Jurnal Elektronik Ilmu Komputer Udayana
Volume 12, No 2. November 2023

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Pengamanan Teks Dalam File Menggunakan Metode Enkripsi/Dekripsi Kombinasi Vigenere Cipher Dan Shift Cipher

I Made Arthya Andika Putra[a1], Agus Muliantara[a2]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana
Jalan Raya Kampus Unud, Jimbaran, Badung, Bali 80361, Indonesia
[1]arthyaandika@gmail.com
[2]muliantara@unud.ac.id

Abstrak

Penelitian ini bertujuan untuk mengimplementasikan sistem enkripsi dan dekripsi untuk keamanan data file sesuai aturan yang digunakan. Untuk mengatasi kekurangan atau kesalahan proses enkripsi dan dekripsi ini, dapat menerapkan kombinasi algoritma kriptografi klasik antara Vigenere Cipher dengan Shift Cipher untuk mengatasi keamanan data file. Algoritma Vigenere Cipher dan Shift Cipher termasuk dalam algoritma kriptografi klasik. Algoritma ini dipilih karena kemampuannya untuk melakukan enkripsi klasik dan pertimbangan keamanan untuk data file. Penelitian ini mengubah isi file teks menjadi password acak (encrypted file) untuk menjaga keamanan data dari orang yang tidak berhak dan hanya mengizinkan pemiliknya untuk mengembalikan dengan file data asli (dekripsi). Diharapkan hasil penelitian yang diperoleh dari kombinasi hyper-encryption dan description akan membantu sistem yang dibuat untuk mendukung dan menjaga keamanan file sebelum proses pengiriman data dalam kerangka suatu perusahaan, sehingga pesan tetap bersifat pribadi sampai saat itu.

Keywords: *Enkripsi, Dekripsi, Vigenere Cipher, Shift Cipher, Keamanan*

1. Pendahuluan

Pada masa ini, teknologi kian berkembang pesat dan semakin canggih. Oleh sebab itu, membuat manusia dapat mencari dan bertukar informasi secara lebih luas dan semakin cepat. Salah satu datanya berupa berbentuk teks. Dengan demikian, semakin banyak pengguna yang memanfaatkan teknologi, semakin rentan pula keamanan informasi tersebut. Semakin banyak oknum yang dapat menyalahgunakan informasi tersebut.

Maka dari itu, dibutuhkan keamanan yang lebih agar data/informasi tidak mudah disalahgunakan oleh oknum tersebut. Maka diperlukan suatu metode/ilmu untuk mengamankan suatu data/informasi berupa teks, file, foto, video, dan lain sebagainya. Keamanan sistem informasi merupakan suatu tindakan untuk pencegahan dari serangan pengguna komputer, pengakses jaringan yang tak bertanggung jawab, dan pendeteksian dari tindakan - tindakan pengganggu yang tidak dikenali oleh sistem [4].

File merupakan unit data yang disimpan dalam sistem yang dapat dimodifikasi dan diakses oleh pengguna. Sebuah file memiliki ID yang berbeda dalam memori di mana ia berada. Lokasi direktori tempat file berada disebut *path*. File seperti aliran data yang berisi kumpulan data terkait, dan atribut tentang file, yang disebut properti, berisi informasi tentang file seperti: informasi tentang kapan file itu dibuat.

Agar keamanannya lebih terjaga, maka ilmu atau metode yang dapat digunakan untuk menjaganya yaitu kriptografi. Kriptografi merupakan sebuah ilmu dan merupakan seni yang berperan untuk memberikan rasa aman saat mengirimkan pesan [4]. Kriptografi juga keilmuan yang mengkaitkan, belajar mengenai menyembunyikan huruf atau tulisan dimana mencegah untuk orang yang selain diberi pesan dapat membaca pesan tersebut, dan hanya yang berhak dapat mengerti isinya [6]. Kriptografi adalah suatu teknik yang belajar untuk menyimpan informasi berupa file atau pesan yang dikirimkan secara aman dari pengirim ke penerima sehingga tidak ada gangguan dari pihak lain [3].

Kriptografi khususnya kriptografi klasik merupakan ilmu untuk mengamankan pesan rahasia (*plain text*) menjadi pesan tersamarkan (*cipher text*) yang dalam prosesnya dilakukan pengubahan tiap karakter

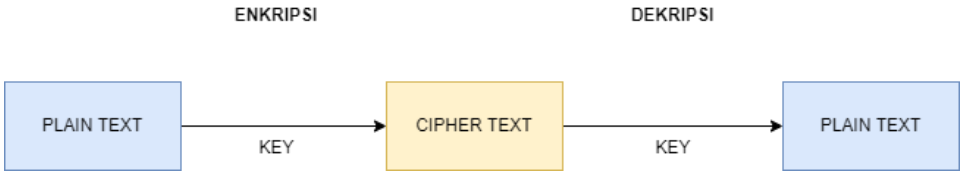
[4]. Proses mengubah *plain text* menjadi *cipher text* disebut enkripsi, sementara proses sebaliknya disebut dekripsi [6]. Pengubahan itu bertujuan untuk mengamankan teks agar tidak dapat diketahui oleh pihak manapun kecuali orang yang berhak mengetahui isi teks tersebut.

Teknik kriptografi mempunyai 2 cara yaitu dengan teknik klasik dan Teknik modern, untuk kriptografi klasik contohnya seperti: *Caesar Cipher*, permutasi, transposisi, *Shift Cipher*, dan *Vigenere Cipher* [1]. Terdapat beberapa cara untuk mengamankan data/informasi menggunakan ilmu kriptografi, salah satunya yaitu kombinasi antara *Vigenere Cipher* dan *Shift Cipher* untuk mengamankan data.

Maka dari itu, pengamanan suatu file/informasi dengan metode enkripsi/dekripsi dapat menggunakan ilmu kriptografi dalam penggunaannya. Pada penelitian kali ini akan menggunakan kombinasi dari dua Teknik kriptografi klasik diantaranya yaitu *Vigenere Cipher dan Shift Cipher*. Pada penelitian ini, data yang diamankan berupa data file teks (*txt*). Proses mengelola data tersebut yaitu file tersebut di enkripsi dengan algoritma *Vignere Cipher* untuk menghasilkan *cipher text* baru dari file tersebut yang bertujuan untuk menjaga keamanan dari file dan informasi yang ada dalam file tersebut. Tujuan dari penelitian ini untuk membuat aplikasi keamanan data file dan informasinya menggunakan kombinasi antara *Vigenere Cipher dan Shift Cipher* yang diimplementasikan pada bahasa pemrograman *Python 3*.

2. Metode

2.1. Teknik Enkripsi dan Dekripsi yang Digunakan



Gambar 1. Illustrasi Proses Enkripsi dan Dekripsi

Proses pada teknik kriptografi ini menggunakan konsep enkripsi dan dekripsi untuk penyelesaian dari kasusnya. Enkripsi merupakan suatu teknik penyandian data yang hanya bisa di buka dengan cara proses dekripsi. Enkripsi sendiri adalah suatu metode yang merubah data pesan (*plain text*) menjadi data sandi (*chipher text*) dan enkripsi juga merupakan sistem yang melakukan pengkodean tabel atau kamus sebagai mesia yang telah terdefinisi sebagagai pengganti kata dari informasi yang telah kirim, bisa memiliki makna bahwa cipher dari algoritma yang digunakan dimana mampu melakukan pengkodean semua aliran informasi (*stream*) yang berasal dari pesan menjadi sebuah cryptogram yang tidak mengerti (unintelligible) [4]. Sedangkan dekripsi merupakan kebalikan dari proses enkripsi yaitu merubah kembali bentuk kode yang masih sulit dimengerti (*cipher text*) menjadi ke bentuk semula (*plain text*) dengan menggunakan kunci/*key* yang ada sesuai aturan algoritma yang digunakan sebelumnya.

2.2. Algoritma Vigenere Cipher

Dalam teknik kriptografi, algoritma *Vigenere Cipher* ini sebelumnya dikembangkan dari algoritma *Caesar Cipher*. Pada penelitian ini, untuk hasil enkripsi dan dekripsi pertama-tama dilakukan dengan menggunakan algoritma *Vigenere Cipher* dan kemudian dilanjutkan dengan algoritma *Shift Cipher*.

Vigenere cipher dipublikasikan pada tahun 1586, tetapi algoritma tersebut baru dikenal luas 200 tahun kemudian yang oleh penemunya cipher tersebut dinamakan *Vigenere cipher*. Cipher ini berhasil dipecahkan oleh *Babbage* dan *Kasiski* pada pertengahan abad 19. Vigenere cipher digunakan oleh tantara Konfiderasi (*Confederate Army*) pada perang sipil Amerika (American Civil war). Algoritma Vigenere cipher sangat dikenal karena mudah dipahami dan diimplementasikan [7].

Vigenere Cipher menggunakan tabel vigenere standart dalam mengenkripsi pesan. Tabel yang digunakan merupakan tabel 26 huruf alfabetik standart, yang dimulai dari A sampai Z. Kunci pada Vigenere Cipher dipakai berulang kali sebanyak pesan yang akan dienkripsi [2]. Semakin beragam huruf alfabetik yang dipakai sebagai kunci, maka semakin kuat juga keamanan algoritma Vigenere Cipher ini [2].

Berikut merupakan rumus enkripsi dan dekripsi *Vigenere Cipher*:

Enkripsi : $c_i = (p_i + k_i) \bmod 26$

Dekripsi : $c_i = (c_i - k_i) \bmod 26$

p-ISSN: 2301-5373
e-ISSN: 2654-5101

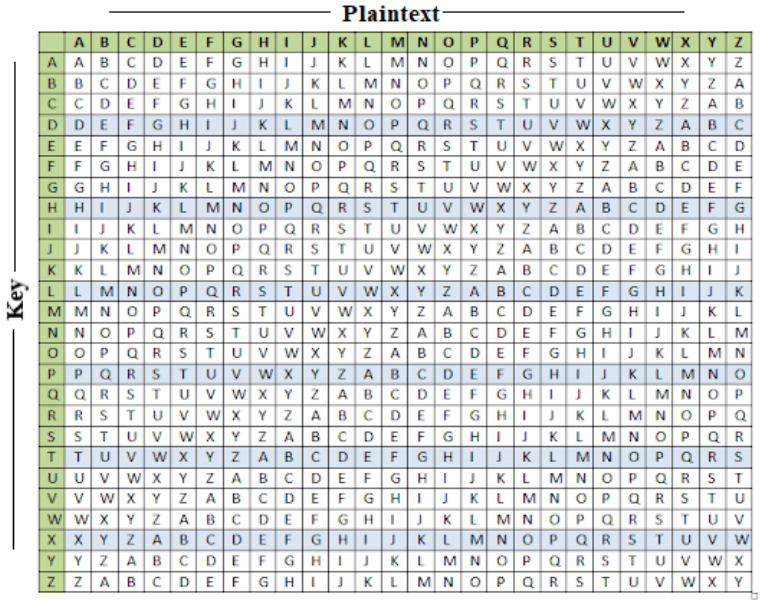
Keterangan:

c_i = nilai dari karakter *cipher teks*

p_i = nilai dari karakter *plain teks*

k_i = nilai dari *key* (diperkirakan jumlah *key* antara A = 0, B = 1 …, Z = 25)

Untuk melakukan proses enkripsi *plain text* dan dekripsi algoritma *vigenere cipher* bisa menggunakan bujur sangkar *vigenere* atau pola tabula recta, yang berguna untuk memudahkan suatu proses berlangsung.



Key \ Plaintext	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 2. Pola tabula recta *vigenere* (huruf)

Contoh:

Plain Text : **MAHASISWA BARU**

Key : **UDAYANA**

Maka cara untuk menentukan *cipher text*-nya yaitu sebagai berikut:

PLAIN TEXT	M	A	H	A	S	I	S	W	A	B	A	R	U
KEY	U	D	A	Y	A	N	A	U	D	A	Y	A	N
CIPHER TEXT	G	D	H	Y	S	V	S	Q	D	B	Y	R	H

Gambar 3. Hasil kriptografi *vigenere* (huruf)

2.3. Algoritma Shift Cipher

Shift Cipher merupakan salah satu bentuk teknik kriptografi klasik yang masih digunakan untuk mengamankan suatu data. Cara kerja *Shift Cipher* yaitu menggeser *plain text* sejauh yang diinginkan oleh pengguna, dengan maksimal penggeseran yaitu 26. Dalam penggunaannya, teknik *shift cipher* menggunakan model perhitungan modulo 26 dan kunci yang digunakan untuk proses enkripsi sama dengan proses dekripsi [5].

Berikut merupakan rumus enkripsi dan dekripsi *Shift Cipher*:

Enkripsi : $C = E(P) = (P + K)$ *Mod* 26

Dekripsi : $P = D(C) = (C - K)$ *Mod* 26

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Q	R	S	T	U	V	W	X	Y	Z
16	17	18	19	20	21	22	23	24	25

Gambar 4. Contoh kriptografi metode *Shift Cipher*/kode geser

Perhatikan contoh dibawah ini:

Plain text : **MAHASISWA BARU**

Plain text diatas diubah menjadi bilangan atau angka yaitu:

M	A	H	A	S	I	S	W	A	B	A	R	U
12	0	7	0	18	8	18	22	0	1	0	17	20

Gambar 5. Contoh metode *Shift Cipher*/kode geser ke angka

Kode Kunci / *Key* : **6**

Caranya yaitu dengan menambahkan angka pada *plain text* dan kunci/*key* 6. Maka hasilnya yaitu sebagai berikut:

M	A	H	A	S	I	S	W	A	B	A	R	U
12	0	7	0	18	8	18	22	0	1	0	17	20
18	6	13	6	24	14	24	2	6	7	6	23	0
S	G	N	G	Y	O	Y	C	G	H	G	X	A

Gambar 6. Hasil kriptografi metode *Shift Cipher*/kode geser

Jika hasil yang telah dijumlahkan lebih dari 2t6, maka hasilnya perlu dikurangi 26. Misalnya yaitu pada huruf W diatas jika ditambahkan *key* 6 maka hasilnya akan menjadi 28, lalu 28 perlu dikurangi 26 dan hasilnya menjadi 2. Setelah itu, hasil penjumlahan dapat dikonversi menjadi huruf sesuai dengan nilai standar setiap huruf yang sudah ditetapkan.

2.4. Kombinasi Vigenere Cipher dan Shift Cipher

Teknik enkripsi teks dapat dimulai dengan menggunakan metode *Vigenere Cipher*, dan kemudian hasil enkripsi dari *Vigenere Cipher* di enkripsi kembali menggunakan metode *Shift Cipher* sehingga terbentuk keamanan dengan menggunakan dua algoritma kriptografi yang bertujuan untuk memberikan keamanan berlapis pada teks. Jika ingin mengembalikan teks agar terbentuk seperti semula (*plain text*), dapat melakukan proses dekripsi menggunakan algoritma yang sama dengan menggunakan kunci yang sama juga. Jadi, prinsip kombinasi *Vigenere Cipher* dan *Shift Cipher* adalah sebagai berikut:

Enkripsi

P → E(*Vigenere*) = C(*Vigenere*)

P(C *Vigenere*) → E(*Shift*) = C(*Shift*)

Dekripsi

C(*Shift*) → D(*Shift*) = P(*Shift*)

P(P *Shift*) → D(*Vigenere*) = P(*awal*)

p-ISSN: 2301-5373
e-ISSN: 2654-5101

2.5. Bahasa Pemrograman Python

Python merupakan suatu bahasa pemrograman yang interpretative dan serbaguna yang dimana model rancangannya hanya ditujukan pada suatu tingkatan terbacanya *syntax* atau kode. *Python* sendiri dikenal dengan suatu fitur dengan mengkombinasikan kemampuan dan kapasitas, sintaks kode yang jelas, serta telah dilengkapi dengan fungsionalitas dan juga lebih komprehensif. *Python* telah banyak digunakan dan penggunaan cakupan *python* ini cukup luas dalam segi kegunaan.

Fitur dari *python* sendiri telah tersedia dengan jumlah yang cukup banyak, baik itu dalam memfasilitasi *tools* dan *library* yang ada serta penggunaan bahasa yang digunakan sangat membantu dalam membuat suatu program yang dapat dikembangkan untuk penggunaan dalam skala lingkup yang besar seperti pengolahan *big data* dan pengolahan data seperti metode *kriptografi*. Bahasa pemrograman *python* dipilih karena penggunaan sintaksnya yang sangat mudah dan dapat mudah dimengerti. Selain itu, telah disediakan berbagai fungsi serta modul yang dapat mempermudah dalam membuat suatu program khususnya menggunakan teknik kriptografi.

3. Hasil dan Pembahasan

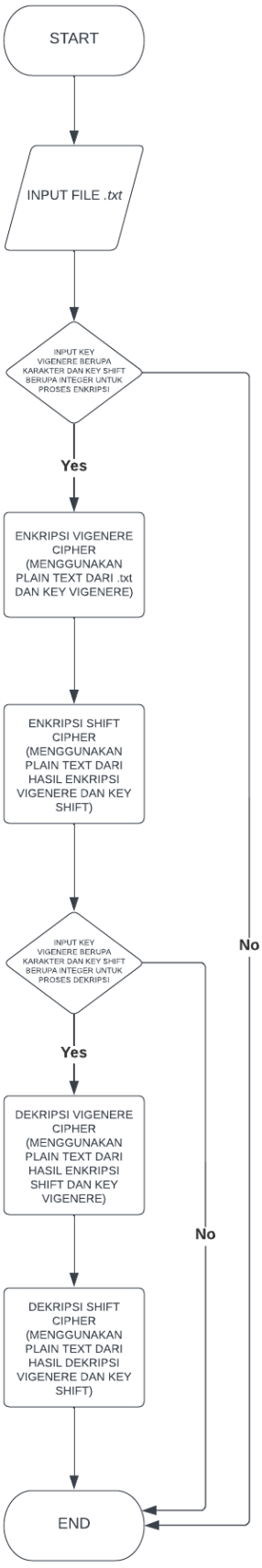
3.1. Analisa Pembahasan

Dalam melakukan proses enkripsi atau dekripsi menggunakan kombinasi dari teknik kriptografi klasik antara algoritma *Vigenere Cipher* dan *Shift Cipher* pada teks yang berada di dalam file berekstensi *.txt* maka dapat menggunakan bahasa pemrograman *Python* yang dapat membantu dalam menyelesaikan dan mengembangkan percobaan kombinasi antara kedua algoritma tersebut. Oleh karena itu, untuk melakukan percobaan tersebut, terlebih dahulu membuat *script* untuk proses kombinasi dari kedua algoritma tersebut sesuai sintaks yang telah disediakan oleh bahasa pemrograman *Python*, kemudian membuat file *.txt* yang didalamnya berisikan *plain text* atau teks yang akan digunakan dalam percobaan.

Setelah itu, program dapat dijalankan dan pertama-tama melakukan proses enkripsi *Vigenere Cipher* dengan memasukkan *key* berbentuk sebuah kata. Lalu, memasukkan *key* berbentuk angka yang akan digunakan pada proses enkripsi algoritma *Shift Cipher*. Lalu, program dapat menghasilkan hasil enkripsi dari *Vigenere Cipher* menggunakan *plain text* serta *key* vigenere dan *Shift Cipher* menggunakan *plain text* dari hasil ekripsi *Vigenere Cipher* serta *key shift*. Untuk proses dekripsi kebalikan dari proses enkripsi, menggunakan *key* yang sama seperti proses enkripsi sebelumnya. ~~ja~~

3.2. Alur Proses Enkripsi dan Dekripsi File

Proses untuk melakukan proses enkripsi dan dekripsidengan menggunakan kombinasi antara algoritma kriptografi klasik *Vigenere Cipher* dan algoritma *Shift Cipher*. *Flowchart* ini bertujuan untuk dapat membantu dalam membuat suatu rancangan program sebelum melakukan proses enkripsi dan dekripsi pada pengolahan data menggunakan file *.txt* ke dalam program yang telah dibuat.



Gambar 7. Flowchart dari program proses enkripsi dan dekripsi

p-ISSN: 2301-5373
e-ISSN: 2654-5101

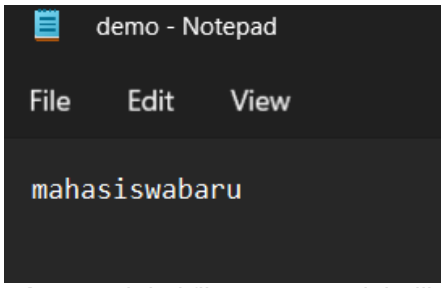
Berikut merupakan rincian dari langkah-langkah pembuatan program:

1. Membuat program berbasis *python* dan memasukkan sintaks yang diperlukan untuk proses enkripsi dan dekripsi menggunakan teknik kriptografi kombinasi dari dua algoritma *Vigenere Cipher* dan *Shift Cipher.* Berikut merupakan beberapa potongan sintaks yang dibutuhkan pada program.

```python
import sys

#Generate key sesuai jumlah karakter text
def generateKey(string, key):
  key = list(key)
  if len(string) == len(key):
    return(key)
  else:
    for i in range(len(string) -len(key)):
      key.append(key[i % len(key)])
  return("" . join(key))

#Enkripsi Vigenere Cipher
def encryptionVigenere(string, key):
  encrypt_text = []
  for i in range(len(string)):
    x = (ord(string[i]) +ord(key[i])) % 26
    x += ord('A')
    encrypt_text.append(chr(x))
  return("" . join(encrypt_text))

#Dekripsi Vigenere Cipher
def decryptionVigenere(encrypt_text, key):
  orig_text = []
  for i in range(len(encrypt_text)):
    x = (ord(encrypt_text[i]) -ord(key[i]) + 26) % 26
    x += ord('A')
    orig_text.append(chr(x))
  return("" . join(orig_text))
```

Gambar 8. Sintaks bahasa pemrograman *python*

2. Masukkan file *.txt* yang telah dibuat ke dalam program yang ingin dieksekusi tersebut yaitu dengan memasukkan nama file tersebut ke dalam program yang sudah dibuat. Isi dari file tersebut akan dijadikan pesan/teks (data) untuk melakukan percobaan penelitian ini. Contoh isi file *.txt* yang telah dibuat yaitu “mahasiswabaru”.



Gambar 9. Isi dari file *.txt* yang telah dibuat

3. Lalu program dapat dijalankan dan dapat melakukan proses enkripsi *Vigenere Cipher* dan *Shift Cipher* terlebih dahulu yaitu dengan memasukkan *key vigenere* (karakter) dan *key shift* (angka/*integer*). Setelah *key* dimasukkan, maka *cipher text* dari *Vigenere Cipher* dapat dibuat dari teks awal dengan *key vigenere*, dan *cipher text* dari *Shift Cipher* dapat dibuat dari *cipher text* hasil *vigenere* sebelumnya dengan key *shift*. Pada program ini, *plain text* dan *key vigenere* wajib dijadikan *uppercase* terlebih dahulu agar lebih mudah dalam melakukan proses enkripsi maupun dekripsi nantinya (karena penulis menggunakan nomor ascii huruf kapital).

```
Plain text mula-mula yang akan di enkripsi : mahasiswabaru
Masukkan key untuk Vigenere Cipher         : udayana
Masukkan key untuk Shift Cipher (angka)    : 6

----Enkripsi Vignere Cipher----

Plain text              : MAHASISWABARU
Key                     : UDAYANA
Enkripsi Vignere Cipher : GDHYSVSQDBYRH


----Enkripsi Shift Cipher----

Plain text (Hasil Enkripsi Vignere) : GDHYSVSQDBYRH
Shift Key                           : 6
Enkripsi Shift Cipher               : MJNEYBYWJHEXN
```

Gambar 10. Output dari proses enkripsi kombinasi algoritma *Vigenere Cipher* dan *Shift Cipher*

4. Lalu program dapat dijalankan dan dapat melakukan proses dekripsi *Vigenere Cipher* dan *Shift Cipher*. Dekripsi merupakan kebalikan dari enkripsi, caranya dengan memasukkan *key vigenere* (karakter) dan *key shift* (angka/*integer*) yang digunakan dalam proses dekripsi. Setelah *key* dimasukkan, maka *plain text* dari *Vigenere Cipher* dapat dibuat dari *cipher* hasil enkripsi sebelumnya dengan *key vigenere*, dan *plain text* dari *Shift Cipher* dapat dibuat dari *text* hasil dekripsi *vigenere* sebelumnya dengan key *shift*. Jika *key vigenere* dan *shift* sesuai dengan *key* enkripsi, maka *plain teks* atau teks awal dapat terlihat kembali.

```
Plain text mula-mula yang akan didekripsi  : MJNEYBYWJHEXN
Masukkan key untuk Vigenere Cipher         : udayana
Masukkan key untuk Shift Cipher (angka)    : 6

----Dekripsi Shift Cipher----

Cipher text (Hasil Enkripsi Shift) : MJNEYBYWJHEXN
Shift Key                          : 6
Dekripsi Shift Cipher              : GDHYSVSQDBYRH


----Dekripsi Vignere Cipher----

Cipher text (Hasil Dekripsi Shift) : GDHYSVSQDBYRH
Key                                : UDAYANA
Decrypted message                  : MAHASISWABARU
```

Gambar 11. Output dari proses dekripsi kombinasi algoritma *Vigenere Cipher* dan *Shift Cipher*

4. Kesimpulan dan Saran

Dari percobaan yang telah dilakukan, maka diperoleh sebuah kesimpulan bahwa dengan adanya ilmu kriptografi klasik contohnya yaitu algoritma *Vigenere Cipher* dan *Shift Cipher* dapat membantu menjaga file ataupun informasi/data di dalamnya agar suatu informasi/data tersebut tidak mudah bocor ke tangan yang tidak berhak. Pengamanan berlapis seperti kombinasi dari algoritma kriptografi klasik *Vigenere Cipher* dengan *Shift Cipher* ini dapat membantu menjaga keamanan data dengan menggunakan *key* yang bersifat unik dan tidak mudah diketahui oleh orang lain karena pengamanan dengan satu metode saja tidak cukup untuk mengamankan suatu informasi/data. Berdasarkan program yang telah dibuat pada bahasa pemrograman *Python 3* yaitu untuk kombinasi algoritma *Vigenere Cipher* dengan *Shift Cipher* pada keamanan data dalam file *.txt* ini, data berhasil dienkripsi maupun didekripsi berdasarkan kunci/*key* yang telah dibuat. Peneliti membuat program ini untuk meminimalisir risiko dalam keamanan data pada saat pengiriman data, sehingga hanya pemilik asli yang dapat melihat atau mendekripsikan file tersebut. Kelemahan dari metode dari peneliti ini yaitu belum bisa mendeteksi karakter *whitespace*. Maka dari itu, peneliti menggunakan sampel berupa kata yang tidak terdapat *whitespace*.

Jadi mengacu pada paragraf kesimpulan diatas, peneliti hanya bisa memberikan pengembangan ke depannya tentang *paper* yang telah peneliti lakukan percobaannya. Maka perkembangan selanjutnya yang dapat dilakukan yaitu menerapkan metode enkripsi dan dekripsi ini pada algoritma kriptografi

klasik maupun modern yang terdapat pada ilmu kriptografi, yang dimana didapatkan hasil penelitian baru dengan maksud memperoleh informasi dan pengetahuan yang lebih baik di masa yang akan datang. Untuk pengembangan program yang telah penulis buat sebaiknya dikembangkan agar metode enkripsi dan dekripsi dengan kombinasi *Vigenere Cipher* dengan *Shift Cipher* ini dapat mendeteksi simbol-simbol serta *whitespace*/spasi yang ada pada tabel *ascii*.

References

[1] Eko Hari Ravhmawanto and Christy Atika Sari, "KEAMANAN FILE MENGGUNAKAN TEKNIK KRIPTOGRAFI SHIFT CIPHER" *Techno.COM,* vol. 14, no. 4, p. 329-335, 2015.

[2] Muhammad Khoiruddin Harahap, “ANALISIS PERBANDINGAN ALGORITMA KRIPTOGRAFI KLASIK VIGENERE CIPHER DAN ONE TIME PAD” *Jurnal Nasional Informatika dan Teknologi Jaringan*, vol. 1, no. 1, p. 61-64, 2016.

[3] Ripto Sudiyarno, "Modifikasi Metode *Base64* Menggunakan *Caesar Cipher* Dan Kunci Rahasia" *JURTI,* vol. 5, no. 01, p. 1-2, 2021.

[4] Salman Farizy and Emi Sita Eriana, KEAMANAN SISTEM INFORMASI, 1ST ed., Tangerang Selatan: Unpam Press, 2022, pp. 1-181.

[5] Septian Widiyanto, Govindu Adnan, Moh. Fatkuroji, Dwi Wahyu Handoyo, and Mhd Arief Hasan, “Pengamanan Pesan Text dengan menggunakan Kriptografi Klasik Metode Shift Chipper dan Metode Subtitution Chipper” *Riau Journal of Computer Science*, vol. 7, no. 1, p. 9-17, 2021.

[6] Soeb Aripin and Muhammad Syahrizal, "Analisis Modifikasi Algoritma Kriptografi Klasik Menggunakan Algoritma Blum-Micali Generator" *Jurnal Sains Komputer & Informatika (J-SAKTI),* vol. 6, no. 1, p. 136-147, 2022.

[7] Tomy Satria Alasi and Pristiwati Fitriani, “Peningkatan Keamanan untuk Password menggunakan Algoritma Vigenere Cipher" *Jurnal Mantik Penusa*, vol. 6, no. 1, p. 1-10. 2022.

This page is intentionally left blank.