3 = 8
3   alpha = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
4   alpha1 = "abcdefghijklmnopqrstuvwxyz"
5   result = ""
6
```

```
7     for letter in txtd:
8       if letter in alpha:
9        letter_index = (alpha.find(letter) - key3) % len(alpha)
10       result = result + alpha[letter_index]
11
12      elif letter in alpha1:
13       letter_index = (alpha1.find(letter) - key3) % len(alpha1)
14       result = result + alpha1[letter_index]
15
16      else:
17       result = result + letter
18    x=result
19
20    rail = [['\n' for i in range(len(x))]
21              for j in range(key4)]
22
23    dir_down = None
24    row, col = 0, 0
25
26    for i in range(len(x)):
27       if row == 0:
28          dir_down = True
29       if row == key4 - 1:
30          dir_down = False
31
32       rail[row][col] = '*'
33       col += 1
34
35       if dir_down:
36          row += 1
37       else:
38          row -= 1
39
40    index = 0
41    for i in range(key4):
42       for j in range(len(x)):
43          if ((rail[i][j] == '*') and
44          (index < len(x))):
45             rail[i][j] = x[index]
46             index += 1
47
48    result = []
49    row, col = 0, 0
50    for i in range(len(x)):
51
52      if row == 0:
53         dir_down = True
54      if row == key4 - 1:
55         dir_down = False
56
57      if (rail[row][col] != '*'):
58         result.append(rail[row][col])
59         col += 1
60
61      if dir_down:
62         row += 1
63      else:
64         row -= 1
65    return("".join(result))
```

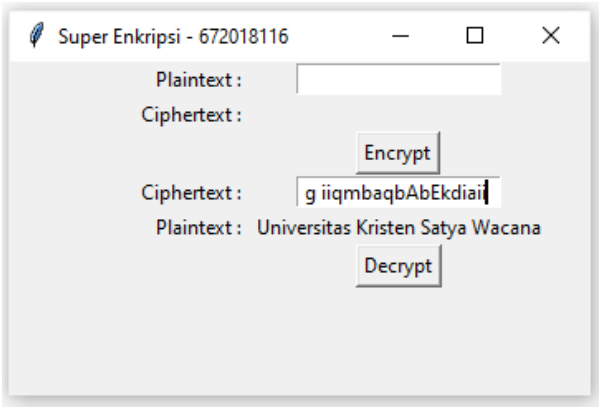
Kode Program 2 dapat dijelaskan sebagai berikut. Perintah Pada baris 1-19 merupakan proses mengembalikan pesan yang dikode atau dekripsi pesan dengan menggunakan metode Caesar *cipher* dengan memproses pesan dalam bentuk *ciphertext* 2 dan menghasilkan teks yang masih berbentuk

ciphertext 1. Proses dekripsi dilanjutkan pada baris 20-65 yang merupakan proses dekripsi dengan menggunakan metode *Rail Fence cipher* dengan memproses *ciphertext* 1 dan menghasilkan *plaintext* atau pesan biasa yang merupakan hasil akhir dari dekripsi pada implementasi super enkripsi ini.



Gambar 3. Antarmuka Proses Enkripsi

Gambar 3 merupakan tampilan antarmuka pada proses enkripsi. *User* memasukkan pesan yang ingin dienkripsikan pada *text box* yang tersedia. Selanjutnya memilih pada tombol "*Encrypt*" untuk melakukan proses enkripsi, selanjutnya hasil enkripsi akan ditampilkan.



Gambar 4. Antarmuka Proses Dekripsi

Gambar 4 merupakan tampilan antarmuka pada proses dekripsi. *User* memasukkan pesan yang ingin didekripsikan pada *text box* yang tersedia. Selanjutnya memilih pada tombol "*Decrypt*" untuk melakukan proses dekripsi, selanjutnya hasil dekripsi akan ditampilkan.

Super enkripsi dengan menggunakan metode *Rail Fence cipher* dan Caesar *cipher* ini diimplementasikan pada data pasien Klinik Eka Karigas dengan mengubah data yang masih berupa *plaintext* dan dikodekan menjadi bentuk *ciphertext* dengan hasil sebagai berikut.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 2, September 2022, pp. 740-753
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Tabel 1. Data Pasien Klinik Eka Karigas

Nomor	Hari, Tanggal	Nama Pasien	Kunjungan	Dokter
1	Kamis, 01 Oktober 2021	Ny. Tina Sopae	Rujukan	dr. Yenny Perinasari Sibot
2	Kamis, 01 Oktober 2021	Ny. Susan	Rawat Jalan	dr. Yenny Perinasari Sibot
3	Kamis, 01 Oktober 2021	Ny. Dwi Handayani	Rawat Jalan	dr. Yenny Perinasari Sibot
4	Sabtu, 03 Oktober 2021	Ny. Neno	Rujukan	dr. Yenny Perinasari Sibot
5	Sabtu, 03 Oktober 2021	Ny. Indah Permata	Rujukan	dr. Yenny Perinasari Sibot
6	Sabtu, 03 Oktober 2021	Ny. Dyan Kristi	Rawat Jalan	dr. Yenny Perinasari Sibot
7	Sabtu, 03 Oktober 2021	Ny. Dewi Purwanti	Rawat Jalan	dr. Yenny Perinasari Sibot
8	Senin, 05 Oktober 2021	Ny. Astriana	Rawat Jalan	dr. Jonathan Joentry
9	Rabu, 07 Oktober 2021	Ny. Sinta Rina	Rawat Jalan	dr. Jonathan Joentry
10	Kamis, 08 Oktober 2021	Ny. Franciska	Rawat Jalan	dr. Yenny Perinasari Sibot
11	Kamis, 08 Oktober 2021	Ny. Novia Rizka	Rawat Jalan	dr. Yenny Perinasari Sibot
12	Sabtu, 10 Oktober 2021	Ny. Elza Yolanda	Rujukan	dr. Yenny Perinasari Sibot
13	Sabtu, 10 Oktober 2021	Ny. Yamasidae	Rawat Jalan	dr. Yenny Perinasari Sibot
14	Rabu, 14 Oktober 2021	Ny. Karlina	Rujukan	dr. Jonathan Joentry
15	Sabtu, 17 Oktober 2021	Ny. Safitri	Rawat Jalan	dr. Yenny Perinasari Sibot
16	Senin, 19 Oktober 2021	Ny. Sherly Adeline	Rawat Jalan	dr. Jonathan Joentry
17	Selasa, 20 Oktober 2021	Ny. Immaculata	Rujukan	dr. Jonathan Joentry
18	Selasa, 20 Oktober 2021	Ny. Nurmaisyarah	Rujukan	dr. Jonathan Joentry
19	Selasa, 20 Oktober 2021	Ny. Ganang R	Rawat Jalan	dr. Jonathan Joentry
20	Rabu, 21 Oktober 2021	Ny. Rezita	Rawat Jalan	dr. Yenny Perinasari Sibot
21	Rabu, 21 Oktober 2021	Ny. Desi Paramita	Rawat Jalan	dr. Yenny Perinasari Sibot
22	Rabu, 21 Oktober 2021	Ny. Nita	Rujukan	dr. Yenny Perinasari Sibot
23	Kamis, 22 Oktober 2021	Ny. Trisna	Rawat Jalan	dr. Yenny Perinasari Sibot
24	Kamis, 22 Oktober 2021	Ny. Mutmainah	Rawat Jalan	dr. Yenny Perinasari Sibot
25	Rabu, 28 Oktober 2021	Ny. Monalisa	Rujukan	dr. Yenny Perinasari Sibot

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 2, September 2022, pp. 740-753
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Nomor	Hari, Tanggal	Nama Pasien	Kunjungan	Dokter
26	Rabu, 28 Oktober 2021	Ny. Fatimah	Rawat Jalan	dr. Yenny Perinasari Sibot
27	Jumat, 30 Oktober 2021	Ny. Maria Asmudi	Rawat Jalan	dr. Jonathan Joentry
28	Jumat, 30 Oktober 2021	Ny. Yeni Kartika	Rujukan	dr. Jonathan Joentry

Tabel 2 merupakan hasil enkripsi data pasien pada Klinik Eka Karigas dengan mengimplementasi skema super enkripsi dengan menggunakan metode *Rail Fence cipher* dan Metode Caesar *cipher*.

Tabel 2. Hasil Enkripsi Pada Data Pasien Klinik Eka Karigas

Nomor	Hari, Tanggal	Nama Pasien	Kunjungan	Dokter
1	S b2i,0sw 0ua1Wjz2q m1	Vvigqixm.B w A	Zvcirsc	lvzzwzmvmqiqjb.GgXva q iA
2	S b2i,0sw 0ua1Wjz2q m1	Vagci.Av	ZRi iebtvii	lvzzwzmvmqiqjb.GgXva q iA
3	S b2i,0sw 0ua1Wjz2q m1	Vqige lg.LPviq iv	ZRi iebtvii	lvzzwzmvmqiqjb.GgXva q iA
4	A b2i,0sw 0jc3Wjz2b m1	Vvgmw.V	Zvcirsc	lvzzwzmvmqiqjb.GgXva q iA
5	A b2i,0sw 0jc3Wjz2b m1	Vlzgvimu.QpXii b	Zvcirsc	lvzzwzmvmqiqjb.GgXva q iA
6	A b2i,0sw 0jc3Wjz2b m1	Viaggvqb.L zq S	ZRi iebtvii	lvzzwzmvmqiqjb.GgXva q iA
7	A b2i,0sw 0jc3Wjz2b m1	Veegmqzi.L cvq Xb	ZRi iebtvii	lvzzwzmvmqiqjb.GgXva q iA
8	A b2m,0sw 0vv5Wjz2q m1	Vbgazi.Iqv i	ZRi iebtvii	lv zzwivRbg.Rbiwv pm
9	Z0w0i 7bj22j, sm 1cWz	Vvvgqbqi.AiZ	ZRi iebtvii	lv zzwivRbg.Rbiwv pm
10	S b2i,0sw 0ua8Wjz2q m1	Viigzvs.Nka q	ZRi iebtvii	lvzzwzmvmqiqjb.GgXva q iA
11	S b2i,0sw 0ua8Wjz2q m1	Vdhgwqqs.ViZi	ZRi iebtvii	lvzzwzmvmqiqjb.GgXva q iA
12	A b2i,1sw 0jc0Wjz2b m1	Vhigtitv.M wl Gi	Zvcirsc	lvzzwzmvmqiqjb.GgXva q iA
13	A b2i,1sw 0jc0Wjz2b m1	Vumgiii.Gal q	ZRi iebtvii	lvzzwzmvmqiqjb.GgXva q iA
14	Z1w0i 4bj22j, sm 1cWz	Vzgit.Sqi v	Zvcirsc	lv zzwivRbg.Rbiwv pm
15	A b2i,1sw 0jc7Wjz2b m1	Vngiq.Abq z	ZRi iebtvii	lvzzwzmvmqiqjb.GgXva q iA
16	A b2m,1sw	VmlgpzImm.At tv	ZRi iebtvii	lv zzwivRbg.Rbiwv pm

Nomor	Hari, Tanggal	Nama Pasien	Kunjungan	Dokter
	0vv9Wjz2q m1	gq		
17	A,s mi Wbz2ta2 wm01i0j2	Vubguiii.Qkt c	Zvcirsc	lv zzwivRbg.Rbiwv pm
18	A,s mi Wbz2ta2 wm01i0j2	Vzigcugz.Viai qp	Zvcirsc	lv zzwivRbg.Rbiwv pm
19	A,s mi Wbz2ta2 wm01i0j2	VvgiiZ.Ov o	ZRi iebtvii	lv zzwivRbg.Rbiwv pm
20	Z2w0i 1bj22j, sm 1cWz	Vhgmq.Zb i	ZRi iebtvii	lvzzwzmvmqiqjb.GgXva q iA
21	Z2w0i 1bj22j, sm 1cWz	Vaigmqzu.L iqi Xb	ZRi iebtvii	lvzzwzmvmqiqjb.GgXva q iA
22	Z2w0i 1bj22j, sm 1cWz	Vbgqi.V	Zvcirsc	lvzzwzmvmqiqjb.GgXva q iA
23	S b2i,2sw 0ua2Wjz2q m1	Vqgza.Bv i	ZRi iebtvii	lvzzwzmvmqiqjb.GgXva q iA
24	S b2i,2sw 0ua2Wjz2q m1	Vbpgcui.Uiv q	ZRi iebtvii	lvzzwzmvmqiqjb.GgXva q iA
25	Z2w0i 8bj22j, sm 1cWz	Vvgwii.Uta q	Zvcirsc	lvzzwzmvmqiqjb.GgXva q iA
26	Z2w0i 8bj22j, sm 1cWz	Vbgiq.Nup i	ZRi iebtvii	lvzzwzmvmqiqjb.GgXva q iA
27	R b2c,3sw 0ub0Wjz2i m1	Vzugiqac.Uill q	ZRi iebtvii	lv zzwivRbg.Rbiwv pm
28	R b2c,3sw 0ub0Wjz2i m1	Vvbgmqzq.G is Si	Zvcirsc	lv zzwivRbg.Rbiwv pm

Hasil dari pengkodean data pasien Klinik Eka Karigas dapat didekripsikan kembali menggunakan super enkripsi dengan metode *Rail Fence cipher* dan Metode Caesar *cipher* agar menghasilkan data pasien kembali dalam bentuk *plaintext* dengan hasil ditunjukan pada Tabel 3.

Tabel 3. Hasil Dekripsi Pada Data Pasien Klinik Eka Karigas

Nomor	Hari, Tanggal	Nama Pasien	Kunjungan	Dokter
1	Kamis, 01 Oktober 2021	Ny. Tina Sopae	Rujukan	dr. Yenny Perinasari Sibot
2	Kamis, 01 Oktober 2021	Ny. Susan	Rawat Jalan	dr. Yenny Perinasari Sibot
3	Kamis, 01 Oktober 2021	Ny. Dwi Handayani	Rawat Jalan	dr. Yenny Perinasari Sibot
4	Sabtu, 03 Oktober 2021	Ny. Neno	Rujukan	dr. Yenny Perinasari Sibot
5	Sabtu, 03	Ny. Indah	Rujukan	dr. Yenny Perinasari

Nomor	Hari, Tanggal	Nama Pasien	Kunjungan	Dokter
	Oktober 2021	Permata		Sibot
6	Sabtu, 03 Oktober 2021	Ny. Dyan Kristi	Rawat Jalan	dr. Yenny Perinasari Sibot
7	Sabtu, 03 Oktober 2021	Ny. Dewi Purwanti	Rawat Jalan	dr. Yenny Perinasari Sibot
8	Senin, 05 Oktober 2021	Ny. Astriana	Rawat Jalan	dr. Jonathan Joentry
9	Rabu, 07 Oktober 2021	Ny. Sinta Rina	Rawat Jalan	dr. Jonathan Joentry
10	Kamis, 08 Oktober 2021	Ny. Franciska	Rawat Jalan	dr. Yenny Perinasari Sibot
11	Kamis, 08 Oktober 2021	Ny. Novia Rizka	Rawat Jalan	dr. Yenny Perinasari Sibot
12	Sabtu, 10 Oktober 2021	Ny. Elza Yolanda	Rujukan	dr. Yenny Perinasari Sibot
13	Sabtu, 10 Oktober 2021	Ny. Yamasidae	Rawat Jalan	dr. Yenny Perinasari Sibot
14	Rabu, 14 Oktober 2021	Ny. Karlina	Rujukan	dr. Jonathan Joentry
15	Sabtu, 17 Oktober 2021	Ny. Safitri	Rawat Jalan	dr. Yenny Perinasari Sibot
16	Senin, 19 Oktober 2021	Ny. Sherly Adeline	Rawat Jalan	dr. Jonathan Joentry
17	Selasa, 20 Oktober 2021	Ny. Immaculata	Rujukan	dr. Jonathan Joentry
18	Selasa, 20 Oktober 2021	Ny. Nurmaisyarah	Rujukan	dr. Jonathan Joentry
19	Selasa, 20 Oktober 2021	Ny. Ganang R	Rawat Jalan	dr. Jonathan Joentry
20	Rabu, 21 Oktober 2021	Ny. Rezita	Rawat Jalan	dr. Yenny Perinasari Sibot
21	Rabu, 21 Oktober 2021	Ny. Desi Paramita	Rawat Jalan	dr. Yenny Perinasari Sibot
22	Rabu, 21 Oktober 2021	Ny. Nita	Rujukan	dr. Yenny Perinasari Sibot
23	Kamis, 22 Oktober 2021	Ny. Trisna	Rawat Jalan	dr. Yenny Perinasari Sibot
24	Kamis, 22 Oktober 2021	Ny. Mutmainah	Rawat Jalan	dr. Yenny Perinasari Sibot
25	Rabu, 28 Oktober 2021	Ny. Monalisa	Rujukan	dr. Yenny Perinasari Sibot
26	Rabu, 28 Oktober 2021	Ny. Fatimah	Rawat Jalan	dr. Yenny Perinasari Sibot
27	Jumat, 30 Oktober 2021	Ny. Maria Asmudi	Rawat Jalan	dr. Jonathan Joentry
28	Jumat, 30 Oktober 2021	Ny. Yeni Kartika	Rujukan	dr. Jonathan Joentry

4. SIMPULAN

Berdasarkan hasil dari implementasi super enkripsi pada data pasien Klinik Eka Karigas, dapat disimpulkan bahwa: (1) Data pasien Klinik Eka

Karigas dapat diamankan menggunakan metode super enkripsi dengan menggunakan metode *Rail Fence cipher* dan Metode Caesar *cipher*. (2) Data yang telah dienkripsikan dapat didekripsikan kembali tanpa ada perubahan karakter sehingga isi pesan asli tidak mengalami perubahan. (3) Keamanan data menggunakan kriptografi klasik dirasa masih kurang aman dikarenakan hanya mengubah huruf yang ada dan mengubah susunan huruf yang ada. Saran untuk penelitian selanjutnya adalah: (1) Super enkripsi dengan menggunakan kriptografi klasik dapat digabungkan dengan kriptografi modern agar memberikan keamanan data yang lebih optimal. (2) Metode super enkripsi pada penelitian ini dapat menjadi media pembelajaran lebih lanjut agar menghasilkan keamanan data yang lebih baik lagi ke depannya.

DAFTAR PUSTAKA

[1]. Mukhtar, Harun, "Kriptografi Untuk Keamanan Data", Deepublish, Yogyakarta, 2018.
[2]. Priyono, Priyono, "Penerapan Algoritma Caesar Cipher dan Algoritma Vigenere Cipher Dalam Pengamanan Pesan Teks.", JURIKOM, 3.5, 2016.
[3]. Ariyus, Dony. "Pengantar Ilmu Kriptografi Teori." Analisis, dan Implementasi, Penerbit Andi, Yogyakarta, 2008.
[4]. El Hakim, Luqman, "Proses enkripsi dan dekripsi dengan menggunakan metode Super Enkripsi." Diss, Universitas Islam Negeri Maulana Malik Ibrahim, 2019.
[5]. Yusuf, Akhmad. "Implementasi Algoritma Rail Fence Cipher dan Least Significant Bit Untuk Pengamanan File Citra.", 2018.
[6]. Megantara, Rama Aria, and Fauzi Adi Rafrastara, "Super Enkripsi Teks Kriptografi Menggunakan Algoritma Hill Cipher Dan Transposisi Kolom.", 2019.
[7]. Kusumaningtyas, Juwita Artanti, "Analisa Algoritma Ciphers Transposition: Study Literature.", Multimatrix, 1.1, 2018.
[8]. Rachmawati, Dian, and Ade Candra. "Implementasi Kombinasi Caesar dan Affine Cipher untuk keamanan Data Teks." JEPIN (Jurnal Edukasi dan Penelitian Informatika), 1.2: 60-63, 2015.
[9]. Gurning, Rita Rio Arjumi, "Perancangan aplikasi pengamanan pesan dengan algoritma caesar chiper." Jurnal Pelita Informatika Budi Darma, 6, 2014.
[10]. Fadlan, M., Sinawati, S., Indriani, A., & Bintari, E. D., "Pengamanan Data Teks Melalui Perpaduan Algoritma Beaufort dan Caesar Cipher.", Jurnal Teknik Informatika 12.2: 149-158, 2019.