Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 2, September 2022, pp. 711-725
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Pengamanan Data Pasien Di UPT. Puskesmas Pujon Kalimantan Tengah Menggunakan Kriptografi Super Enkripsi

Lee Valdho Falensky[1*], Magdalena A. Ineke Pakereng[2]
[1,2]Jurusan Teknik Informatika, FTI UKSW, Salatiga, Indonesia
e-mail : [1]672018377@student.uksw.edu ,[2]ineke.pakereng@uksw.edu

Abstract

Along with the development of information and communication technology nowaday, data security in exchanging information is increasingly important. One technique that can be used to secure the data is super encryption cryptography. Super encryption is a cryptographic technique that combines two or more algorithms. In this research, the encryption decryption process data text of patient biodata of Technical Implementation Unit Pujon Health Center Central Kalimantan was conducted using three cryptography, namely Columnar Transposition, Vigenere Cipher and Monoalphabetic. The result of this research is that the super encryption that has been built can encode (encrypt) and return (decrypt) messages in text. data text of patient biodata of Technical Implementation Unit Pujon Health Center Central Kalimantan tested, before decryption encryption and after decryption encryption did not change the number of characters. The number of characters does not affect the speed of the process because the number of characters used can produce the same processing speed.

Keywords*: Super Ecrytion, Cryptography, Encryption, Decryption*

Abstrak

Seiring berkembangnya teknologi informasi dan komunikasi pada jaman sekarang, keamanan data dalam bertukar informasi semakin penting dilakukan. Salah satu teknik yang dapat digunakan untuk pengamanan data tersebut adalah kriptografi super enkripsi. Super enkripsi merupakan salah satu teknik kriptografi yang menggabungkan dua algoritma atau lebih. Pada penelitian ini, proses enkripsi dekripsi data text biodata pasien UPT. Puskesmas Pujon Kalimantan Tengah dilakukan menggunakan tiga kriptografi yaitu Transposisi Columnar, Vigenere Cipher dan Substitusi Monoalphabetic. Hasil dari penelitian ini adalah super enkripsi yang telah dibangun dapat melakukan pengkodean (enkripsi) dan mengembalikan (dekripsi) pesan dalam format text. Data text biodata pasien UPT. Puskesmas Pujon Kalimantan Tengah yang diuji, sebelum dienkripsi dekripsi dan setelah dienkripsi dekripsi tidak mengalami perubahan terhadap jumlah karakternya. Jumlah karakter tidak mempengaruhi kecepatan proses karena banyak sedikitnya jumlah karakter yang digunakan dapat menghasilkan kecepatan proses yang sama.

Kata kunci*: Super Enkripsi, Kriptografi, Enkripsi, Dekripsi*

1. PENDAHULUAN

Melakukan kerahasiaan dalam sebuah pertukaran data adalah hal yang sangat penting dalam komunikasi data, baik untuk tujuan keamanan bersama, maupun untuk keamanan individu. Bagi yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan akan selalu berusaha untuk mengamankan informasi data tersebut. Perlindungan terhadap kerahasiaan data pun akan meningkat, salah satu dengan cara penyandian data atau enkripsi.

Super Enkripsi merupakan salah satu kriptografi berbasis karakter yang menggabungkan metode substitusi dan transposisi. Hal tersebut dilakukan dengan tujuan untuk memperoleh kriptografi yang lebih kuat daripada hanya menggunakan satu metode saja sehingga tidak mudah untuk dipecahkan. Secara teori penggabungan dua proses tersebut dapat menghilangkan hubungan satu ke-satu antara *plaintext* dan *ciphertext*. Metode ini juga dapat menahan serangan kriptanalisis analisis frekuensi[1].

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan atau data yang diperoleh dengan men-nyandikannya menjadi pesan yang tidak mempunyai makna. Kriptografi dapat digunakan untuk men-nyamarkan informasi yang bersifat rahasia dari orang atau pihak yang tidak berhak membacanya. Dalam kriptografi terdapat dua proses penyandian, yaitu enkripsi dan dekripsi[2].

Enkripsi adalah sebuah proses penyandian yang mengubah *text*-asli atau pesan yang dapat dimengerti *(plaintext)* menjadi *text*-kode atau pesan yang tidak dapat dimengerti *(ciphertext)*. Dekripsi adalah sebuah proses pembalikan yang mengubah *text*-kode atau pesan yang tidak dapat dimengerti *(ciphertext)* menjadi sebuah *text*-asli atau pesan yang dapat dimengerti *(plaintext)*[2].

Masalah keamanan data merupakan salah satu aspek penting dari sebuah sistem informasi. Salah satu masalah keamanan data yang kurang mendapat perhatian adalah keamanan data pada sistem pasien Unit Pelaksana Teknis Pusat Kesehatan Masyarakat (UPT Puskesmas) Pujon Kalimantan Tengah, data yang dimaksud ini hanya berfokus pada biodata pasien UPT. Puskesmas Pujon Kalimantan Tengah saja. Penelitian ini bisa dijadikan sebagai sebuah bahan untuk melakukan pengamanan terhadap data-data yang ada pada sistem pasien UPT. Puskesmas Pujon Kalimantan Tengah dengan menggunakan metode pengamanan yang berbeda yaitu dengan menggunakan Kriptografi Super Enkripsi.

2. METODOLOGI PENELITIAN

2.1. Tinjauan Pustaka

Penelitian yang berjudul Pengamanan Data Informasi Menggunakan Kriptografi Klasik, membahas tentang proses enkripsi dan dekripsi menggunakan kriptografi klasik sehingga data informasi dapat diamankan dengan baik[4].

Penelitian yang berjudul Pengamanan Data Rekam Medis Pasien Menggunakan Kriptografi *Vigenere Cipher*, membahas tentang masalah keamanan data yang merupakan salah satu aspek dari sebuah sistem informasi. Sehingga peneliti mendapatkan salah satu masalah keamanan data yang kurang mendapat perhatian adalah keamanan data pada aplikasi rekam medis pasien, dan peneliti menggunakan *vigenere cipher* untuk mengamankan data rekam medis pasien[3].

Penelitian yang berjudul Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, isi File Dokumen, Dan File Dokumen Menggunakan

Algoritma *Advance Encryption Standard*, membahas tentang membuat sebuah sistem keamanan data dengan mengimplementasikan kriptografi pada pesan teks, isi file dokumen, dan file dokumen dengan melakukan perhitungan algoritma *Advanced Encryption Standard(AES)*. *AES* merupakan algoritma *cryptographic* yang dapat digunakan untuk mengamankan data dimana algoritmanya adalah blok *chipertext* simetrik yang dapat mengenkripsi *(encipher)* dan dekripsi *(decipher)* informasi[5].

Penelitian yang berjudul Penerapan Teknik Kriptografi *Stream-Cipher* Untuk Pengamanan Basis Data, mengambil contoh database nasabah suatu sistem informasi perbankan, setiap entitas nasabah mempunyai berbagai atribut yang melekat, antara lain nama, alamat, umur dan nomor pin. Atribut nama, alamat dan umur adalah atribut yang bersifat umum yang dapat diketahui semua orang. Tetapi atribut nomor pin setiap nasabah merupakan informasi yang bersifat rahasia[6].

Penelitian yang berjudul Implementasi *S-Box AES* Dan Komparasi Rancangan *Permutation Box (P-Box)* Dalam Skema Super Enkripsi bertujuan untuk menciptakan kriptografi baru agar menjadi alternatif dalam mengamankan data sehingga kerahasiaan data terjaga dengan lebih baik[7].

Penelitian yang berjudul Perancangan Super Enkripsi Menggunakan Metode Substitusi *S-Box AES* dan Metode Transposisi dengan Pola *Vertikal-Horizontal* ini adalah untuk merancang algoritma kriptografi menggunakan skema super enkripsi dengan menggunakan transposisi *vertikal* dan *horizontal* dan juga *s-box AES* untuk melakukan proses substitusi. Penggunaan *s-box AES*, karena kriptografi ini menjadi standar pengamanan informasi yang ditetapkan oleh *National Security Agency (NSA)*[1].

Penelitian yang berjudul Pengamanan File Dokumen Menggunakan Kombinasi Metode Substitusi Dan *Vigenere Cipher*. Dalam penelitian ini pengamanan data menggunakan penggabungan dua metode kriptografi, dapat menghasilkan keamanan data yang lebih maksimal untuk *proteksi* data. Untuk perancangan sistem dalam penelitian ini menggunakan metode *System Development Life Cycle (SDLC) Waterfall*. Dengan menggunakan dua metode kriptografi sebagai pengamanan data, maka diharapkan hal ini dapat menjadi solusi terhadap serangan kriptanalisis. Berdasarkan hal ini maka penelitian ini akan melakukan pengamanan file dokumen menggunakan kombinasi metode subtitusi dan *vigenere cipher*[2].

Transposisi *Columnar, plaintext* akan ditulis dalam baris dengan panjang tertentu, kemudian dibaca kembali dari kolom ke kolom. Pembacaan perkolomnya berdasarkan urutan yang acak. Panjang baris dan permutasi kolomnya biasanya didefinisikan oleh sebuah kata kunci. Sebagai contoh kata COLUMN, maka urutanya akan menjadi (1 5 2 6 3 4). Pada Transposisi *Columnar* pada umunya semua area kosong diisi dengan nilai *dummy.*Sedangkan pada beberapa Transposisi *Columnar* yang lain, area kosong dibiarkan tetap kosong[8].

Contoh proses enkripsi pesan pada kriptografi Transposisi *Columnar* dapat dilihat pada Gambar 1. Kunci yang digunakan adalah tiga. Jumlah

kolom dibentuk sesuai kunci yang digunakan pada proses enkripsi, jumlah barisnya disesuaikan dengan panjang karakter dari *plaintext*. contoh *plaintext* yang digunakan "FALENSKY". *Plaintext* ditulis secara *horizontal* dengan lebar tetap sesuai dengan kunci yang digunakan.

Plaintext : FALENSKY

Enkripsi :

F	A	L
E	N	S
K	Y	

Gambar 1. Contoh Proses Enkripsi Transposisi Columnar

Gambar 1 merupakan proses enkripsi Transposisi *Columnar*, maka *ciphertext*-nya dapat dibaca secara *vertikal* yaitu menjadi "FEKANYLS". Setelah hasil dari proses enkripsi Transposisi *Columnar* didapatkan. Selanjutnya dilakukan contoh proses dekripsi pesan yang dilakukan dengan membagi panjang *ciphertext* dengan kunci yang ditentukan seperti pada waktu proses enkripsi. Proses dekripsi untuk *ciphertext* "FEKANYLS" yang merupakan hasil dari proses enkripsi sebelumnya dapat dilihat pada Gambar 2. Hasil dekripsi yang diperoleh dengan membaca setiap kolom pada Gambar 2 adalah "FALENSKY".

Ciphertext : FEKANYLS

Enkripsi :

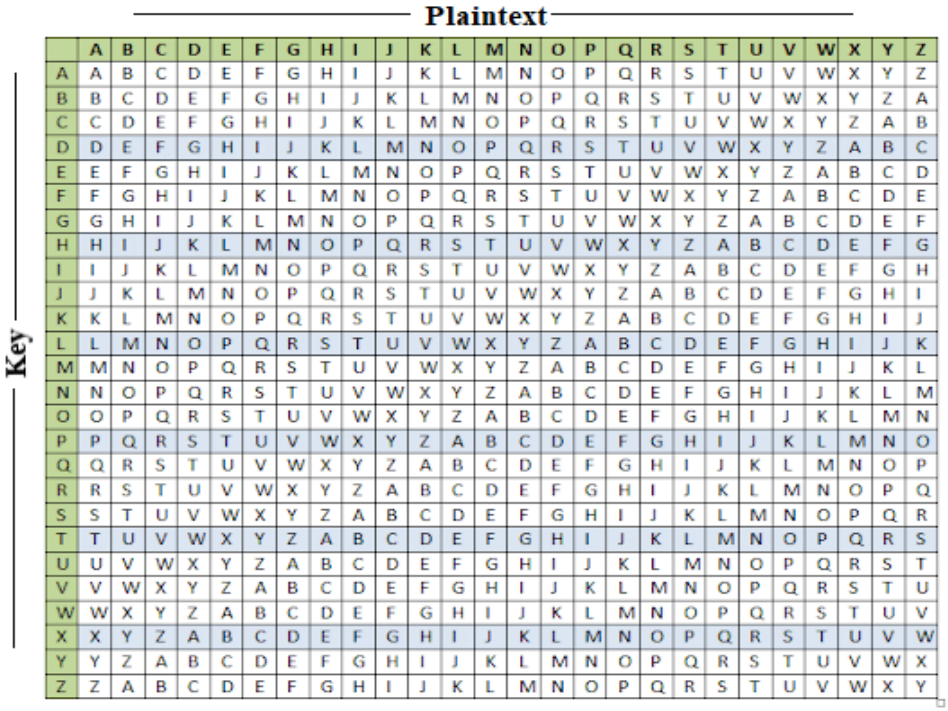
F	E	K
A	N	Y
L	S	

Gambar 2. Contoh Proses Dekripsi Transposisi Columnar

Vigenere Cipher adalah salah satu dari jenis algoritma klasik yang menggunakan substitusi abjad majemuk. pada *Vigenere cipher*, pergeseran karakternya ditentukan oleh karakter yang ada pada kata kunci dan kata ini selalu diulang. Akibatnya, karakter yang sama pada *plaintext* boleh jadi memiliki karakter yang berbeda pada *ciphertext-nya*. Karena hal ini lah, *Vigenere cipher* merupakan *cipher* substitusi abjad-majemuk[4].

Rumus enkripsi *cipher vigenere* adalah Ci = (Pi + Ki) – 26 kalau hasil penjumlahan Pi dan Ki lebih dari 26, lalu untuk rumus dekripsi *cipher vigenere* adalah Pi = (Ci – Ki) + 26 kalau hasil pengurangan Ci dengan Ki minus. Ci = nilai desimal karakter *ciphertext* ke-I, Pi = nilai desimal karakter *plaintext* ke-I, Ki = nilai desimal karakter kunci ke-I. Nilai desimal karakter adalah A=0 B=1 C=2 ... Z=25. Sebagai contoh, jika *plaintext* adalah STIKOMBALI dan kunci adalah KAMPUS maka proses enkripsi yang terjadi adalah *Plaintext*: STIKOMBALI, *Key*: KAMPUSKAMP, *Ciphertext*: CTUZIELAXX.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 2, September 2022, pp. 711-725
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti



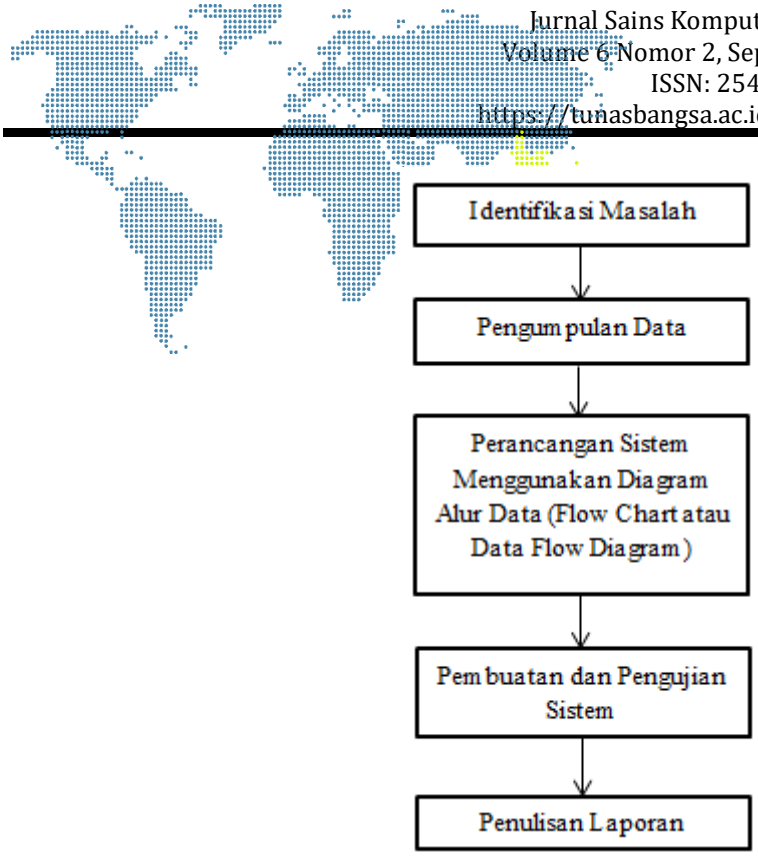
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Gambar 3. Vigere Cipher

Substitusi *Monoalphabetic* adalah teknik kriptografi substitusi yang mengganti setiap karakter *plaintext*-nya menjadi karakter lain pada *chipertext*. Huruf yang sama pada *plaintext*, akan memiliki huruf pengganti yang sama pula pada *chipertext*-nya. Seperti pada contoh *Caesar chiper*, huruf A pada *plaintext* akan selalu diganti dengan huruf D pada *chipertext*. Metoda lain pada *monoalphabetic* chiper adalah *ROT*13 yang mengganti setiap huruf pada *plaintext*-nya dengan huruf yang letaknya 13 posisi darinya. Oleh karena itu hubungan antara *plaintext* dengan *chipertext*-nya mudah diterka, karena huruf yang sering muncul pada *palintext* akan sering muncul pula pada *chipertext*. Substitusi *Monoalphabetic* mengenkripsi setiap karakter dalam pesan, sehingga memiliki Kunci26!. Algoritma telah dikenal sehingga mudah didekripsi tanpa kunci menggunakan metode terkaan. Teknik substitusi *monoalphabetic* juga tidak dapat menyembunyikan hubungan antara *plaintext* dengan *ciphertext*. Huruf yang sama di-enkripsi menjadi huruf *ciphertext* yang sama, sehingga huruf yang sering muncul di dalam *plaintext*, sering muncul pula di dalam *ciphertext*-nya[9].

2.2. Metode Penelitian

Tahapan yang dilakukan dalam penelitian ini, terdiri dari 5 (lima) tahapan, yaitu: (1) Identifikasi Masalah, (2) Pengumpulan Data, (3) Perancangan Algoritma, (4) Pembuatan dan Pengujian Algoritma, dan (5) Penulisan Laporan.

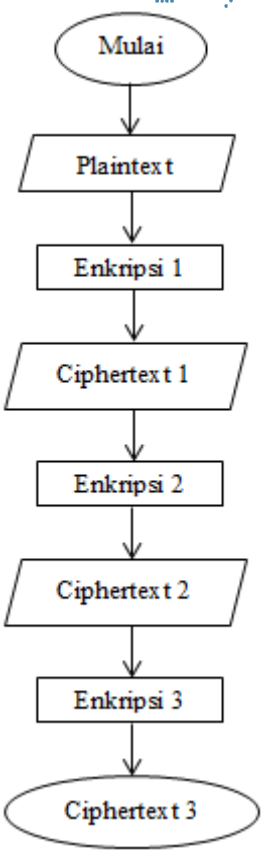


Gambar 4. Tahapan Penelitian

Langkah pertama identifikasi masalah dilakukan dengan meneliti masalah yang kaitannya dengan kriptografi Super Enkripsi. Selain itu, menentukan batasan masalah dalam penelitian ini yaitu; Kriptografi yang digunakan hanya Transposisi *Columnar*, *Vigenere Cipher* dan Substitusi *Monoalphabetic*. Data hanya berisi biodata pasien tidak termasuk jenis penyakit atau obat-obatan dan lainya. Langkah kedua pengumpulan data, tahapan pertama adalah observasi yang dimana peneliti melakukan survei dan pengamatan langsung di UPT. Puskesmas Pujon Kalimantan Tengah tersebut, untuk memperoleh data-data primer beserta informasinya. Lalu tahap yang kedua adalah wawancara yang tujuannya adalah untuk meningkatkan keakuratan data dengan cara peneliti mewawancarai pada bagian staff untuk mengetahui proses yang berhubungan dengan data dari pasien UPT. Puskesmas Pujon Kalimantan Tengah. Langkah ketiga perancangan kriptografi super enkripsi. Membuat rancangan untuk proses enkripsi dan dekripsi *plaintext* dengan kriptografi yang digunakan yaitu Transposisi *Columnar*, *Vigenere Cipher* dan Substitusi *Monoalphabetic*. Tahapan perancangan secara umum dapat dilihat Gambar 5 dan Gambar 6. Langkah keempat membuat aplikasi kriptografi super enkripsi dan menguji hasil pembuatan terhadap data yang telah dikumpulkan. Langkah kelima atau yang terakhir adalah penulisan laporan yang berisi hasil penelitian yang selesai dilakukan kemudian ditulis ke dalam artikel ilmiah.

Penjelasan tahapan perancangan sistem (Enkripsi) adalah sebagai berikut; *plaintext* = data pasien UPT. Puskesmas Pujon Kalimantan Tengah, enkripsi Transposisi *Columnar* = enkripsi 1, hasil enkripsi Transposisi

Columnar = *ciphertext* 1, enkripsi *Vigenere Cipher* = enkripsi 2, hasil enkripsi *Vigenere Cipher* = *ciphertext* 2, enkripsi Substitusi *Monoalphabetic* = enkripsi 3, hasil enkripsi Substitusi *Monoalphabetic* = *ciphertext* 3.



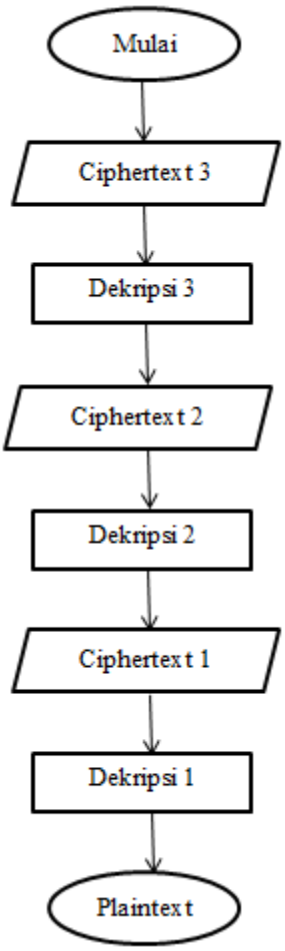
Gambar 5. Flowchart Perancangan Sistem (Enkripsi)

Berdasarkan rancangan secara umum yang telah dilihat pada Gambar 5. Proses enkripsi akan dibuat dengan cara mengolah *plaintext* yang merupakan data *text* pasien UPT. Puskesmas Pujon Kalimantan Tengah menggunakan kriptografi yang pertama yaitu kriptografi Transposisi *Columnar*, hasil enkripsi dari kriptografi Transposisi *Columnar* adalah berupa *ciphertext*. Selanjutnya hasil enkripsi dari Transposisi *Columnar* akan dienkripsikan kembali menggunakan kriptografi *Vigenere Cipher*. Setelah hasil enkripsi yang didapat dari *Vigenere Cipher* telah didapatkan maka dilakukanlah enkripsi pada kriptografi yang terakhir yaitu Substitusi *Monoalphabetic*. Hasil dari enkripsi Substitusi *Monoalphabetic* inilah yang merupakan hasil akhir dari super enkripsi yang saya rancang.

Penjelasan tahapan perancangan sistem (Dekripsi) adalah sebagai berikut; *ciphertext 3* = hasil super enkripsi, dekripsi Substitusi *Monoalphabetic* = dekripsi 3, hasil dekripsi Substitusi *Monoalphabetic* = *ciphertext* 2, dekripsi *Vigenere Cipher* = dekripsi 2, hasil dekripsi *Vigenere*

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 2, September 2022, pp. 711-725
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Cipher = *ciphertext* 1, dekripsi Transposisi *Columnar* = dekripsi 1, hasil dekripsi Transposisi *Columnar* = *plaintext*.



Gambar 6. Flowchart Perancangan Sistem (Dekripsi)

Selanjutnya pada Gambar 6. proses dekripsi akan dibuat dengan cara mengolah hasil enkripsi dengan kriptografi super enkripsi yang telah didapat. Lalu hasil enkripsi dari super enkripsi tersebut akan didekripsikan dengan cara membalikkan metode yang digunakan pada proses enkripsi. Hasil enkripsi dari super enkripsi akan didekripsikan menggunakan kriptografi Substitusi *Monoalphabetic* yang menghasilkan *ciphertext* 2. Selanjutnya hasil dari dekripsi Substitusi *Monoalphabetic* didekripsikan kembali menggunakan kriptografi *Vigenere Cipher* yang menghasilkan *ciphertext* 1. Selanjutnya hasil dari dekripsi *Vigenere Cipher* akan didekripsikan kembali menggunakan kriptografi Transposisi *Columnar* yang menghasilkan *plaintext* dari data *text* pasien UPT. Puskesmas Pujon Kalimantan Tengah.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 2, September 2022, pp. 711-725
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

3. HASIL DAN PEMBAHASAN

Berikut merupakan kode program menggunakan bahasa pemograman *python* yang akan digunakan dalam pembuatan aplikasi super enkripsi pada penelitian ini. Pembuatan aplikasi super enkripsi dalam penelitian ini hanya melakukan proses enkripsi dan dekripsi pada data *text* biodata pasien UPT. Puskesmas Pujon Kalimantan Tengah dan akan dijelaskan sebagai berikut.

Kode Program 1. Perintah untuk Proses Enkripsi pada Pembuatan Super Enkripsi

```
1.  def encrypt(msg):
2.    key = "HACK" #columnar
3.    cipher = ""
4.
5.    k_indx = 0
6.
7.    msg_len = float(len(msg))
8.    msg_lst = list(msg)
9.    key_lst = sorted(list(key))
10.
11.   col = len(key)
12.
13.   row = int(math.ceil(msg_len / col))
14.
15.   fill_null = int((row * col) - msg_len)
16.   msg_lst.extend('_' * fill_null)
17.
18.   matrix = [msg_lst[i: i + col]
19.                for i in range(0, len(msg_lst), col)]
20.
21.   for _ in range(col):
22.         curr_idx = key.index(key_lst[k_indx])
23.         cipher += ''.join([row[curr_idx]
24.                                       for row in matrix])
25.         k_indx += 1
26.
27.   keyword = "kunci" #vigenere
28.   keyword = list(keyword)
29.   if len(cipher) == len(keyword):
30.     return(keyword)
31.   else:
32.     for i in range(len(cipher) -len(keyword)):
33.       keyword.append(keyword[i % len(keyword)])
34.   keyv = "" . join(keyword)
35.
36.   string = cipher
37.   string = string.upper()
38.   encrypt_text = []
```

```
    for i in range(len(string)):
      x = (ord(string[i]) +ord(keyv[i])) % 26
      x += ord('A')
      encrypt_text.append(chr(x))
    cipher2 = "" . join(encrypt_text)

    keym = "53124" #monoalphabetic
    if keym.isupper():
      keym = ord(keym) - 65
    elif key.islower():
      keym = ord(keym) - 97
    else:
      keym = int(keym)

    cipher3 = ""
    for i in cipher2:
      if i.isupper():
        cipher3 += chr((ord(i) + keym - 65) % 26 + 65)
      elif i.islower():
        cipher3 += chr((ord(i) + keym - 97) % 26 + 97)
      else:
        cipher3+=" "

    return cipher3
```

Pada Kode Program 1 terdapat tiga kriptografi yang digunakan yaitu Transposisi *Columnar*, *Vigenere Cipher* dan Substitusi *Monoalphabetic.* ketiga kriptografi tersebut digabungkan dalam satu fungsi; *def encrypt(msg):* yang akan melakukan proses enkripsi secara berurutan. Pada baris 2 hingga baris 26 melakukan proses enkripsi Transposisi *Columnar* yang merupakan Enkripsi 1 dan menghasilkan *Ciphertext* 1. Pada baris 27 hingga baris 44 melakukan proses Enkripsi 2 yaitu *Vigenere Cipher* dan menghasilkan *Ciphertext* 2. Pada baris 45 hingga 62 melakukan proses Enkripsi 3 yaitu Substitusi *Monoalphabetic* dan menghasilkan *Ciphertext* 3 yang merupakan hasil akhir dari proses enkripsi pada pembuatan super enkripsi ini.

Kode Program 2. Perintah untuk Proses Dekripsi pada Pembuatan Super Enkripsi

```
def decrypt(cipher):
  keym = "53124" #monoalphabetic
  if keym.isupper():
    keym = ord(keym) - 65
  elif keym.islower():
    keym = ord(keym) - 97
  else:
    keym = int(keym)

  plain1 = ""
  for i in cipher:
    if i.isupper():
      plain1 += chr((ord(i) - keym - 65) % 26 + 65)
    elif i.islower():
      plain1 += chr((ord(i) - keym - 97) % 26 + 97)
    else:
      plain1+=" "
```

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 6 Nomor 2, September 2022, pp. 711-725
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

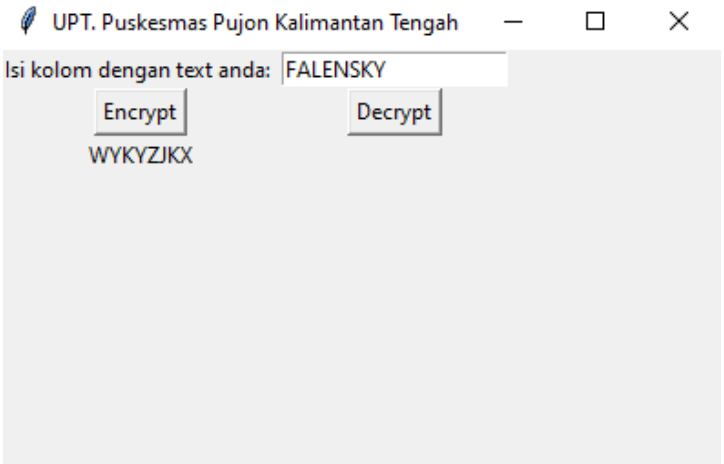
```
18.
19.    keyword = "kunci" #vigenere
20.    keyword = list(keyword)
21.    if len(cipher) == len(keyword):
22.      return(keyword)
23.    else:
24.      for i in range(len(cipher) -len(keyword)):
25.        keyword.append(keyword[i % len(keyword)])
26.    keyv = "" . join(keyword)
27.
28.    plain1 = plain1.upper()
29.    orig_text = []
30.    for i in range(len(plain1)):
31.      x = (ord(plain1[i]) -ord(keyv[i]) + 26) % 26
32.      x += ord('A')
33.      orig_text.append(chr(x))
34.    plain2 = "" . join(orig_text)
35.
36.    key = "HACK" #columnar
37.    msg = ""
38.
39.    k_indx = 0
40.
41.    msg_indx = 0
42.    msg_len = float(len(plain2))
43.    msg_lst = list(plain2)
44.
45.    col = len(key)
46.
47.    row = int(math.ceil(msg_len / col))
48.
49.    key_lst = sorted(list(key))
50.
51.    dec_cipher = []
52.    for _ in range(row):
53.          dec_cipher += [[None] * col]
54.
55.    for _ in range(col):
56.          curr_idx = key.index(key_lst[k_indx])
57.
58.          for j in range(row):
59.                  dec_cipher[j][curr_idx] = msg_lst[msg_indx]
60.                  msg_indx += 1
61.          k_indx += 1
62.
63.    try:
64.          msg = ''.join(sum(dec_cipher, []))
65.    except TypeError:
66.          raise TypeError("This program cannot",
67.                                        "handle repeating words.")
68.
69.    null_count = msg.count('_')
70.
71.    if null_count > 0:
72.          return msg[: -null_count]
73.
74.    return msg
```

Kode Program 2 merupakan proses dekripsi dimana kriptografi yang digunakan pada proses enkripsi akan di proses terbalik pada proses dekripsi ini. Pada baris 2 hingga 18 melakukan proses dekripsi Substitusi *Monoalphabetic* yang merupakan Dekripsi 3 dan menghasilkan *Ciphertext* 2. Pada baris 19 hingga 35 melakukan proses Dekripsi 2 yaitu *Vigenere Cipher*

dan menghasilkan *Ciphertext* 1. Pada baris 36 hingga 74 melakukan proses Dekripsi 1 yaitu Transposisi *Columnar* dan menghasilkan *Plaintext* yang merupakan hasil akhir dari proses dekripsi pada pembuatan super enkripsi ini.

Gambar 7. Hasil Kode Program Saat Dijalankan

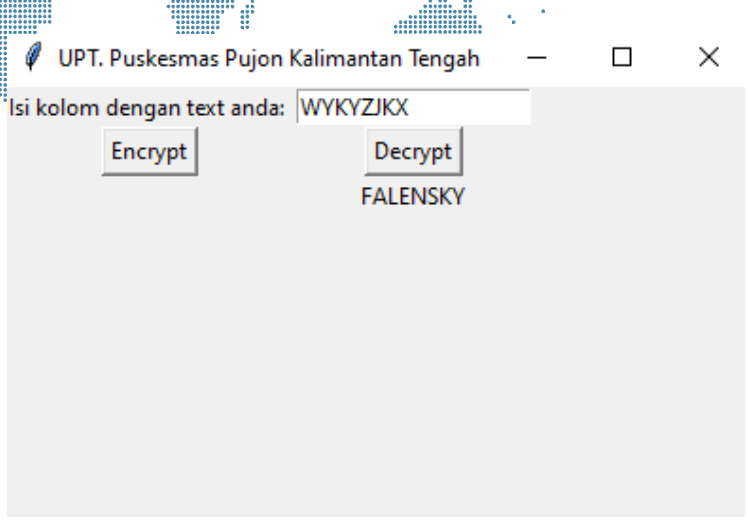
Gambar 7 merupakan hasil kode program ketika dijalankan, proses nya adalah *plaintext* yang diisi dengan *text* FALENSKY di enkripsi dan menghasilkan *ciphertext* WYKYZJKX. Hasil dari enkripsi yang didapat selanjutnya didekripsikan dan mendapatkan hasil *plaintext* yang telah diisi diawal yaitu *text* FALENSKY.



Gambar 8. Antar Muka untuk Proses Enkripsi pada Aplikasi Super Enkripsi

Gambar 8 merupakan tampilan antar muka untuk proses enkripsi pada pembuatan aplikasi super enkripsi ini. Dimana *user* akan memasukkan data pasien UPT. Puskesmas Pujon Kalimantan Tengah yang berupa *text*. Selanjutnya seperti pada contoh Gambar 8 *user* memasukkan *plaintext* yang

berisi *text* FALENSKY dan ketika *button Encrypt* dipilih maka hasil dari enkripsinya adalah berupa *ciphertext* yang berisi *text* WYKYZJKX.



Gambar 9. Antar Muka untuk Proses Dekripsi pada Aplikasi Super Enkripsi

Gambar 9 merupakan tampilan antar muka untuk proses dekripsi pada pembuatan aplikasi super enkripsi ini. Dimana *user* akan memasukkan hasil akhir dari proses enkripsi. Selanjutnya seperti pada contoh Gambar 9 *user* memasukkan *ciphertext* yang didapat dari hasil akhir proses enkripsi pada kolom *text* yang tersedia dan ketika *button Decrypt* dipilih maka *ciphertext* tersebut akan di proses dan menghasilkan hasil akhir yang berupa *plaintext* dari data *text* pasien UPT. Puskesmas Pujon Kalimantan Tengah yaitu FALENSKY.

Pada pembuatan super enkripsi yang telah dibuat dengan menggunakan kriptografi Transposisi *Columnar*, *Vigenere Cipher* dan Substitusi *Monoalphabetic* maka akan dilakukan pengujian terhadap data yang telah diperoleh. Yaitu pengujian terhadap data *text* biodata pasien UPT. Puskesmas Pujon Kalimantan Tengah dengan hasil sebagai berikut.

Tabel 1. Hasil Pengujian Super Enkripsi

Data Pasien UPT. Puskesmas Pujon *(Plaintext)*	**Hasil Akhir Proses Enkripsi *(Ciphertext)***	**Hasil Akhir Proses Dekripsi *(Plaintext)***	**Waktu Enkripsi dan Dekripsi (S)**
WIJANOTO	EUIHQJGN	WIJANOTO	10
DESI	AYCW	DESI	8
AERIELLYBELVANIA	ARDBLHRHOYXGHMPW	AERIELLYBELVANIA	8
TIMOTIUS	EOLINPUR	TIMOTIUS	7
ALIFMUHAMMAD	HALWBWGLAZWJ	ALIFMUHAMMAD	8
KUSMONOE	QTRCEKSD	KUSMONOE	13
UDUN	ZATB	UDUN	10
ALDISONA	HUCBUOOZ	ALDISONA	7
KURNADIE	QJQWEWTD	KURNADIE	9
EDISETYOBUDI	ZZTWSZKDPMKO	EDISETYOBUDI	8
ADRIANBUNTUR	ZTSFVQGZBCQX	ADRIANBUNTUR	8
SUDARLIN	QRCWMNGM	SUDARLIN	8
PRIYANTO	NTHHJWEN	PRIYANTO	7

Data Pasien UPT. Puskesmas Pujon *(Plaintext)*	Hasil Akhir Proses Enkripsi *(Ciphertext)*	Hasil Akhir Proses Dekripsi *(Plaintext)*	Waktu Enkripsi dan Dekripsi (S)
ISABELLA	ORZZCAHZ	ISABELLA	7
FRANSISKUSJELINO	NORWUOPMTMQRMYYK	FRANSISKUSJELINO	10
EDIYOARDREYNALDO	ZGDZCNECSINGXRHK	EDIYOARDREYNALDO	11
SURIYATI	QGQHMUOH	SURIYATI	9
RUSMIASI	QGRGLESH	RUSMIASI	7
THOMSONMEDIANTON	DUCHIJONHMATLAUJ	THOMSONMEDIANTON	8
KURNIADI	QGQREETH	KURNIADI	8
FIOJERIKIOSO	EXNCCOLDWDGU	FIOJERIKIOSO	8
SARUTOMO	WUQAMPAN	SARUTOMO	7
FENDISAPUTRA	AYSBUNLHIXLG	FENDISAPUTRA	8
RANO	WTQC	RANO	7
RUSMIKARWATY	QQZGUPXHKGNE	RUSMIKARWATY	9
YUDI	QJXW	YUDI	11
ARIFSUPRIONO	NANWJJGRWZNU	ARIFSUPRIONO	9
PASIRAHI	WGRVJNOH	PASIRAHI	6
RAWI	WCQW	RAWI	7
MIRASARI	EGQFGOGH	MIRASARI	7
TUTURSWIHADI	QYZHQZZQVOEO	TUTURSWIHADI	12
ELDA	HJDO	ELDA	6
SITIMAISARAH	EGQHCWYLOCON	SITIMAISARAH	6
MAHYUDIN	WJGWGQEM	MAHYUDIN	7
FIKO	EQEC	FIKO	8
MULIANUR	QTKIGWOQ	MULIANUR	7
DEMIWATI	AGLHXSOH	DEMIWATI	8
NORHAIYA	KOQMHWNZ	NORHAIYA	10
RESSASAPUTRI	AYSGUNXZIMLO	RESSASAPUTRI	6
IRMA	NSHO	IRMA	7

Pengujian pada Tabel 1 dilakukan dengan meggunakan data yang telah diporelah dari UPT. Puskesmas Pujon Kalimantan Tengah yang merupakan data *text* biodata pasien. Data pasien yang digunakan sebagai *plaintext* akan menghasilkan *ciphertext* jika telah dienkripsi, hasil enkripsi yang berupa *ciphertext* akan didekripsikan dan menghasilkan *plaintext* dari data pasien. Pada Tabel 1 dapat dilihat bahwa *plaintext* yang diproses dalam enkripsi dan dekripsi tidak mengubah jumlah karakter awal dari *plaintext* tersebut. Waktu proses enkripsi dan dekripsi yang terdapat pada Tabel 1 menunjukkan bahwa rata-rata waktu prosesnya adalah 8 detik. Untuk jumlah karakter *text* tidak mempengaruhi waktu proses enkripsi dan dekripsinya.

4. SIMPULAN

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, maka dapat diambil kesimpulan. Super enkripsi yang dibangun menggunakan kriptografi Transposisi *Columnar*, *Vigenere Cipher* dan Substitusi *Monoalphabetic*, dapat melakukan pengkodean (enkripsi) dan mengembalikan (dekripsi) pesan dalam format *text*. Berdasarkan hasil pengujian data *text* biodata pasien UPT. Pukesmas Pujon Kalimantan Tengah. Data *text* biodata pasien UPT. Pukesmas Pujon Kalimantan Tengah sebelum dienkripsi dekripsi dan setelah dienkripsi dekripsi tidak mengalami perubahan terhadap jumlah karakternya. Berdasarkan hasil pengujian terhadap waktu proses enkripsi dekripsi waktu rata-rata yang didapat adalah

8 detik. Jumlah karakter tidak mempengaruhi kecepatan proses karena banyak sedikitnya jumlah karakter yang digunakan dapat menghasilkan kecepatan proses yang sama. Berdasarkan tiga kriptografi yang digunakan dalam pembuatan super enkripsi ini ketiga kriptografi tersebut masih dalam kriptografi klasik.

DAFTAR PUSTAKA

[1]. A. Ilmiah *et al.*, "Perancangan Super Enkripsi Menggunakan Metode Substitusi S-Box AES dan Metode Transposisi dengan Pola Vertical-Horizontal," 2016.

[2]. S. Budi, A. B. Purba, and J. Mulyana, "Pengamanan File Dokumen Menggunakan Kombinasi Metode Subtitusi Dan Vigenere Cipher," *Ilk. J. Ilm.*, vol. 11, no. 3, pp. 222–230, 2019, doi: 10.33096/ilkom.v11i3.477.222-230.

[3]. E. Gunadhi and A. Sudrajat, "Pengamanan Data Rekam Medis Pasien Menggunakan Kriptografi Vigènere Cipher," *J. Algoritm.*, vol. 13, no. 2, pp. 295–301, 2017, doi: 10.33364/algoritma/v.13-2.295.

[4]. J. Sasongko, "Pengamanan Data Informasi menggunakan Kriptografi Klasik," vol. X, no. 3, pp. 160–167, 2005.

[5]. F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, p. 20, 2016, doi: 10.30872/jim.v10i1.23.

[6]. N. D. Nathasia and a. E. Wicaksono, "Penerapan Teknik Kriptografi Stream-Cipher Untuk Pengaman Basis Data," *ICT Research Center UNAS*, vol. 6, no. 1. pp. 1–22, 2011.

[7]. Fatima, "Artikel Ilmiah Artikel Ilmiah," *STIE Perbanas Surabaya*, no. 682012043, pp. 0–16, 2020.

[8]. Y. Reswan, U. Juhardi, and B. T. Yuliansyah, "Implementasi Kompilasi Algoritma Kriptografi Transposisi Columnar Dan Rsa Untuk Pengamanan Pesan Rahasia," *J. Inform. Upgris*, vol. 4, no. 2, 2019, doi: 10.26877/jiu.v4i2.2812.

[9]. Y. Permanasari, "Kriptografi Klasik Monoalphabetic," *Matematika*, vol. 16, no. 1, pp. 7–10, 2017, doi: 10.29313/jmtm.v16i1.2543.