KOMBINASI ALGORITMA KRIFTOGRAFI CAESAR CIPHER DAN PERMUTATION CIPHER UNTUK PESAN TEKS MENGGUNAKAN PYTHON

Riyan Feraldi[1], Aida Khairuna[2], Mhd Arief Hasan[3], Rafael Rezky[4], Hardiansyah Ramadhan[5]

[1,2,3,4,5]Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Lancang Kuning
Jl. Yos Sudarso No.KM. 8, Rumbai, Pekanbaru, Riau 28266
e-mail: [1] riyanferaldis11@gmail.com , [2]aidakhairuna03@gmail.com, [3]m.arif@unilak.ac.id,
[4]rafaelrezky05@gmail.com, [5]hardivolly28@gmail.com

Abstrak: *Saat ini, khususnya pada perkembangan teknologi informasi berkembang begitu pesat. Menjaga dan melindungi pesan teks informasi dari berbagai pihak yang bisa merugikan sangatlah penting. Menjaga pesan teks informasi memiliki ilmu, seperti kriptografi. Kriptografi dalam pesan teks untuk melindungi data-data yang penting agar tidak merugikan pemilik. Oleh karena itu, kami perlu meningkatkan pesan teks, terutama data seperti berkas dokumen serta pesan teks. Sehingga, keaslian data dapat terjaga dengan aman. Kombinasi algoritma kriptografi yang digunakan untuk pengamanan pesan teks yang digunakan yaitu algoritma caesar cipher dan algoritma permutation cipher. Sehingga, dengan menggunakan kombinasi algoritma caesar cipher dan algoritma permutation cipher, tingkat keamanan pesan teks bisa lebih terjaga keaslian datanya.*

Kata kunci **:** *Kriptografi, Pesan teks, Caesar cipher, Permutation cipher.*

Abstract: *Currently, especially in the development of information technology is developing so rapidly. Safeguarding and protecting informational text messages from various parties that can harm is very important. Maintaining informed text messages has a science, like cryptography. Cryptography in text messages to protect important data so as not to harm the owner. Therefore, we need to improve text messaging, especially data such as document files and text messages. So, the authenticity of the data can be maintained safely. The combination of cryptographic algorithms used to secure text messages is the Caesar Cipher algorithm and the Permutation Cipher algorithm. So, by using a combination of the caesar cipher algorithm and the permutation cipher algorithm, the security level of text messages can be more maintained for the authenticity of the data.*

Keywords**:** *Cryptography, Text messages, Caesar cipher, Permutation cipher.*

1.PENDAHULUAN

Perkembangan ilmu pengetahuan dan teknologi saat ini mengalami perubahan dari hari ke hari terutama di bidang komunikasi. Komunikasi dapat berlangsung dengan berbagai cara, salah satunya dengan menggunakan tulisan atau pesan teks. Dengan menulis (teks), banyak informasi yang dapat di peroleh, dan terkadang informasi rahasia dimasukkan ke dalam teks. Pertukaran informasi terjadi setiap detik di Internet, jadi beberapa pihak yang tidak bertanggung jawab akan mencuri banyak informasi. Untuk membuat data atau pesan teks yang di kirim dari berbagai aman. Oleh karenanya, pesan teks atau data di sembunyikan dengan menggunakan mengkombinasi algoritma Caesar cipher dan Permutation cipher (Kriptografi and Transposition 2017).

Permasalahan di dalam pesan teks adalah suatu bagian terpenting dalam melindungi penyimpanan data-data yang terpenting data yang sudah di simpan seperti dalam bentuk digital. Masalah ini karena perkembangan teknologi yang begitu pesat serta konsep system terbuka yang sudah banyak digunakan, jadi dengan mudahnya seseorang menghancurkan data yang sudah disimpan dalam bentuk digital tanpa harus diketahui oleh pemilik data. Karena itu, perlu dikelola pesan teks digital dengan mengkombinasi dua algoritma caesar cipher dan algoritma permutation cipher yang berfungsi untuk meningkatkan suatu keamanan pesan teks.

Kriptografi juga dapat diartikan sebagai ilmu menjaga suatu keamanan dari pesan teks. Ketika sebuah pesan di kirim dari tempat yang satu ke tempat lainnya, isi dari sebuah pesan nantinya dapat diretas ataupun disadap oleh orang-orang yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk melindungi pesan teks, itu dapat diubah menjadi suatu kode yang tidak bisa dipahami oleh pihak lain (Pseudocode 2016).

Penggunaan kriptografi digunakan untuk mencegah adanya peretasan data saat proses pengiriman dengan mengenkripsi data. Enkripsi data yaitu dengan cara mengubah teks asli (plaintext) menjadi teks bersandi (ciphertext) yang tidak berarti dan tidak dapat dibaca.

Metode yang digunakan adalah dengan menggunakan enkripsi untuk penyandian dan dekripsi untuk mengaktifkan enkripsi. Proses enkripsi mengubah data asli (plaintext) menjadi teks tersandi (ciphertext). Proses enkripsi mengubah data asli (plaintext) menjadi data tersandi. Pada saat yang sama, ketika data di terima, proses deskripsi mengubah data yang di sandikan (ciphertext) menjadi data asli (plaintext). Proses enkripsi dan dekripsi membutuhkan algoritma kriptografi (kata sandi). Algoritma kriptografi ini begitu beragam, dan tujuannya adalah membuat pesan serumit mungkin sehingga data atau pesan teks di dalamnya aman, danhanya orang-orang yang berwenang yang dapat menggunakan data tersebut (Kusumaningtyas 2018).

2. TINJAUAN PUSTAKA

2.1.Kriptografi

Kriptografi adalah penelitian ilmiah dan artistic yang di lakukan untuk menjaga pesan teks atau informasi yang di kirim, dan juga merupakan ilmu memecahkan pesan terenkripsi (tersamar). Dimana kriptografi adalah seni mendeskripsikan data dalam bentuk gambar, suara dan pesan teks. Adapun tujuan dari penerapan kriptografi merupakan untuk menyembunyikan sesuatu, baik berupa pesan rahasia seperti teks, gambar, suara atau video (Septiarini 2011).

Kriptografi adalah studi tentang bagaimana menjaga suatu data agar aman untuk menghindari gangguan dari pihak ketiga saat mengirimkan dan menyimpan data, dan kriptografi juga memiliki tujuan untuk melindungi kerahasiaan (Deolika 2020).

Muhammad Nurtanzis Sutoyo dan Murhaban menegaskan (Sutoyo 2016) bahwa aspek-aspek pesan teks dalam kriptografi adalah sebagai berikut.

a. *Confidentiality*, yaitu upaya melindungi informasi atau data dari suatu percobaan penyerangan seperti penyadapan.
b. *Integrity*, informasi atau data terjaga keasliannya tanpa adanya perubahan yang dilakukan oleh pihak yang tidak berkepentingan terhadap data yang dikirimkan.
c. *Availability*, ketersediaan informasi apabila dibutuhkan. Upaya penyerangan dapat berupa menghapus atau menghilangkan data.
d. *Authentication,* menjaga keaslian data dengan melakukan autentikasi terhadap sumber,server, dan orang yang ingin menggunakan data.
e. *Access Control*, memiliki akses untuk mengatur siapa yang bisa mengakses informasi dan melakukan apa terhadap informasi.

Adnan Buyung Nasution menegaskan (Nasution 2019) bahwa tujuan dari kriptografi ialah untuk memberikan layanan keamanan yaitu:

1. Penyembunyian (*Confidentiality*) Menyembunyikan informasi dari pihak yang tidak berkepentingan sehingga kerahasiaan informasi terjaga.
2. Kelengkapan Data *(Integrity*) Data yang diterima oleh penerima tidak terganti selama pengiriman berlangsung.
3. Keaslian (*Message Authentication*) Identitas dan sumber data yang terkait memiliki kejelasan terhadap autentikasi data.
4. Tidak ada penolakan (*Nonrepudiation)* Menjamin data yang dikirim dan diperoleh tidak dapat disangkal ataupun ditolak.

2.2.Enkripsi

Enkripsi adalah sebuah proses menggunakan algoritma tertentu untuk mengubah informasi atau sebuah data yang akan akan di kirim ke dalam bentuk yang mungkin tidak dapat dketahui sebagai informasi aslinya (Mulawarman et al. 2015).

Enkripsi merupakan suatu proses mengubah data ataupun mengubah informasi menjadi suatu bentuk yang mungkin hamper tidak bisa di tandai seperti informasi asli dengan menggunakan suatu algoritma tertentu. Teks biasa atau plainteks merupakan informasi ata pesan yang akan dikirim dengan format yang mudah terbaca atau format asli (Sutoyo 2016).

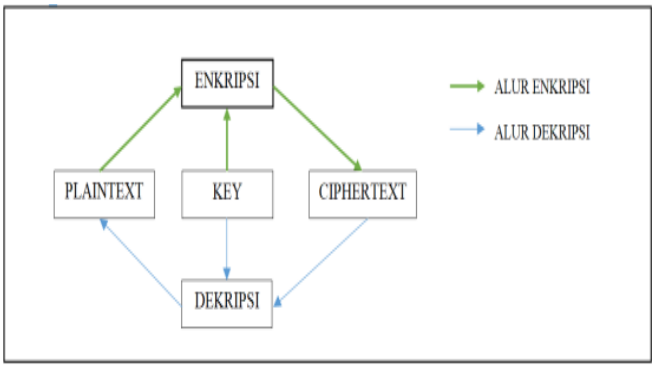
Enkripsi berfungsi untuk menyandikan data ataupun informasi maka orang yangtidak berkepentingan tidak berhak membacanya. Maka, dengan adanya data anda dienkripsi dengan kunci. Untuk membuka data atau pesan teks, kuncinya sama dengan kunci yang digunakan untuk enkripsi (untuk enkripsi kunci privat) atau memiliki kunci yang berbeda (untuk enkripsi kunci publik)(Sasongko 2005).

2.3.Dekripsi

Dekripsi merupakan kebalikan dari enkripsi itu dapat mengubah bentuk terselubung kembali ke pesan teks. Pesan teks atau daya yang masih asli dan tidak terenkripsi disebut teks biasa (plaintext).

Selanjutnya, sesudah disamarkan melalui penyandian, jadi teks biasa (plaintext) disebut teks asli (ciphertext). Proses penyamaran diri dari plaintext menjadi ciphertext disebut enkripsi, dan proses pengembalian teks dari ciphertext menjadi plaintext kembali disebut dekripsi (Mulawarman et al. 2015).

Dekripsi merupakan proses mengubah formulir tersamar ke formulir awal (Sutoyo 2016).



Gambar 1.Alur enkripsi dan dekripsi dengan menggunakan kunci.

2.4.Pesan Teks

Menurut (Mulawarman et al. 2015) pesan adalah informasi atau data yang maknanya mudah dipahami. Nama lain dari pesan yaitu plaintext atau teks jelas yaitu cleartext.

Menurut (Septiarini 2011) pesan merupakan informasi atau data yang mudah dibaca dan dipahami.

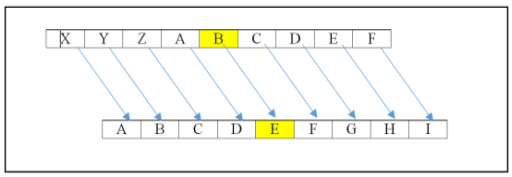
Untuk mencegah pesan tidak dapat diketahui pihak lain, pesan tersebut perlu dikodekan dalam bentuk lain yang tidak mudah di pahami. Bentuk pesan yang disandikan disebut ciphertext. Ciphertext harus bisa diubah kembali ke plaintext agar pesan yang akan di terima dapat terbaca (Informatika, Darma, and Septiarini 2014).

2.5.Caesar Cipher

Substitusi pertama di bidang pesan teks yaitu pada masa pemerintahan Julius Caesar. Maka disebut sebagai Caesar Cipher yang mengubah posisi inisialnya (Gunawan, n.d.).

Kode Caesar (Caesar Cipher) di gunakan oleh raja Yunani kuno, yaitu Julius Caesar. Anda dapat mengganti tiap karakter alphabet dengan karakter yang terletak di 3 posisi berikutnya dari alphabet yang di gunakan (Kriptografi and Transposition 2017).

Caesar Cipher merupakan persoalan khusus dari kata sandi satu huruf, dimana pengaturan huruf-huruf teks kata sandi di peroleh dengan memindahkan huruf-huruf dari huruf sejauh tiga karakter (Studi and Informatika 1996).



Gambar 2. Proses Caesar Cipher

2.6.Permutation Cipher

Menurut (Liu, n.d.) bahwa cipher permutation menyimpan sekelompok permutasi dan nilai kunci rahasia digunakan untuk menentukan permutasi spesifik yang digunakan untuk enkripsi.

Menurut (Studi and Informatika 1996) dalam sandi yang diubah urutannya, plaintext tetap sama, namun urutannya di ubah. Dengan nama lain, algortima akan mengubah urutan rangkaian karakter dalam teks.

Menurut (Nasution 2019) transposition cipher merupakan teknologi enkripsi pesan dengan mengganti posisi tiap huruf pada plaintext (pesan asli tidak trenkripsi) dengan ciphertext (pesan terenkripsi) pada bagian tertentu.

Sasongko menegaskan (Sasongko 2005) bahwa ciphertext di peroleh dengan menggantikan posisi harus dalam plaintext. Dengan nama lain, algortima ini menggantikan serangkaian huruf dalam plaintext. Metode ini biasanya dengan metode permutasi, dikarenakan transposisi tiap karakternya sama dengan karakter tersebut.

Cipher Transposition dapat disebut juga sebagai cipher permutasi karena sebenarnya metode cipher transposition ini memutasikan karakter-karakter plainteks, yaitu dengan menyusun ulang urutan karakter dalam pesan. Metode Cipher Transposition dimana posisi plainteks (karakter atau kode khusus) dirubah, sehingga hasilnya menjadi cipherteks dengan urutan yang berubah atau berbeda. Sehingga Cipher Transposition merupakan metode yang digunakan untuk mengubah plainteks menjadi cipherteks dengan mengubah urutannya (Kusumaningtyas 2018).

3. METODE PENELITIAN

Metode penelitian yang di gunakan merupakan metode literatur atau metode kepustakaan, yaitu dengan mengumpulkan data dan informasi yang diperlukan seperti jurnal, buku dan artikel ilmiah yang berkaitan dengan kriptografi, Caesar cipher, permutation cipher, pesan teks dan lain sebagainya yang berkaitan dengan permasalahan penelitian.

3.1.Rumus Yang Digunakan

3.1.1.Caesar Cipher

Caesar cipher dalam kriptografi adalah metode enkripsi yang sangat sederhana dan populer.Semua huruf dalam teks asli (plaintext) diganti dengan kode,kemudian kode tersebut diubah ke huruf lain dengan perbedaan posisi tertentu dalam alfabet. Huruf-huruf diubah dengan huruf yang selanjutnya dari posisi alphabet yang sama.

Berikut persamaan 1 yang digunakan dalam enkripsi:

$$Cp= (Pt + k) \text{ modulo } 26$$

Dimana 26 adalah jumlah alphabet. Berikut persamaan 2 yang digunakan dalam dekripsi:

$$Pt= (Cp-k) \text{ modulo } 26$$

3.1.2.Permutation Cipher

Tranposisi cipher adalah teknik untuk memindahkan ataupun merotasi setiap karakter dalam teks dengan model-model tertentu. Prinsip pada transposisi berlawanan dengan substitusi yang posisi karakternya tetap hanya diganti oleh karakter lainnya, sedangkan transposisi sendiri karakter tidak diganti namun diubah posisinya.

3.2.Alur Program

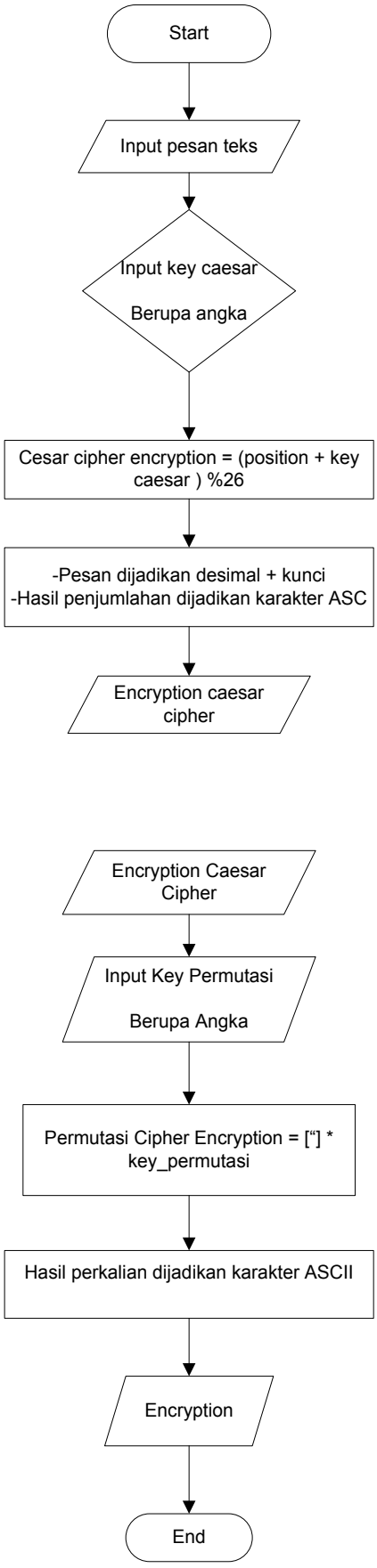
Menggambarkan algoritma dari kriptografi caesar cipher pada proses enkripsi. Enkripsi dimulai dari mendeklarasi variabel, menginput plaintext dan key dari caesar cipher dan menjadi ciphertext.

Selanjutnya, enkripsi dari caesar cipher kemudian dikunci lagi dengan key baru, lalu menjadi enkripsi permutation cipher.

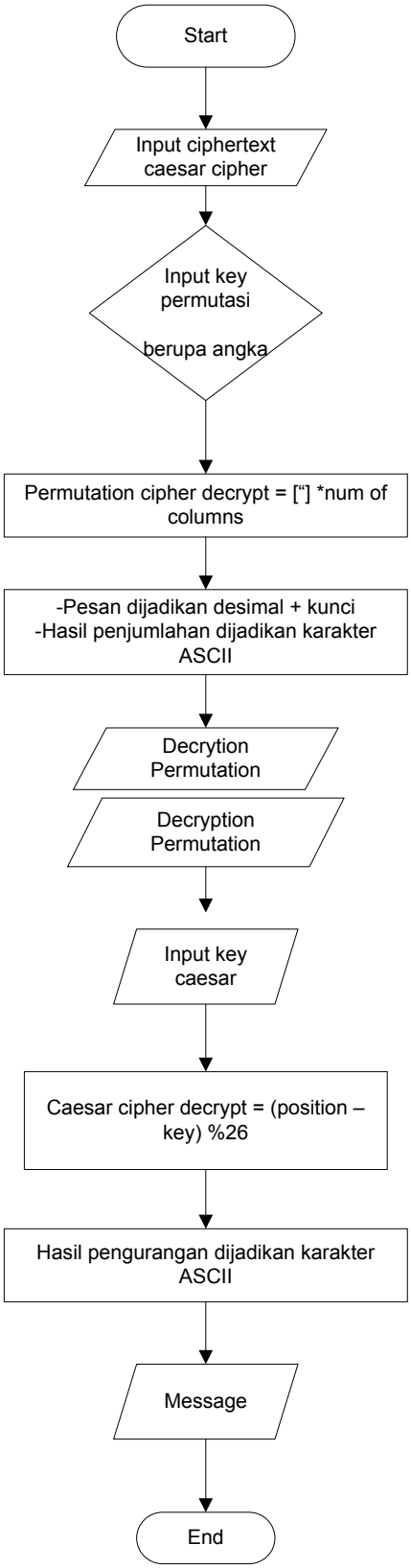
3.3.Pengujian Program

Untuk menguji enkripsi dan dekripsi dengan kombinasi caesar cipher dan permutation cipher, pengujian dilakukan dengan membuat program dengan python guna mendapatkan hasil eksekusi melalui data uji python.

Python adalah bahasa yang ditafsirkan dengan ex-sintaks tekan yang telah dibandingkan dieksekusi. (Computing 2007).



Gambar 3. *Flowchart* Enkripsi



Gambar 4. *Flowchart* Dekripsi

4. HASIL DAN PENGUJIAN

4.1.Enkripsi Caesar Cipher

Mengenkripsi plainteks "KRIPTOGRAFI", dengan key = 3, jadi diperoleh ciphertext "**NULSWRJUDIL"** ". Dengan persamaan 1,dilakukan proses enkripsi terhadap pesan.

Plaintext : KRIPTOGRAFI
Kunci : 3

K = (10 + 3) mod 26
= 13 = N
R = (17 + 3) mod 26
= 20 = U
I = (8 + 3) mod 26
= 11 = L
P = (15 + 3) mod 26
= 18 = S
T = (19 + 3) mod 26
= 22 = W
O = (14 + 3) mod 26
= 17 = R
G = (6 + 3) mod 26
= 9 = J
R = (17 + 3) mod 26
= 20 = U
A = (0 + 3) mod 26
= 3 = D
F = (5 + 3) mod 26
= 8 = I
I = (8 + 3) mod 26
= 11 = L

4.2.Enkripsi Permutation Cipher

Menkripsikan chipertext Caesar cipher **"NULSWRJUDIL"**, dengan key = 6, jadi diperoleh "LWNRSUDLJXIU". Untuk penyelesaian perhatikan langkah-langkah berikut.

Plaintext = NULSWRJUDIL
Key = 6

Plaintext :

1	2	3	4	5	6	1	2	3	4	5	6
N	U	L	S	W	R	J	U	D	I	L	X

Ciphertext :

3	5	1	6	4	2	3	5	1	6	4	2
L	W	N	R	S	U	D	L	J	X	I	U

Jadi Chipertextnya : LWNRSUDLJXIU

4.3.Dekripsi Caesar Cipher

Selanjutnya, proses dekripsi menggunakan persamaan 2.

Ciphertext = NULSWRJUDIL
Kunci = 3

N = (13 - 3) mod 26

= 10 = K
U = (20 - 3) mod 26
= 17 = R
L = (11 - 3) mod 26
= 8 = I
S = (18 - 3) mod 26
= 15 = P
W = (22 - 3) mod 26
= 19 = T
R = (17 - 3) mod 26
= 14 = O
J = (9 - 3) mod 26
= 6 = G
U = (20 - 3) mod 26
= 17 = R
D = (3 - 3) mod 26
= 0 = A
I = (8 - 3) mod 26
= 5 = F
L = (11 - 3) mod 26
= 8 = I

4.4.Dekripsi Permutation Cipher

Plaintext = LWNRSUDLJXIU
Key = 6

Plaintext :

1	2	3	4	5	6	1	2	3	4	5	6
L	W	N	R	S	U	D	L	J	X	I	U

Ciphertext :

3	6	1	5	2	4	3	6	1	5	2	4
N	U	L	S	W	R	J	U	D	I	L	X

Jadi Chipertextnya : NULSWRJUDIL

4.5.Pengujian

Proses pengujian ini dengan menggunakan bahasa pemrograman python. Pengujian enkripsi dengan menggunakan plainteks dan key untuk pesan teks sebagai berikut.

4.5.1.Program Enkripsi

```
def caesar_cipher(plainteks,kunci_caesar):

cipherteks = ""
        for c in plainteks:
          if c in alphabet:
          position = alphabet.find(c)
        new_position = (position + kunci_caesar) % 26
          new_character = alphabet[new_position]
cipherteks += new_character
          else:
        cipherteks += c

   return cipherteks

def permutasi_cipher(message,kunci_permutasi):
```

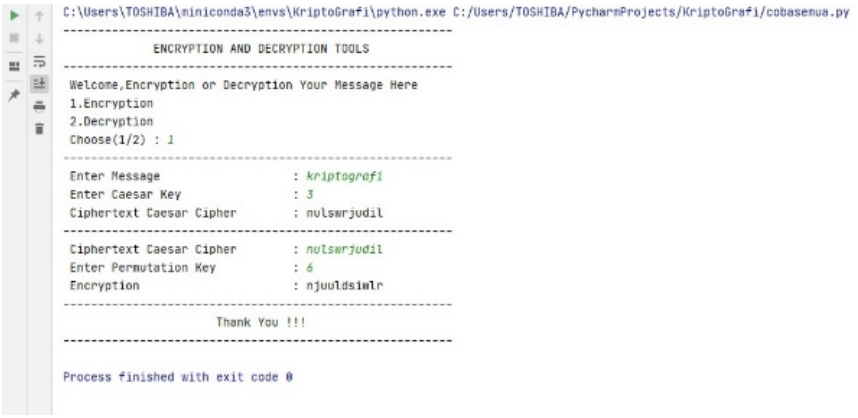
```
ciphertext = [''] * kunci_permutasi

    for column in range(kunci_permutasi):
        currentIndex = column

        while currentIndex < len(message):
            ciphertext[column] += message[currentIndex]

            currentIndex += kunci_permutasi


    return ''.join(ciphertext)
```

4.5.2.Program Dekripsi

```
def decryptcaesar(encrypted_message,key):

    decrypted_message = ""

    for c in encrypted_message:

        if c in alphabet:
            position = alphabet.find(c)
            new_position = (position - key) % 26
            new_character = alphabet[new_position]
            decrypted_message += new_character

        else:
            decrypted_message += c

    return decrypted_message

def decrypt_permutation(key, message):

    numOfColumns = math.ceil(len(message) / key)

    numOfRows = key

    numOfShadedBoxes = (numOfColumns * numOfRows) - len(message)

    plaintext = [''] * numOfColumns

    col = 0

    row = 0

    for symbol in message:

        plaintext[col] += symbol

        col += 1

        if (col == numOfColumns) or (col == numOfColumns - 1 and row >= numOfRows -
numOfShadedBoxes):
            col = 0
            row += 1

    return ''.join(plaintext)
```

4.5.3.Hasil Pengujian

Pengujian program menggunakan bahasa pemrograman python, seperti berikut ini.



Gambar 5. Enkripsi Plaintext

Untuk proses dekripsi, dapat dilihat pada gambar 6.

Gambar 6. Dekripsi Ciphertext

5.Kesimpulan dan Saran

5.1.Kesimpulan

Pesan teks dapat digunakan untuk mensgirim pesan yang tidak dapat diketahui orang lain. Dimana plaintext di enkripsi menjadi ciphertext, yang dapat membantu bertukar pesan dalam bentuk teks dan jumlah plaintext yang di isi pun tidak terbatas.

Daftar Pustaka

[1] Computing, Scientific. 2007. "Python for Scientific Computing," 10–20.
[2] Deolika, Agatha. 2020. "MODIFIKASI METODE HILL CIPHER DAN VERNAM CIPHER MENGUNAKAN KODE ADMINISTRASI DAN PAJAK" 4 (2).
[3] Gunawan, Indra. n.d. "Kombinasi Algoritma Caesar Cipher Dan Algoritma Rsa Untuk Pengamanan File Dokumen Dan Pesan Teks," no. 1: 124–29.
[4] Informatika, Pelita, Budi Darma, and Anindita Septiarini. 2014. "IMPLEMENTASI ALGORITMA KRIPTOGRAFI HILL CIPHER," no. 0911610: 76–81.
[5] Kriptografi, Kata Kunci, and Cipher Transposition. 2017. "ANALISA DAN IMPLEMENTASI KRIPTOGRAFI PADA PESAN RAHASIA" 3 (1): 1–11.

[6] Kusumaningtyas, Juwita Artanti. 2018. "Analisa Algoritma Ciphers Transposition : Study Literature" I (1): 1–12.
[7] Liu, Nan. n.d. "Compressing Encrypted Data and Permutation Cipher," no. 2014: 1–17.
[8] Mulawarman, Jurnal Informatika, Fresly Nandar Pabokory, Indah Fitri Astuti, Awang Harsa Kridalaksana, Program Studi, Ilmu Komputer, Universitas Mulawarman, Pesan Teks, and Isi File Dokumen. 2015. "IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS , ISI FILE DOKUMEN , DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION" 10 (1).
[9] Nasution, Adnan Buyung. 2019. "IMPLEMENTASI PENGAMANAN DATA DENGAN MENGGUNAKAN" 3 (1): 1–6.
[10] Pseudocode, Jurnal. 2016. "KOMUNIKASI BERBASIS TEKS" III (September): 129–36.
[11] Sasongko, Jati. 2005. "Pengamanan Data Informasi Menggunakan Kriptografi Klasik" X (3): 160–67.
[12] Septiarini, Anindita. 2011. "Sistem Kriptografi Untuk Text Message Menggunakan Metode Affine" 6 (1): 50–53.
[13] Studi, Program, and Teknik Informatika. 1996. "Penyandian Dalam Kriptografi."
[14] Sutoyo, Muhammad Nurtanzis. 2016. "Kombinasi Algoritma Kriptografi Caesar Chiper Dan" 2 (1): 58–66.