Journal on Education
Volume 05, No. 03, Maret-April 2023, pp. 8563-8573
E-ISSN: 2654-5497, P-ISSN: 2655-1365
Website: http://jonedu.org/index.php/joe

Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks

Vara Maulidyah Hidayah[1], Dadang Iskandar Mulyana[2], Yuliana Bachtiar[3]

[1,2,3]STIKOM CKI, Jl. Raden Inten II No.8, RT.5/RW.14, Duren Sawit, Kec. Duren Sawit, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta
varamaulidya456@gmail.com

Abstract

Cryptography is a science that studies information security on data with the aim of preventing other people from wanting to know its contents, by using certain codes and rules and other methods so that only authorized people can see the contents of the code. By creating an application which uses the Java programming language with NetBeans to maintain the security of text input information sent by someone so that it is not easy to read, confidential text. The caesar algorithm is a classic substitution-based cipher system that is simple in encryption and decryption of a caesar cipher system using shift operations. The Vigenere Cipher algorithm is a classic cryptographic algorithm that utilizes the vigenere square principle to perform encryption.
Keywords: Cryptography, Caesar Chipper, Vigenere Cipher, Text Input

Abstrak

Kriptografi merupakan ilmu yang mempelajari cara keamanan informasi terhadap data dengan tujuan mencegah dari orang lain yang ingin mengetahui isinya, dengan menggunakan kode-kode dan aturan-aturan tertentu dan metode lainnya sehingga hanya orang yang berhak untuk dapat melihat isi kode tersebut.Dengan membuat suatu aplikasi yang menggunakan bahasa pemrograman java dengan netbeans untuk menjaga keamanan Informasi Penginputan text yang dikirim seseorang agar tidak mudah terbaca, teks yang rahasia. Algoritma caesar merupakan sistem persandian klasik berbasis subtitusi yang sederhana pada enkripsi dan dekripsi sebuah sistem persandian caesar menggunakan operasi shift.Algoritma Vigenere Cipher merupakan salah satu algoritma kriptografi klasik yang memanfaatkan prinsip bujursangkar vigenere untuk melakukan enkripsi.
Kata Kunci: Kriptografi, Caesar Chiper, Vigenere Cipher, Penginputan text

✉ Corresponding author: Vara Maulidyah Hidayah
Email Address: varamaulidya456@gmail.com (Jl. Raden Inten II No.8, RT.5/RW.14, Duren Sawit, Kec. Duren Sawit, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta)
Received 01 February 2023, Accepted 10 February 2023, Published 11 February 2023

PENDAHULUAN

Keamanan biasanya digambarkan sebagai kebebasan dari bahaya atau sebagai kondisi keselamatan. Keamanan komputer, secara rinci adalah perlindungan data di dalam suatu sistem melawan terhadap otorisasi tidak sah, modifikasi, atau perusakan dan perlindungan sistem komputer terhadap penggunaan tidak sah atau modifikasi. Keamanan informasi adalah cabang studi dari teknologi informasi yang mengkhususkan diri untuk mempelajari metode dan teknik untuk melindungi informasi dan sistem informasi dari akses, penggunaan, penyebaran, perusakan, perubahan, dan penghancuran tanpa otorisasi yang sah.

Ada beberapa cara melakukan pengamanan data ataupun pesan, diantaranya adalah dengan menggunakan teknik penyamaran data yang disebut dengan kriptografi dan teknik penyembunyian data yang disebut dengan steganografi.

Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan.

Dalam kriptografi, data atau pesan yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa. Sehingga seandainya data tersebut bisa diperoleh dan dibaca oleh orang lain, maka pihak yang tidak berhak atau berwenang tersebut tidak akan bisa mengerti arti dari data tersebut. Dalam bidang kriptografi terdapat dua konsep yang sangat penting atau utama yaitu enkripsi dan dekripsi. (Lestari et al., n.d.)

Kriptografi (cryptography) berasal dari bahasa Yunani: "cryptos" artinya "secret" (rahasia), sedangkan "graphein" artinya "writing" (tulisan). Jadi, kriptografi berarti "secret writting" (tulisan rahasia). Ada beberapa defenisi kriptografi yang telah dikemukakan didalam berbagai literatur [Kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.

Caesar Chipper adalah sebuah algoritma yang digunakan termasuk ke dalam sistem kriptografi simetri dan digunakan jauh sebelum sistem kriptografi kunci publik ditemukan, kriptografi klasik yang ada dan beberapa bentuk algoritma klasik tersebut sudah tidak trend (dianggap tidak optimal) karena mudah dipecahkan. Tetapi dalam belajar dasar kriptografi, metode klasik adalah dasar yang sangat bagus untuk melanjutkan ke dalam pengembangan kriptografi modern khususnya dalam pembinaan penalaran logika berpikir. Beberapa alasan mengapa penting mempelajari algoritma kriptografi klasik antara lain 1) Untuk memberikan pemahaman konsep dasar kriptografi; 2) Dasar pengembangan algoritma kriptografi modern; 3) Dapat memahami potensi-potensi kelemahan sistem chiper. Ilmu kriptografi terletak pada proses logika saat untuk proses enkripsi dan dekripsi dimana proses tersebut sebaiknya dibuktikan bukan hanya sekedar teoritis saja yang nanti para pengguna dapat mengembangkan proses dasar dari caesar chiper ini menjadi sebuah kriptografi modern. untuk menguji sebuah proses logika diperlukan sebuah software penguji.

Kelemahan dari caesar chipper ini adalah tidak dapat mengenkrip ataupun mendekrip pesan yang terdiri dari beberapa kata atau kalimat, dan juga dengan rumus yang disediakan yaitu posisi huruf ditambah angka round (kunci) dibagi 26 dan sisa baginya adalah posisi huruf pesan yang disandikan (pesan baru) dimana dapat dijelas dilihat posisi huruf awal adalah angka 1 (satu) sedangkan 26 Mod 26 sisanya adalah 0 (nol) maka pesan yang akan disandikan tidak akan pernah ditemukan dan perlu juga dipahami bahwa pesan itu tidak pernah terdiri dari satu kata sehingga spasi tidak bisa dimasukkan.

Dalam penulisan ini dibuat sebuah aturan tambahan untuk mengatasi kelemahan dalam penulisan jarak dari kata ke kata ('spasi') dengan mengubah hasil mod dari 26 menjadi 27, dan untuk mengatasi index 0 (nol) maka dibuat sebuah kondisi jika hasil mod adalah 0 maka posisi pesan yang disandikan adalah posisi huruf ditambah round (kunci). Proses ini akan diuji dengan menggunakan Matlab R2010a dengan memberikan contoh visualisasi grafiknya menggunakan fasilitas figure yang disediakan oleh aplikasi matlab tersebut. (Minarto & Khairuzzaman, n.d.)

Termasuk ke dalam cipher abjadmajemuk (polyalpabetic substitution cipher). Ditemukan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigènere pada abad 16. Sudah berhasil dipecahkan pada Abad 19. Vigènere Cipher menggunakan Bujursangkar Vigènere untuk melakukan enkripsi. Setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan Caesar Cipher. Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik. Bila panjang kunci adalah m, maka periodenya dikatakan m.

Vigènere Cipher dapat mencegah frekuensi huruf-huruf di dalam cipherteks yang mempunyai pola tertentu yang sama seperti pada cipher abjad-tunggal. Jika periode kunci diketahui dan tidak terlalu panjang, maka kunci dapat ditentukan dengan menulis program komputer untuk melakukan exhaustive key search. (Basuki et al., 2016a)

Vigenère Chiper merupakan sistem sandi poli alfabetik yang sederhana. Sistem sandi poli-alfabetik mengenkripsi sekaligus sebuah teks yang terdiri dari beberapa huruf. Vigenère Chiper menggunakan substitusi dengan fungsi shift seperti pada Caesar Chiper (Utomo et al., n.d.)

Teknik untuk menghasilkan ciphertext bisa dilakukan menggunakan substitusi angka maupun bujursangkar vigènere. Teknik susbtitusi vigènere dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser (Cahya Hardita et al., n.d.)

Kriptanalisis pada kriptografi vigenere cipher dapat dilakukan dengan mencoba semua kemungkinan yang ada atau biasa disebut dengan brute force attack atau exhaustive attack namun ini dirasa kurang optimal, karena memerlukan waktu yang lama. Kriptanalisis vigenere cipher dengan mengimplementasikan algoritma genetika pernah dilakukan namun menggunakan teks cipher berbahasa inggris sebagai objek, dan memberikan hasil yang optimal dibanding algoritma lainnya. (Amin et al., 2016)

Metode Vigenere Cipher menyembunyikan pesan berupa teks melalui teknik substitusi dengan mengubah setiap huruf menjadi huruf lain berdasarkan kunci yang digunakan. Metode ini dapat mengubah pesan menggunakan kombinasi 26 huruf alfabet dan memerlukan waktu cukup lama untuk memecahkan algoritma tersebut, sehingga keamanan pesan dapat terjaga. (Tonni Limbong, 2015)

Dalam dunia teknologi informasi, tidak bisa disangkal lagi bahwa data harus diamankan dari pihakpihak yang tidak berwenang membacanya. Karena adanya pemikiran untuk mengamankan data, maka lahirlah ilmu khusus yang mempelajari tentang kamanan data tersebut. Dalam sejarah terciptanya ilmu ini, ada banyak cara dalam mengamankan data secara tradisional, misalnya saja seperti pesan singkat yang ditulis di kertas panjang yang digulung pada sebuah kayu (scytale), dan apabila gulungan kertas tersebut dibuka, maka pesan akan berbentuk huruf-huruf sandi yang sulit dimengerti.

Pada zaman yang lebih modern, ilmu keamanan data ini sudah dikenal dengan kriptografi. Pada masa data telah diolah dengan komputer (secara komputerisasi), kriptografi juga ikut berkembang. Kriptografi yang sebelumnya hanya diterapkan secara tradisional, kini sudah berkembang dengan melibatkan perhitungan matematika dan teori. (Nurtanzis Sutoyo, 2016)

METODE

Kriptografi

Kriptografi Kriptografi (crytography) berasal dari bahasaa Yunani: “cryptos” artinya “secret” (rahasia), sedangkan “graphein” artinya “writing” (tulisan). Jadi kriptografi berarti “secret writing” (tulisan rahasia). Ada beberapa defenisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Defenisi yang dipakai di dalam buku-buku yang lama menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.

Defenisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi di kalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih dari sekedar privacy, tetapi juga untuk tujuan data integrity, authentication, dan non-repudiation. Defenisi lain dari kriptografi yaitu, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (Rinaldi Munir, 2006). Beberapa istilah yang akan ditemukan di dalam kriptografi yaitu :

Pesan, Plainteks dan Cipherteks

Pesan (message) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah plainteks (plaintext). Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut cipherteks (chipertext). Chiperteks harus dapat ditransformasikan kembali menjadi plainteks semula agar pesan yang diterima bisa dibaca.

Pengirim dan penerima

Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (sender) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (receiver) adalah entitas yang menerima pesan.

Enkripsi dan dekripsi

Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (encryption), sedangkan proses menjadikan cipherteks menjadi plainteks semula dinamakan dekripsi (decryption).

Cipher dan kunci

Algoritma kriptografi disebut juga cipher yaitu aturan untuk enkripsi daan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Kunci (key) adalah parameter yang digunakan untuk transformasi enkripsi dan dekripsi. Kunci biasanya berupa string atau deretan bilangan.

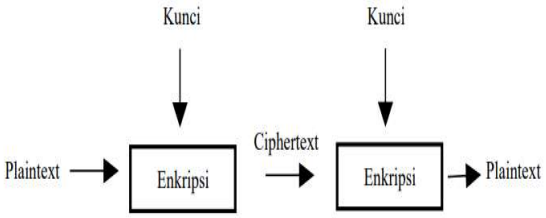
Sistem kriptografi

Kriptografi membentuk sebuah sistem yang dinamakan sistem kriptografi. Sistem kriptografi adalah kumpulan yang terdiri dari algoritma kriptografi, semua plainteks, cipherteks yang mungkin dan kunci.

Kriptanalisis dan kriptologi

Kriptanalisis (cryptanalysis) adalah ilmu dan seni untuk memecahkan chiperteks menjadi plainteks tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis. Jika seorang

kriptografer (cryptografer) mentransformasikan plainteks menjadi cipherteks dengan suatu algoritma dan kunci maka sebaliknya seorang kriptanalis berusaha untuk memecahkan cipherteks tersebut untuk menemukan plainteks dan kunci. (Aditya Permana, 2018)



Gambar 1. Skema enkripsi dan dekripsi dengan menggunakan kunci

Caesar Cipher

Didalam *caesar cipher,* tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan alphabet. *Caesar cipher* tidak memiliki kunci, keamanan algoritma terletak pada kerahasiaan algoritmanya (hanya raja Julius Caesar para gubernurnya yang tahu). Dalam buku Practical Workbook: Information Theory, 4th edition, Department of Computer & Information System Engineering NED University of Engineering & Technology, Karachi, Pakistan, dijelaskan bahwa metode *Caesar cipher* yang digunakan menggunakan prinsip modulo 26. (Basuki et al., 2016b)

Pada teknik Caesar cipher ada dua deretan baris alphabet yang disusun, pada deratan baris pertama berisikan urutan alphabet A-Z dan pada deretan kedua berisikan alphabet sandi untuk mengenkripsi pergesaran dari plaintext.

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
Ciphertext	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

Gambar 2. Tabel Subtitusi Pergeseran dari Plaintext

Jadi, huruf a pada *plaintetx* disubstitusikan dengan D, huruf b disubstitusi dengan E, demikian seterusnya. Pergeseran huruf tersebut besifat siklik, jadi huruf x digeser menjadi A, huruf y menjadi B, dan huruf z menjadi C. Dalam prakteknya pegeseran siklik didalam *caesar cipher* ini dapat diimplementasikan dengan sebuah roda yang bernama *Caesar wheel.* (Ats Tsauri, 2017)

Gambar 3 memperlihatkan *Caesar wheel. Caesar wheel* terdiri dari dua buah lempeng lingkaran besi. Lingkaran besi paling luar menyatakan huruf-huruf p*laintext* sedangkan lingkaran besi terdalam menyatakan huruf-huruf *ciphertext.* Lingkaran besi terdalam dapat diputar sejauh pergeseran yang diinginkan. Misalnya jika lingkaran besi terdalam digeser sejauh 3 huruf, maka susunan huruf-huruf didalam kedua lingkaran besi merepresentasi- kan tabel substitusi diatas.

Gambar 3. *Caesar Wheel*
Sumber Sumber: www.prizecodebreaker.com

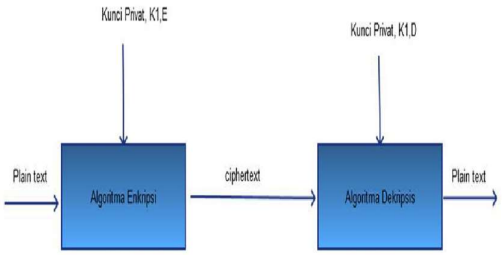
Untuk penerapan pengkodean pesan dengan cara mencari pesan huruf yang mau disandikan pada *alphabet* pertama kemudian tuliskan huruf sesuai dengan apa yang ada pada alphabet kedua.

Proses penghitungan biasa menggunakan rumus matematis operasi modulus dengan cara diketahui angka, A=0, B=1, Z=25. Enkripsi (E_n) dari "huruf" x dengan digeser n secara rumus diketahui dengan,

$$E_n(x) = (x + n) mod\ 26 \quad (1)$$

Adapun untuk proses pemunculan setelah dikodekan melalui Pendekripsian kode (D_n) yaitu:

$$D_n(x) = (x - n) mod\ 26 \quad (2)$$



Gambar 4. Proses Enkripsi dan Dekripsi

Proses pengaanan pesan atau plaintext pada *Caesar Cipher* yaitu dngan cara pengenkripsian dengan menggunakan unci (*Key*) sehingga menghasilkan *Ciphertext.* Adaun dalam proses Dekripsi dengan cara *ciphertext* dimasukkan kemudian menggunakan kunci (*key*) yang sama ketika proses enkripsi sehingga menghasilkan *plaintext* kembali. (Sasongko, 2005)

Vignere Chiper

Hallim (2010: 3) Vigenère cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1986. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenère, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku La Cifra del Sig. Giovan Batista Belaso, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553.

Cara kerja dari Vigenère cipher ini mirip dengan Caesar cipher, yaitu mengenkripsi plainteks pada pesan dengan cara menggeser huruf pada pesan tersebut sejauh nilai kunci pada deret alphabet. Vigenère cipher adalah salah satu algoritma kriptografi klasik yang menggunakan metode

substitusi abjadmajemuk. Substitusi abjad-majemuk mengenkripsi setiap huruf yang ada menggunakan kunci yang berbeda, tidak seperti Caesar cipher yang menerapkan metode substitusi abjad-tunggal yang semua huruf di suatu pesan dienkripsi menggunakan kunci yang sama. (Gautam et al., 2018)

Contoh dari penerapan algoritma Vigenère cipher adalah jika kita memiliki sebuah plainteks yang ingin dienkripsi:

MAKALAH KRIPTOGRAFI

Dan kita menggunakan kunci:

TUGAS

Maka plainteks akan dienkripsi dengan cara:

Plaintext : MAKALAH KRIPTOGRAFI

Kunci : TUGASTU GASTUGASTUG

Ciphertext : FUQADTB QRAINUGJTZO

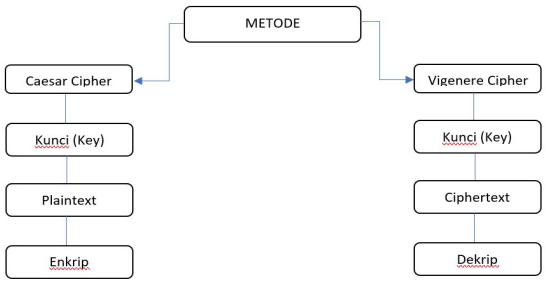
Huruf pada kunci akan dikonversi menjadi sebuah nilai, misalnya A = 0, B = 1, sampai dengan Z = 25. Setelah itu prosesnya sama seperti pada Caesar cipher dimana setiap huruf pada plainteks akan digeser sejauh nilai kunci yang posisinya bersesuaian. Pergeseran huruf-huruf ini bisa dipetakan dalam bentuk tabel 26x26 yang memetakan antara huruf pada plainteks dengan huruf pada kunci seperti yang diperlihatkan pada Gambar 5.

	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 5. Tabel pemetaan Vigenère Cipher

HASIL DAN DISKUSI

Perancangan Sistem Aplikasi Kriptografi, Sistem ini dirancang sedemikian rupa, sehingga Penginputan Teks dapat mengenkripsi pesan (plain text) yang diterima. Teks yang akan dikirim akan diterima oleh penerima dalam keadaan terenkripsi (chiper text), sehingga penerima teks harus melakukan dekripsi pada teks tersebut dengan bertukar kunci (key) untuk mengubah chiper text menjadi plain text awal. Sistem berhasil dirancang dengan skema di bawah ini (Gambar 6).



Gambar 6. Skema Jalannya Dengan Masing Metode

Sistem kriptografi teks pesan pada penelitian ini merupakan salah satu teknik yang dilakukan untuk menjaga keamanan Penginputan Teks. Proses enkripsi dan dekripsi metode Caesar Cipher Dan Vigenere Cipher ini dilakukan dengan mengubah isi Teks yang akan dikirim ataupun diterima.

Plaintext adalah pesan atau informasi yang akan dikirimkan dalam format yang mudah dibaca atau dalam bentuk aslinya. Ciphertext adalah informasi yang sudah dienkripsi. (Efrandi & Asnawati, 2014)

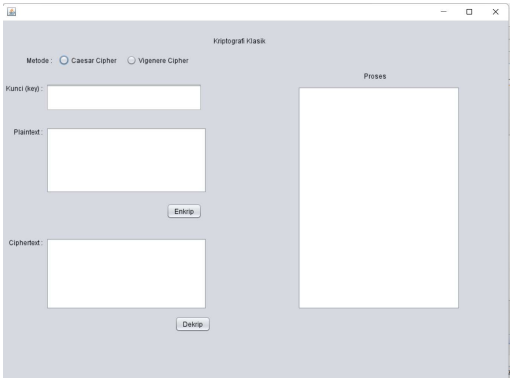
Hasil penelitian yang diperoleh adalah dapat diterapkannya algoritma kriptografi klasik dengan mengkombinasikan algoritma Caesar Chiper dan Vigenere Chiper untuk menghasilkan pesan teks rahasia. Teks asli dapat di ubah menjadi teks yang dirahasiakan (chiperteks) dengan mengkombinasikan algoritma Caesar Chiper dan Vigenere Chiper, serta teks yang telah di enkripsi dapat dikembalikan menjadi teks asli (plainteks). Sedangkan penginisialan huruf alfabet A-Z menjadi angka 0 – 25 disajikan seperti Tabel l . (Ramdani et al., n.d.)

Tabel 1. Penginisialan Huruf Alfabet

Huruf :	A	B	C	D	…	Z
Angka :	0	1	2	3	…	25

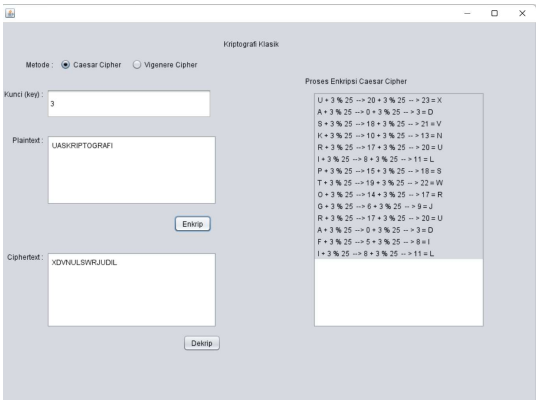
Hasil dan Output

Tampilan awal halaman Aplikasi Kriptografi Klasik dapat terjadi pada saat aplikasi pertama kali dijalankan atau di run. Berikut Gambar 7 merupakan tampilan awalnya.



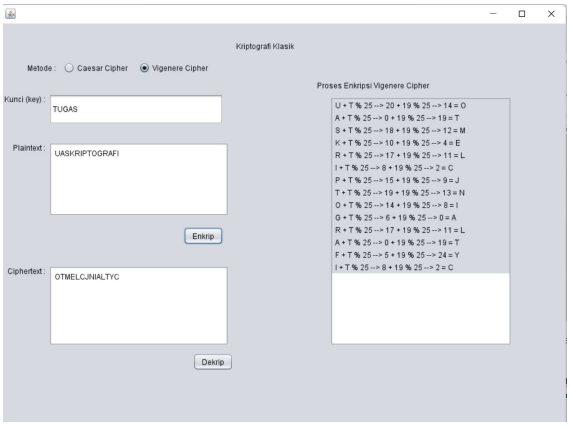
Gambar 7. Tampilan Awal

Pada halaman ini, user dapat memilih metode yang ingin dipakai seperti Caesar cipher atau Vigenere Cipher. Dengan kunci(key) 1-25 dan abjad A-Z, kita akan mencoba untuk menggunakan Caesar Cipher terlebih dahulu. Berikut tampilannya pada Gambar 8.



Gambar 8. Tampilan Menggunakan Metode Caesar Cipher

Pada halaman selanjutnya akan menggunakan Metode Vigenere Cipher, bedanya dengan Caesar Cipher ialah pada key(kunci), yang dimana Vigenere Cipher mengisi bagian key nya dengan Huruf sedangkan Caesar cipher mengisi dengan angka. Berikut tampilan pada metode vigenere cipher Gambar 9.



Gambar 9. Tampilan Menggunakan Metode Vigenere Cipher

Tabel dibawah ini akan memberikan beberapa percobaan yang telah dilakukan dengan 2 metode Caesar cipher dan Vigenere Cipher.

Tabel 2. Tabel Hasil Enkripsi Contoh Kalimat Dengan Enkripsi Caesar Ciphiper

Plaintext	Key	Ciphertext
hai	1	IBJ
UAS KRIPTOGRAGI	24	TYRXJQHOSNFQYFH
JURNAL KRIPTOGRAFI	18	CNKGSERDKBIMHYKSXB

Tabel 3. Tabel hasil Enkripsi Contoh Kalimat dengan Dekripsi Vigenere Ciphiper

Ciphertext	Key	Plaintext
JUMAT	HAI	QCTHB
SENIN	HELLO	DHYHGCSP
SENIN KRIPTO DAN IOT	TUGAS	MXHCHELCJNIWTHCIN

KESIMPULAN

Berdasarkan Pengujian Pada Aplikasi Kriptografi dan penyelesaian masalah pada bab-bab sebelumnya, maka dapat ditarik kesimpulan sebagai berikut: a. Keamanan Penginputan Teks sangat diperlukan untuk menjaga kerahasiaan pesan. b. Enkripsi dan Dekripsi dengan caesar cipher dan vigenere cipher menggunakan key acak menjadikan teks yang sama menghasilkan ciphertext dan plaintext yang berbeda sehingga menjadi lebih aman untuk keamanan Penginputan Teks.

Aplikasi pesan email dengan enkripsi caesar cipher dan vignere chipper masih memiliki banyak kekurangan, dan diperlukan pengembangan lebih lanjut guna mencapai hasil keamanan yang maksimal. Berikut ini saran yang dijadikan acuan untuk pengembangan aplikasi selanjutnya: a. Adanya penambahan fitur agar user dapat membuka aplikasi tanpa harus melalui java netbeans. b. Adanya penambahan fitur metode yang selain Caesar cipher dan vigenere cipher.

REFERENSI

Aditya Permana, A. (2018). *Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android* (Vol. 4, Issue 3).

Amin, M. M., Komputer, J. T., Negeri, P., & Palembang, S. (2016). IMPLEMENTASI KRIPTOGRAFI KLASIK PADA KOMUNIKASI BERBASIS TEKS. *Jurnal Pseudocode*, *2*.

Ats Tsauri, T. (2017). APLIKASI ALGORITMA GENETIKA UNTUK MENEBAK KATA KUNCI PADA DEKRIPSI VIGENERE CIPHER TEKS BAHASA INDONESIA. In *JISKa* (Vol. 2, Issue 2).

Basuki, A., Paranita, U., & Hidayat, R. (2016a). *PERANCANGAN APLIKASI KRIPTOGRAFI BERLAPIS MENGGUNAKAN ALGORITMA CAESAR, TRANSPOSISI, VIGENERE, DAN BLOK CHIPER BERBASIS MOBILE*. 6–7.

Basuki, A., Paranita, U., & Hidayat, R. (2016b). *PERANCANGAN APLIKASI KRIPTOGRAFI BERLAPIS MENGGUNAKAN ALGORITMA CAESAR, TRANSPOSISI, VIGENERE, DAN BLOK CHIPER BERBASIS MOBILE*. 6–7.

Cahya Hardita, V., Wahyu Sholeha, E., Raya Jl Obos No, P. G., Raya, P., Tengah, K., Informasi, T., Negeri Tanah Laut Jl Yani NoKm, P. A., Pelaihari, K., Tanah Laut, K., & Selatan, K. (n.d.). *PENERAPAN KOMBINASI METODE VIGENERE CIPHER, CAESAR CIPHER DAN SIMBOL BACA DALAM MENGAMANKAN PESAN*.

Efrandi, & Asnawati, Y. (2014). APLIKASI KRIPTOGRAFI PESAN MENGGUNAKAN ALGORITMA VIGENERE CIPHER. In *Jurnal Media Infotama* (Vol. 10, Issue 2).

Gautam, D., Sharma, P., Agrawal, C., Mehta, M., & Saini, P. (2018). *An Enhanced Cipher Technique using Vigenere and Modified Caesar Cipher*.

Lestari, W. A., Tulloh, R., Novianti, A., & St, S. (n.d.). *MEDIA PEMBELAJARAN INTERAKTIF ENKRIPSI CAESAR CIPHER, VIGENERE CIPHER, DAN ALGORITMA RSA Interactive Learning Media of Caesar Cipher, Vigenere Cipher, and RSA Algorithm Encryption*.

Minarto, G. B., & Khairuzzaman, M. Q. (n.d.). *Penerapan Kriptografi Menggunakan Caesar Cipher Dan Vigenere Cipher*.

Nurtanzis Sutoyo, M. (2016). *Kombinasi Algoritma Kriptografi Caesar Chiper dan Vigenere Chiper Untuk Keamanan Data*. *2*(1).

Ramdani, A., Iskandar Mulyana, D., Septian, W., & Sugiharto, T. (n.d.). *ENKRIPSI DEKRIPSI ALGORITMA CAESAR CHIPER PADA CHATTING BERBASIS JAVA*.

Sasongko, J. (2005). Pengamanan Data Informasi menggunakan Kriptografi Klasik. *Jurnal Teknologi Informasi DINAMIK*, *X*(3), 160–167.

Tonni Limbong. (2015). *PENGUJIAN KRIPTOGRAFI KLASIK CAESAR CHIPPER MENGGUNAKAN MATLAB*. https://www.researchgate.net/publication/313791310

Utomo, W., Latifah, R., & Risanty, R. D. (n.d.). *APLIKASI KRIPTOGRAFI BERBASIS ANDROID MENGGUNAKAN ALGORITMA CAESAR CIPHER DAN VIGENERE CIPHER*. Teknologi Informasi dan Komputer. https://jurnal.umj.ac.id