SATIN – Sains dan Teknologi Informasi
Journal Homepage : http://jurnal.sar.ac.id/index.php/satin

Enkripsi dan Deskripsi File Menggunakan Kombinasi Vigenere dan Shift Cipher di Python

Megawati[1], Muhammad Fitra Hamidy[2], Sasqia Ismi Aulia[3], Yuhendri Putra[4], Mhd Arief Hasan, M. Kom[5]
[1]Universitas Lancang Kuning, megaaw08@gmail.com, Jl. Yos Sudarso KM. 8 Rumbai , Pekanbaru, Indonesia
[2]Universitas Lancang Kuning, fitrahamidy99@gmail.com, Jl. Yos Sudarso KM. 8 Rumbai , Pekanbaru, Indonesia
[3]Universitas Lancang Kuning, saskiaaulia99@gmail.com, Jl. Yos Sudarso KM. 8 Rumbai , Pekanbaru, Indonesia
[4]Universitas Lancang Kuning, yuhendri204@gmail.com, Jl. Yos Sudarso KM. 8 Rumbai, Pekanbaru, Indonesia
[5]Universitas Lancang Kuning, m.arif@unilak.ac.id, Jl. Yos Sudarso KM. 8 Rumbai, Pekanbaru, Indonesia

Informasi Makalah

Submit : Jan 1, 2021
Revisi : May 31, 2021
Diterima : Juni 16, 2021

Kata Kunci :

Kriptografi
Vigenere Cipher
Shift Cipher
File
Enkripsi
Deskripsi

Abstrak

Penelitian ini bertujuan untuk menerapkan sistem super enkripsi dan deskripsi pada keamanan data file yang sesuai dengan aturan yang digunakan. Untuk mangatasi kesalahan pada proses super enkripsi dan deskripsi ini dapat dilakukan dengan algoritma kriptografi yaitu menerapkan kombinasi Vigenere Cipher dan Shift Cipher pada keamanan data file txt. Algoritma Vigenere Cipher dan Shift Cipher adalah salah satu algoritma dalam Kriptografi klasik. Algoritma ini di pilih karena mampu melakukan super enkrispi dan deskripsi pada keamanan data file txt. Penelitian ini dilakukan dengan mengubah isi file txt menjadi sandi acak (file enkripsi) untuk menjaga keamanan data dari orang yang tidak berhak, dan hanya pemiliknya yang bisa mengembalikan menjadi data file aslinya (deskripsi). Hasil penelitian yang di dapat dari kombinasi super enkripsi dan deskripsi ini diharapkan agar sistem yang dibuat dapat membantu dan menjaga keamanan data file sebelum proses mengirim data dilakukan dalam lingkup perusahaan, supaya pesan tetap rahasia sampai ke tangan orang yang berhak.

Abstract

This study aims to implement a super encryption system and a description of the data file security in accordance with the rules used. To resolve errors in the super encryption and description process, it can be done with a cryptographic algorithm, namely applying a combination of Vigenere Cipher and Shift Cipher on txt file data security. The Vigenere Cipher and Shift Cipher algorithms are one of the algorithms in classical cryptography. This algorithm was chosen because it is able to perform super encryption and description of the txt file data

Sasqia Ismi Aulia
Email: saskiaaulia99@gmail.com

security. This research was conducted by changing the contents of the txt file into a random password (file encryption) to maintain data security from unauthorized persons, and only the owner can restore the original file data (description). The research results obtained from the combination of super encryption and description are expected so that the system created can help and maintain the security of data files before the process of sending data is carried out within the scope of the company, so that messages remain secret in the hands of the entitled people.

1. Pendahuluan

Semakin canggihnya teknologi pada masa sekarang ini membuat manusia bertukar informasi menjadi semakin luas dan cepat. Salah satunya data berupa text, oleh sebab itu semakin banyak pengguna memanfaatkan teknologi semakin rentan pula keamanan informasi tersebut disalah gunakan oleh pihak yang tidak dikenal.

Sehingga di butuhkan keamanan agar data yang dimiliki tidak disalah gunakan, oleh karena itu diperlukan ilmu untuk mengamankan data misalnya berupa text,file,foto,dll. Keamanan data sendiri menjadi masalah isu yang penting untuk menjaga kerahasiaan dari suatu lembaga, perusahaan, ataupun pribadi dari orang yang tidak berhak. (Qilla Aulia Suri, 2019)

File merupakan suatu unit sebuah data yang disimpan dalam sistem dan bisa diatur perubahannya dan diakses hak pakai oleh pengguna. suatu file memiliki identitas yang berbeda dalam penyimpanan di mana letaknya. Lokasi untuk direktori pada suatu berkas ditempatkan disebut dengan path.

File seperti aliran data yang berisi suatu kumpulan data yang berhubungan, sedangkan atribut pada berkas disebut properties yang berisi informasi mengenai file yang tersebut seperti informasi mengenai kapan sebuah berkas dibuat.

Agar kemanannya terjaga maka ilmu yang dikembangkan untuk menjaga kemanan data tersebut adalah kriptografi. Kriptografi merupakan suatu teknik yang mempelajari cara menjaga informasi baik berupa file ataupun pesan agar terjaga keamanan saat melakukan pengiriman, oleh pihak yang mengirim ke pihak yang menerima dengan aman sehingga tidak ada gangguan dari pihak yang lain (Azlin et al., 2018). Teknik kriptografi juga berhubungan dengan aspek keamanan informasi seperti integritas data, autentikasi data, kerahasiaan data, dan keabsaan data (Efrand, Asnawati, 2014).

Seorang ahli ilmu kriptografi biasanya disebut dengan Cryptographers. Sebuah algoritma kriptografi disebut dengan cipher, yang merupakan persamaan matematik atau suatu sistem yang digunakan pada proses enkripsi dan deskripsi (Lestari & Riyanto, 2012).

Supaya mengamankan data agar terjaga kerahasiaanya, kriptografi bisa merubah plaintext (pesan asli) kedalam bentuk ciphertext (kata sandi) supaya isi pesan yang ingin kita amankan tidak dapat diketahui oleh pihak manapun kecuali orang yang berhak (WM et al., 2018). Teknik kriptografi mempunyai 2 cara yaitu dengan teknik klasik dan teknik modern, untuk klasik seperti Caesar cipher, permutasi, transposisi, shift cipher dan vigenere cipher (Rachmawanto et al., 2015). Ada beberapa cara untuk mengamankan data menggunakan ilmu kriptografi salah satunya yaitu menggabungkan algoritma vignere cipher dan shift cipher untuk mengamankan data agar tidak mudah diretas oleh pihak yang tidak dikenal. (Sinaga, 2017)
(Azis, 2018)Prinsip – prinsip yang mendasari kriptografi, yaitu:

Sasqia Ismi Aulia
Email: saskiaaulia99@gmail.com

SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 102-111
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.686

a) Confidentiality, yaitu informasi atau data hanya diakses oleh pihak penerima/berwenang.
b) Authentication, yaitu teknik dengan menyatakan bahwa informasi tersebut benar-benar asli atau pengirim maupun penerima mengetahui bahwa informasi/pesan yang dikirim benar-benar berasal orang yang dimaksud.
c) Integrity, yaitu suatu jaminan bahwa informasi tidak boleh dimanipulasi tanpa izin dari pemilik informasi tersebut untuk dikirim ke penerima
d) Nonrepudiation, yaitu layanan penyangkalan yang tujuannya agar seseorang tidak dapat mengelak bahwa dialah telah mengirimkan atau menerima informasi tersebut.
e) Access Control, yaitu membatasi kapasitas sumber informasi untuk orang lain yang berwenang.
f) Availability, yaitu berhubungan dengan ketersediaan data/informasi ketika dibutuhkan

Untuk proses enkripsi dan deskripsi membutuhkan kunci untuk terjadinya transformasi. Algoritma kriptografi yang lain, yaitu vigener cipher, shift cipher, affine cipher, roti13, hill cipher, AES, DES, dll. (Syapriadi et al., 2013).

Kode Vigenere termasuk ke dalam Polyalphabet Substitution Cipher yang diperkenalkan dari duta France, Blaise de Vigenere saat abad ke-16 1586. Algoritma jenis ini disangat dikenal karena sederhana dan mudah diimplementasikan. Algoritma Vigenere sendiri untuk caranya dapat menggunakan bujur sangkar maupun substitusi angka. Vigenere Cipher dikenal luas dan cara kerjanya mudah dipahami dan sandinya cukup sulit dipecahkan.

Menurut Gede Angga Pradita (Pradipta, 2016) untuk meningkatkan keamanan pada algoritma vigenere agar lebih sulit untuk dipecahkan dikarenakan ciphertext yang dihasilkan ketika diawal akan melalukan enkripsi dengan cara merubah posisi pada bagian karakter dengan cara tranposisi.

Sedangkan menurut Jesmon dan Zekson (Simangunsong & Matondang, 2008) untuk pengamanan informasi/data pada pesan rahasia dapat melakukan enkripsi dan deskripsi pada file teks atau menggunakan kunci berlapis 3 dengan menginput 46 karakter yang ada.

Shift cipher adalah kembangan Caesar Cipher yang sederhana dan banyak digunakan. Shift Cipher termasuk bagian substitusi, dimana pada huruf plaintextnya digantikan oleh huruf lain yang posisinya tetap pada alfabet. Shift Cipher memakai jenis enkripsi dengan pergeseran sejumlah kunci yang sama dengan Caesar cipher tetapi shift cipher lebih aman daripada Caesar cipher. Perubahan Shift Cipher ini juga dapat diterapkan dengan menyesuaikan kunci plaintext dengan ciphertext pada banyak jumlah pergeseran yang terjadi.

Menurut Ibnu Utomo, Ajib Susanto, dll. (WM et al., 2018) Pada penelitian tersebut menggunakan uji coba perhitungan PSNR. Yang bertujuan untuk membuat histogram gambar asli dengan histogram gambar deskripsi tidak berbeda, sehingga hasil enkripsi nya sama sekali tidak bisa dibaca atau dikenali secara visual. Dan saat melakukan dekripsi kualias pada gambar tidak merubah pixel pada gambar aslinya.

Selanjutnya penelitian yang dilakukan oleh Imam Wahyu Utomo dkk (Utomo et al., 2018). Untuk proses pengujian dilakukan berbagai teks dan kunci yang berbeda agar mudah mengetahui apakah algoritma yang dipakai dapat melakukan proses enkripsi dan deskripsi dengan sesuai. Ketepatan suatu enkripsi dan deskripsi juga berlaku untuk semua jenis teks dengan kunci yang berbeda-beda, jika terdapat suatu teks yang berbeda karakter atau tidak sesuai karakter maka tidak dapat diproses.

SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 102-111
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.686

Pada kasus ini data yang diamankan berupa data file txt. Dimana proses mengelola data tersebut yaitu data file yang ada di enkipsi dengan algoritma Vignere Cipher dan hasil enkripsi tersebut akan di enkripsikan kembali dengan algoritma Shift Cipher untuk menghasilkan ciphertext baru pada file tersebut yang bertujuan untuk menjaga keamanan data tersebut. Tujuan dari penelitian ini untuk membuat aplikasi keamanan data file pada kombinasi algoritma vigenere cipher dan algoritma shift cipher yang diimplementasikan pada Python 3 dimana orang lain tidak akan tahu isi dari file tersebut kecuali pemiliknya.

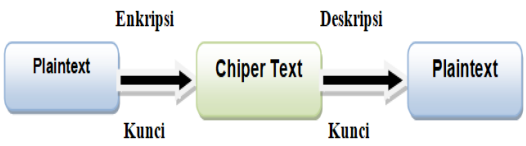
Adapun manfaatnya yaitu :

a) Memahami cara mengubah enkripsi dan deskripsi begitupun sebaliknya dengan menggunakan metode vigenere cipher dan shif cipher.
b) Memberikan tingkat keamanan atau kerahasiaan dalam komunikasi ataupun informasi.
c) Menerapkan dan mengaplikasikan ilmu pengetahuan yang kami dapatkan.

Maka sesuai penjelasan latar belakang tersebut peneliti menetapkan judul **"Enkripsi dan Deskripsi File Menggunakan Kombinasi Vigenere dan Shift Cipher di Python".**

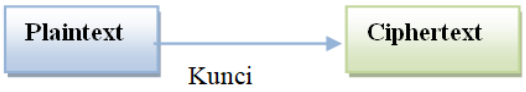
2. Metode Penelitian

2.1 Teknik Enkripsi dan Deskripsi yang digunakan



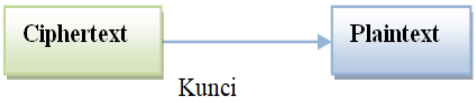
Gambar 1. Ilustrasi proses enkripsi dan deskripsi

Proses pada teknik kriptografi ini menggunakan konsep enkripsi dan deskripsi untuk penyelesaian kasusnya. Enkripsi adalah suatu teknik penyandian data yang hanya bisa di buka dengan cara proses deskrpsi (Budiman & Noviardi, 2016). Enkripsi dilakukan pada perubahan suatu kode atau teks yang mudah di pahami, disebut plaintext, menjadi sebuah sandi acak yang sulit dipahami, disebut ciphertext.



Gambar 2. Ilustrasi enkripsi

Sedangkan proses deskripsi merupakan kebalikan dari proses enkripsi yaitu merubah kembali bentuk kode yang tidak bisa dimengerti atau disebut chipertext ke bentuk semula atau pesan yang bias dimengerti, disebut dengan plaintext dengan menggunakan kunci yang ada sesuai aturan algoritma yang digunakan.



Gambar 3. Ilustrasi deskripsi

2.2 Algoritma Vigenere Cipher

Pada penelitian ini akan dilakukan penggabungan metode Vigenere Cipher dan Shift cipher. Dalam teknik kriptogarfi jenis algoritma ini sebelumnya dikembangkan dari algoritma caesar, pada penelitian berikut untuk hasil enkripsi dan dekripsi pertama kali dilakukan dengan algoritma Vigenere Cipher dan dilanjutkan dengan algoritma Shift Cipher. Penerapan metode vigenere cipher ini menggunakan 26 huruf alphabet dari A sampai Z. Jika banyak panjang suatu key nya sangat rendah dibandingkan panjang plainteks, oleh karena itu kunci akan diulang terus menerus padakalanya. (Sasongko, 2005)

SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 102-111
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.686

Rumus :

a) Enkripsi

c_i = (p_i + k_i)modulo 26

b) Deskripsi

p_i = (c_i - k_i)modulo 26

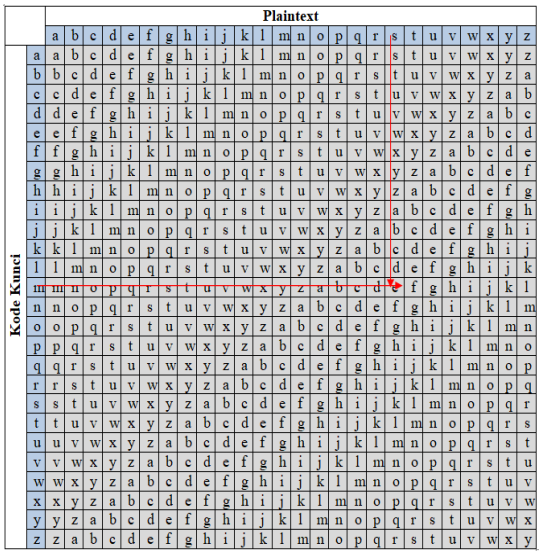
Keterangan :

C_i = nilai dari karakter cipherteks

P_i = nilai dari karakter plaintext

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

Untuk melakukan proses enkripsi plaintext dan deskripsi algoritma vigenere cipher bisa menggunakan bujur sangkar vigenere atau polatabula recta, yang berguna untuk memudahkan suatu proses berlangsung. (Qilla Aulia Suri, 2019)



Gambar 4. Polatabula recta kode vigener (huruf)

Contoh :

Plaintext : **SAYA PASTI BISA**

Kunci : **M A H A S I S W A**

Maka cara menentukan chipertext-nya adalah:

PLAINTEXT	S	A	Y	A	P	A	S	T	I	B	I	S	A
KUNCI	M	A	H	A	S	I	S	W	A	M	A	H	A
CIPHERTEXT	E	A	F	A	H	I	K	P	I	N	I	Z	A

Gambar 5. Hasil kriptografi kode vigener (huruf)

2.3 Algoritma Shift Cipher

Shift cipher adalah salah satu algoritma klasik bagian dari monoalpabet, shift cipher menggunakan 26 kunci pergeseran sehingga algoritma ini lebih aman (WM et al., 2018). Algoritma ini menggunakan sisa pembagian pada perhitungan yang dilakukan, dan untuk proses penyandiannya menggunakan operasi modulo 26.(Rachmawanto et al., 2015)

Rumus :

a) Enkripsi :

$$C = E(P) = (P + K)\ Mod\ 26$$

b) Deskripsi :

$$P = D(C) = (C - K)\ Mod\ 26$$

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 6. Contoh kriptografi metode kode geser

Perhatikan contoh dibawah ini:

Plaintext : **BELAJAR KRIPTOGRAFI KLASIK**

Plaintext diatas diubah menjadi bilangan atau angka yaitu:

B	E	L	A	J	A	R	K	R	I	P	T	O	G	R	A	F	I	K	L	A	S	I	K
1	4	11	0	9	0	17	10	17	8	15	19	14	6	17	0	5	8	9	11	0	18	8	10

Gambar 7. Contoh metode kode geser ke angka

Kode Kunci : **5**

Caranya yaitu dengan menambahkan angka pada plaintext dan kunci 5.Maka hasilnya:

B	E	L	A	J	A	R	K	R	I	P	T	O	G	R	A	F	I	K	L	A	S	I	K
1	4	11	0	9	0	17	10	17	8	15	19	14	6	17	0	5	8	9	11	0	18	8	10
6	9	16	5	14	5	22	15	22	13	20	24	19	11	22	5	10	13	14	16	5	23	13	15
G	K	Q	F	O	F	W	P	W	N	U	Y	T	L	W	F	K	N	O	Q	F	X	N	P

Gambar 8. Hasil kriptografi metode kode geser

Jika hasil yang dijumlahkan lebih dari 26, maka hasil dikurangi 26. Misalnya: 24 + 12 = 36 – 26 = 10. Selanjutnya hasil penjumlahan dikonversi menjadi huruf sesuai

SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 102-111
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.686

dengan nilai standar setiap huruf. (Rambe, 2019)

2.4 Kombinasi Vigenere dan Shift Cipher

Teknik penyandian data file .txt di mulai dengan menggunakan vigener cipher, kemudian hasil enkripsi vigener di enkripsi lagi menggunakan shift cipher sehingga terbentuk keamanan dua algoritma kriptografi. Dan untuk megembalikan file txt agar terbaca lakukan dekripsi menggunakan algoritma yang sama dengan kunci yang sama.

Jadi, prinsip kombinasi vigener dan shift adalah:

Enkripsi

P $\longrightarrow$ E(Vigener) = C(Vigener)

P(C Vigener) $\longrightarrow$ E(Shift) = C (Shift)

Deskripsi

C(Shift) $\longrightarrow$ D(Shift) = P(Shift)

C(P Shift) $\longrightarrow$ D(Vigener) = P (awal).

2.5 Phyton

Python merupakaan suatu bahasa program yang interpretative dan serbaguna yang model rancangannya hanya ditujukan di suatu tingkatan terbacanya syntax atau code. Python sendiri dikenal dengan suatu fitur dengan mengkombinasikan kemampuan, kapasitas, pada sintaks code yang jelas, serta dilengkapi dengan fungsionalitas dan juga komprehensif. Python merupakan bahasa pemrograman yang mendukung multi paradigma, seperti halnya program orientasi objek, pemrograman imperatif, dan pemrograman fungsional.

Bahasa python banyak dipakai untuk script walaupun untuk prakteknya penggunaan cakupan python ini lebih luas dalam segi kegunaan seperti pada biasanya tidak gunakan dengan penggunaan bahasa pemograman jenis script. Bahasa pemogrman ini sendiri banyak dipakai dalam perkembangan pada perangkat lunak supaya bisa dijlankan berbagai jenis system operasi. Untuk itu bahasa pemograman ini disalurkan pada banyak model izin yang terdapat perbedaan dengan jenis versinya. Aplikasi python bisa didapatkan dan digunakan dengan mudah dan bebas, contohnya untuk kebutuhan seperti berniaga. Untuk lisensinya bahasa pemograman ini berbentuk Open Source dan tidak bertentangan dengan GPL(General Public License).(Syahrudin & Kurniawan, 2018). Fitur dari python sendiri banyak baik itu dalam memfasilitasi tools dan library yang ada serta penggunaan bahasa yang digunakan sangan membantu dalam membuat suatu sistem yang dapat dikembangkan untuk penggunaan skala lingkup besar seperti pengolaan big data dan pengolahan data pada teknik kriptografi.

3. Hasil dan Pembahasan

3.1 Analisa Pembahasan

Dalam melakukan proses enkripsi dan deskripsi kombinasi teknik kriptografi klasik antara algoritma viginere cipher dan algoritma shift cipher pada file txt maka bisa menggunakan bahasa pemograman python yang dapat membantu dalam menyelesaikan percobaan kombinasi algoritma tersebut. Oleh karena itu untuk melakukan percobaan tersebut terlebih dahulu memasukan script atau file yang yang dibutuhkan untuk melakukan proses enkripsi dan deskripsi sesuai dengan syntax yang terdapat pada bahasa pemograman python.

Kemudian menentukan pesan yang ingin dikirim pada file txt dan ini nantinya sebagai plaintext. Kemudian melakukan proses enkripsi dengan kunci misalnya bulan lahir untuk enkripsi viginere cipher dan tanggal lahir untuk kunci shift cipher sehingga dapat menghasilkan ciphertext dari pesan tersebut. Maka untuk proses deskripsinya yaitu dengan menggunakan kunci yang sama seperti proses enkripsi sebelumnya sehingga dapat

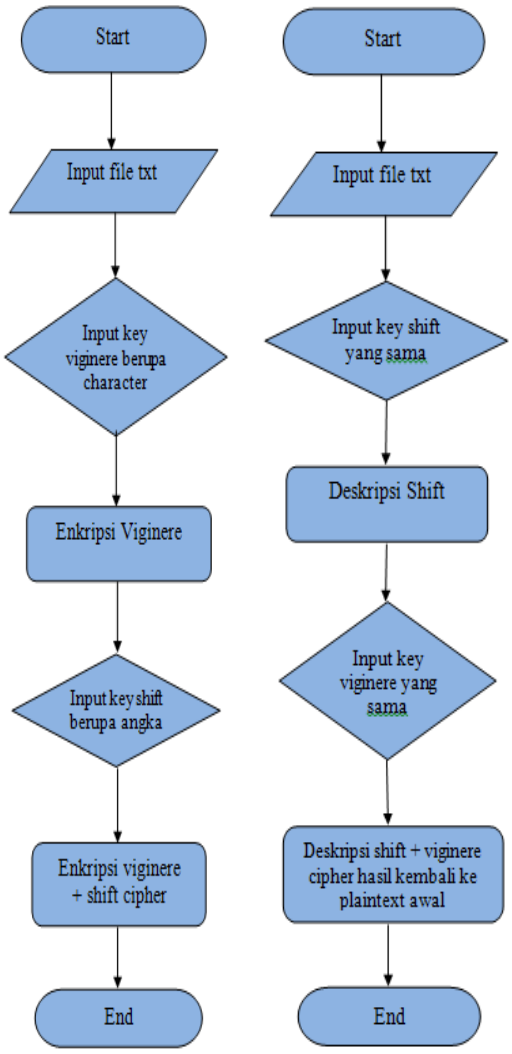
SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 102-111
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.686

menghasilkan pesan semula atau plaintext dari kombinasi kedua algoritma tersebut.

3.2 Alur Proses Enkripsi dan Deskripsi File txt

Proses untuk melakukan super enkripsi dan deskripsi dengan menggunakan kombinasi algoritma vigenere cipher dan algoritma shift cipher.

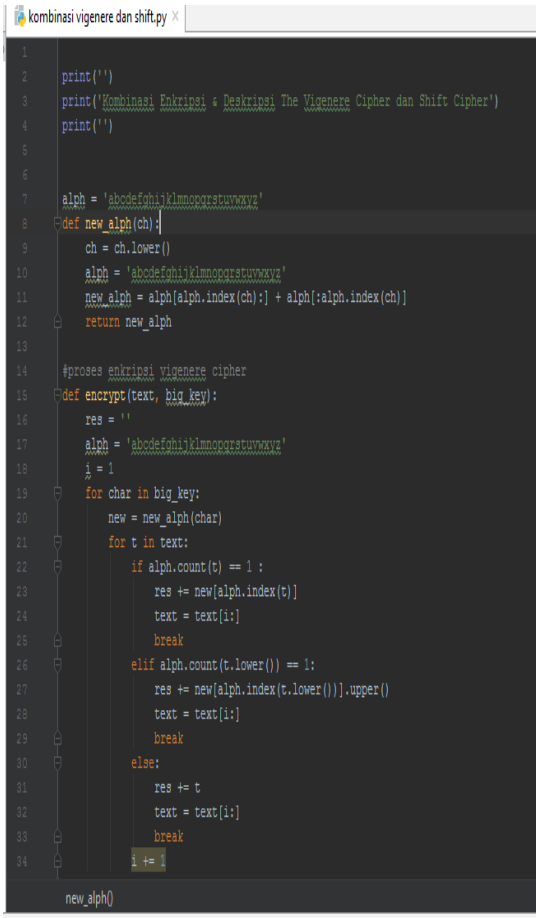
Flowchart ini bertujuan untuk membantu dalam membuat suatu perancangan sebelum melakukan proses super enkripsi dan deskripsi pada pengolahan data file txt ke dalam sistem yang dibuat.



Gambar 9. Flowchart proses enkripsi dan dekripsi

Langkah – langkahnya, yaitu :

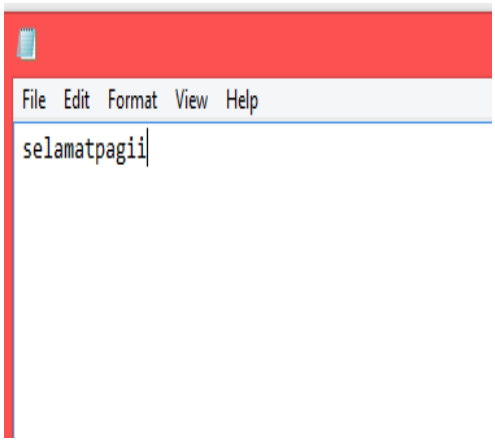
1. Memasukan syntax-syntax pada python yang sesuai dengan apa saja yang dibutuhkan oleh pengguna untuk melakukan proses enkripsi dan deskripsi pada teknik kriptografi menggunakan kombinasi algoritma vigenere cipher dan algoritma shift cipher (gambar dibawah ini merupakan beberapa potong bagian syntax yang butuhkan)



Gambar 10. Syntax pada bahasa pemograman python

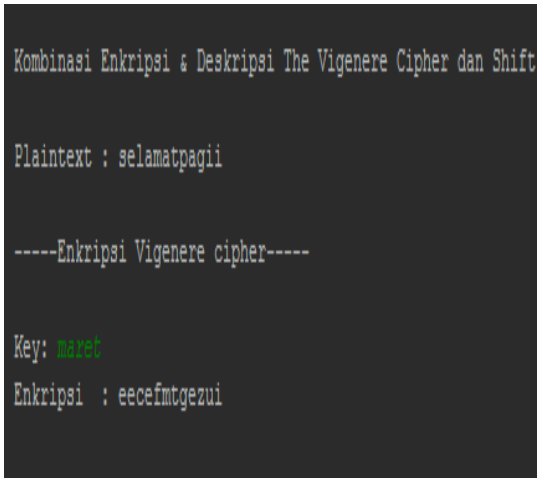
2. Input file txt yang ada ke dalam sistem yang ingin dieksekusi yaitu dengan memasukkan nama file tersebut ke dalam sistem yang sudah dibuat, file tersebut akan dijadikan pesan (data) untuk melakukan percobaan ini. Isi file txt pada notepad yaitu **selamatpagii.**

SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 102-111
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.686



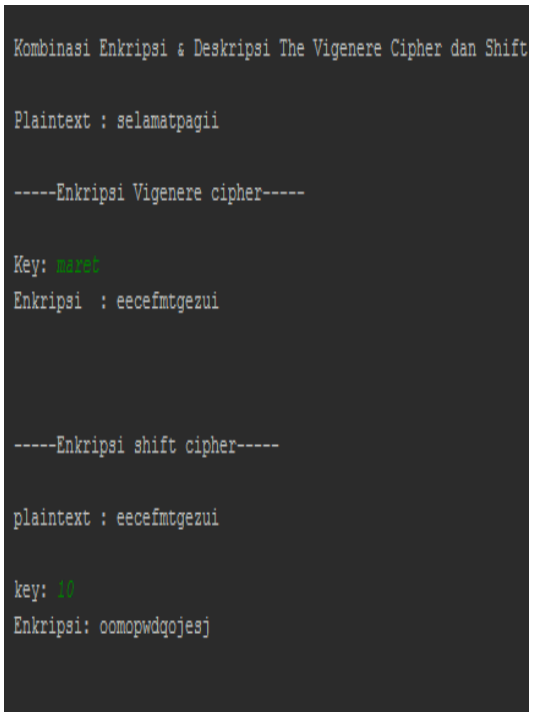
Gambar 11. File txt di notepad

3. Kemudian lakukan proses enkripsi vigenere cipher yaitu dengan memasukan kunci bulan lahir misalnya:
   Kunci: **maret**, maka hasil ciphertext yang didapat yaitu: **eecefmtgezui**



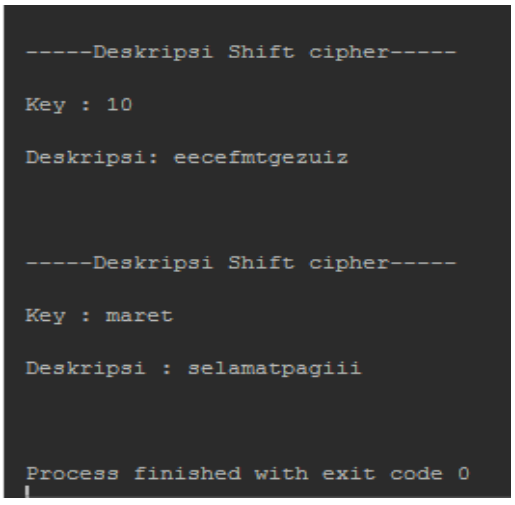
Gambar 12. Proses enkrpsi viginere cipher di python

4. Selanjutnya lakukan proses enkripsi shift cipher dengan ciphertext yang sudah didapatkan dari proses enkripsi Vigenere sebagai plaintextnya kemudian memasukan kunci tanggal lahir misalnya:
   Kunci: **10**, maka menghasilkan ciphertext : **oomopwdqojesj**



Gambar 13. Proses shift cipher di python

5. Kemudian pada tahap untuk proses deskripsi yaitu dengan menggunakan kunci yang sama pada proses enkripsi sebelumnya dengan kombinasi algoritma vigenere cipher dan algoritma shift cipher, maka dapatlah pesan aslinya kembali atau plaintextnya yaitu **selamatpagii.**



Gambar 14. Proses deskripsi vigenere dan shift cipher di python

SATIN – Sains dan Teknologi Informasi
Vol. 07, No. 01, Juni 2021, pp. 102-111
ISSN: 2527-9114, DOI 10.33372/stn.v7i1.686

4. Penutup

4.1 Kesimpulan

Maka dari percobaan yang sudah dilakukan, jadi diperoleh sebuah kesimpulan yaitu dengan adanya Kriptogarafi klasik yaitu Algoritma Vigenere Cipher dan Shift Cipher dapat membantu menjaga agar suatu data atau informasi tidak bocor ke tangan yang tidak berhak. Berdasarkan sistem yang dibuat pada aplikasi python 3 yaitu untuk kombinasi algoritma vigenere dan shift cipher pada keamanan data file txt, data berhasil dienkripsi dan dideskripsi berdasarkan kunci yang sama. Sistem ini di buat untuk meminimalisir resiko dalam keamanan data pada saat pengiriman, sehingga hanya pemilik aslinya yang tahu untuk mendeskripsi kan file txt tersebut

4.2 Saran

Jadi mengacu pada kesimpulan dan saran yang didapatkan, peneliti hanya bisa memberikan pengembangan ke depannya tentang paper yang telah peneliti lakukan percobaan. Maka perkembangan untuk selanjutnya dapat diterapkan pada algoritma kriptografi klasik maupun modern yang terdapat pada ilmu kriptografi, dimana didapatkan hasil penelitian baru dengan maksud memperoleh informasi dan pengetahuan yang lebih baik di masa yang akan datang

5. Referensi

Azis, N. (2018). Perancangan Aplikasi Enkripsi Dekripsi Menggunakan Metode Caesar Chiper Dan Operasi Xor. Ikraith-Informatika, 2(1), 1–9.

Azlin, Musadat, F., & Nur, J. (2018). Aplikasi Kriptografi Keamanan Data Menggunakan Algoritma Base64. Jurnal Informatika, 7(2), 1–5.

Budiman, A., & Noviardi. (2016). Penerapan Keamanan Penggunaan Data Pada Database Kepegawaian Menggunakan Teknik Transparent Data Encryption (Studi Kasus Sekolah Tinggi Teknologi Payakumbuh). Satin-Sains Dan Teknologi Informasi, 2(2).

Efrand, Asnawati, Y. (2014). Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher. Jurnal Media Infotama, 10(2), 120–128.

Lestari, D., & Riyanto, M. Z. (2012). Suatu Algoritma Kriptografi Stream Cipher Berdasarkan Fungsi Chaos. November, 1–9.

Pradipta, G. A. (2016). Penerapan Kombinasi Metode Enkripsi Vigenere Chiper Dan Transposisi Pada Aplikasai Client Server Chatting. Jurnal Sistem Dan Informatika, 10(2), 119–127.

Qilla Aulia Suri, A. M. G. (2019). Fakultas Teknik – Universitas Muria Kudus. Prosiding Snatif Ke-6 Tahun 2019, 2007, 96–101.

Rachmawanto, E. H., Sari, C. A., & Kunci, K. (2015). Keamanan File Menggunakan Teknik Kriptografi Shift Cipher. Jl. Nakula Semarang, 14(50131024), 329–335.

Rambe, A. (2019). Modifikasi Metode Affine Ciphers Pada Kriptografi Klasik. Ready Star, 2(1), 256–261.

Sasongko, J. (2005). Pengamanan Data Informasi Menggunakan Kriptografi Klasik. Jurnal Teknologi Informasi Dinamika, X(3), 160–167.

Simangunsong, J., & Matondang, Z. A. (2008). Modifikasi Algoritma Vigenere Cipher Untuk Pengamanan Pesan Rahasia. Jurnal Kontol, 1(2), 1–5.

Sinaga, M. C. (2017). Kriptografi Dan Python. Https://Doi.Org/10.31227/Osf.Io/6su2h

Syahrudin, A. N., & Kurniawan, T. (2018). Input Dan Output Pada Bahasa Pemrograman Python. Jurnal Dasar Pemrograman Python Stmik, January, 1–7.

Syapriadi, Rahmiati, & Erlinda, S. (2013). Implementasi Sistem Keamanan Data Untuk Semua Jenis File Dengan Menggunakan Teknik Steganografi End Of File (Eof) Dan Algoritma Kriptografi Rivest Code 4 (Rc4). Sains Dan Teknologi Informasi, 2(2), 14.

Utomo, I. W., Latifah, R., & Risanty, D. (2018). Aplikasi Kriptografi Berbasis Android Menggunakan Algoritma Caesar Cipher Dan Vigenere Cipher. Jurnal Sistem Informasi, Teknologi Informasi Dan Komputer, 9(2), 142–149.

Wm, I. U., Susanto, A., Rachmawanto, E. H., & Setiadi, D. R. I. M. (2018). Fakultas Teknik – Universitas Muria Kudus. Prosiding Snatif Ke-5 Tahun 2018, 379–384.