

## PENGUJIAN PENGEMBANGAN TERHADAP ALGORITMA VIGENERE KEY KRIPTOGRAFI

Chyquitha Danuputri<sup>1</sup>, Nico Santosa<sup>2</sup>, Fernando Dedi Samuel<sup>3</sup>

<sup>1,2,3</sup> Teknik Informatika, Teknologi dan Desain, Universitas Bunda Mulia  
Jl. Lodan Raya No. 2 Ancol, Indonesia

e-mail: chyquitha@gmail.com<sup>1</sup>, nico.santosa1@gmail.com<sup>2</sup>, fernando.dedi2@gmail.com<sup>3</sup>

Received : February, 2021	Accepted : April, 2022	Published : April, 2022
---------------------------	------------------------	-------------------------

### Abstract

*The process of digital communication through media that is already integrated with the internet requires a security system in order to prevent confidential data from being acquired by unauthorized third parties and misused by these third parties. In order not to know the confidentiality of the data, techniques and algorithms are needed that can make secret messages not understand the meaning of the secret message. One of the data security techniques is cryptography, which can scramble the arrangement of characters that humans understand into characters that are not understood by humans with various languages. This research is the development of the Vigenere Key Kriptography algorithm for the encryption and decryption process in text messages that include all the characters on the computer keyboard keys. The results of the encryption will be in the form of a.txt file which contains cipher text and the results of the decryption will be plain text that appears in the application text box and the test uses the Python programming language. This research can produce cryptographic techniques that can produce ciphertext of all characters on the computer keyboard keys and can scramble text so that it cannot be understood by human language for data security.*

**Keywords:** Security Data, Cryptography, Python, Vigenere Key

### Abstrak

*Proses komunikasi digital melalui media yang sudah terintegrasi dengan internet membutuhkan sistem keamanan agar dapat mencegah perolehan data rahasia oleh pihak ketiga yang tidak memiliki wewenang dan disalahgunakan oleh pihak ketiga tersebut. Agar tidak dapat diketahui kerahasiaan data, maka dibutuhkan teknik dan algoritma yang dapat membuat pesan rahasia tidak dipahami arti dari pesan rahasia tersebut. Salah satu teknik pengamanan data adalah Kriptografi yang dapat mengacak susunan karakter yang dipahami manusia menjadi susunan karakter yang tidak dipahami manusia dengan berbagai bahasa. Penelitian ini merupakan pengembangan rumus algoritma Vigenere Key Kriptografi untuk proses enkripsi dan dekripsi pada pesan yang berbentuk teks meliputi semua karakter pada tombol keyboard komputer. Hasil enkripsi akan berupa file .txt yang berisikan chiper text dan hasil dekripsi akan berupa plain text yang tampil pada text box aplikasi dan pengujiannya menggunakan bahasa pemrograman Python. Penelitian ini dapat menghasilkan teknik kriptografi yang dapat menghasilkan chipertext semua karakter pada tombol keyboard komputer dan dapat mengacak teks menjadi tidak dapat dipahami oleh bahasa manusia untuk keamanan data.*

**Kata Kunci:** Keamanan Data, Kriptografi, Python, Vigenere Key

## 1. PENDAHULUAN

Komputer diciptakan untuk mempermudah aktifitas manusia di dunia nyata, dari proses perhitungan, penyimpanan data, pemrosesan data dan menghasilkan output yang dapat diandalkan manusia dalam menyelesaikan atau memberikan solusi atas masalah yang ada. Salah satunya adalah proses komunikasi digital melalui media yang sudah terintegrasi dengan internet sering terjadi perolehan data rahasia oleh pihak ketiga yang tidak memiliki wewenang dan disalahgunakan oleh pihak ketiga tersebut.

Keamanan data merupakan sebuah aspek penting dalam media transmisi data terutama pada masa modern ini dimana berdasarkan survey yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mengatakan bahwa dari 2.500 responden di seluruh Indonesia, 89.35% menggunakan layanan chatting[1].

Untuk mengamankan pesan yang dikirim tersebut dapat diterapkan sebuah teknik yang dikenal dengan teknik kriptografi. Kata kriptografi sendiri berasal dari bahasa Yunani yang terdiri dari kata *kryptos* yang memiliki arti tersembunyi dan *graphein* memiliki arti menulis, sehingga ketika kedua kata tersebut digabungkan dapat diartikan sebagai seni menulis pesan rahasia (The art of secret writing)[2].

Terdapat berbagai macam metode dalam kriptografi untuk mengamankan sebuah data salah satunya adalah metode sandi Vigenère, sandi Vigenere adalah algoritma kriptografi klasik yang mulai diperkenalkan pada abad ke-16. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenère[3].

Cara kerja dari sandi Vigenère dalam menyandikan sebuah pesan adalah dengan menggunakan sebuah tabel alphabet. Tabel inilah yang disebut sebagai Vigenère. Tabel Vigenère terdiri dari 26 kolom horizontal dan 26 baris vertical (sejumlah dengan abjad a sampai z). Setiap huruf dapat disandikan dengan menggunakan baris atau kolom yang berbeda-beda menyesuaikan dengan kata kunci yang diulang[4].

Pada penelitian ini, penulis bermaksud untuk mengembangkan sebuah aplikasi pengaman

pesan berbasis dekstop menggunakan bahasa pemrograman python yang menerapkan metode sandi Vigenère yang sehingga tidak terbatas pada 26 abjad saja tetapi mencakup keseluruhan abjad pada keyboard atau karakter pada desimal ke-32 sampai ke-126 pada tabel ASCII. Aplikasi ini dibuat dengan maksud untuk mengamankan pesan sebelum dikirim ke penerima.

### 1.1 Tinjauan Pustaka

#### 1.1.1 Kriptografi

Kriptografi adalah ilmu dan seni dalam menyembunyikan atau menyamarkan sebuah makna dari suatu pesan sehingga orang yang tidak berkepentingan tidak dapat mengetahui makna asli didalam pesan tersebut. Dalam ilmu ini, terdapat dua buah proses yaitu melakukan proses untuk menyamarkan atau menyembunyikan makna yang dikenal dengan sebutan enkripsi dan proses untuk menemukan atau mengambil makna tersembunyi dalam pesan yang dikenal dekripsi[5].

#### 1.1.2 Enkripsi dan Dekripsi

Enkripsi adalah sebuah proses menyamarkan atau menyembunyikan makna dengan melakukan penyandian pesan asli (*plaintext*) menjadi teks tersandi (*Ciphertext*) sedangkan dekripsi adalah sebuah proses kebalikan dari enkripsi yaitu untuk mendapatkan kembali makna asli dari suatu pesan dengan melakukan penyandian kembali teks tersandi (*Ciphertext*) menjadi pesan asli (*plaintext*)[6]. Proses enkripsi ini diterapkan pada pesan yang hendak dikirim sedangkan dekripsi diterapkan pada pesan yang diterima[7].

#### 1.1.3 Vigenère

Vigenère cipher merupakan algoritma kriptografi klasik yang diperkenalkan pada abad ke-16 atau sekitar tahun 1586. 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 [8]. Teknik ini umumnya diterapkan dengan menggunakan angka dan huruf.

Vigenère Cipher dengan angka adalah metode menyandikan teks alfabet dengan

menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci.

Vigenère Cipher dengan huruf menggunakan tabel *Vigenère* yang berisi alfabet yang dituliskan dalam 26 baris dan kolom, dimana setiap baris akan digeser kekiri satu urutan dari baris sebelumnya sehingga nantinya akan menghasilkan sandi Caesar sebanyak 26 buah. Pada metode ini setiap huruf akan disandikan dengan baris yang berbeda sesuai bergantung dengan kata kunci yang diulang. Adapun rumus dari enkripsi dan dekripsi metode Vigenère cipher sebagai berikut[9]:

Enkripsi:

$$C_i = (P_i + K_i) \bmod 26$$

Dekripsi:

$$P_i = (C_i - K_i) \bmod 26; \text{ untuk } C_i \geq K_i$$

$$P_i = (C_i + 26 - K_i) \bmod 26; \text{ untuk } C_i < K_i$$

### 1.1.4 ASCII(American Standart Code for Information Interchange)

ASCII (American Standart Code for Information Interchange) merupakan standar kode huruf dan juga simbol yang berjumlah 255. Kode ASCII dari 0 sampai 127 adalah kode untuk memanipulasi teks sedangkan kode dengan nilai dari 128 sampai 255 adalah kode untuk memanipulasi gambar/grafik[10].

Standard ASCII The first 32 characters are control codes.				Extended ASCII (DOS)							
0	Null	33	!	81	Q	128	Ç	174	«	220	⌘
1	Start of heading	34	"	82	R	129	Ù	175	»	221	⌘
2	Start of text	35	#	83	S	130	É	176	⌘	222	⌘
3	End of text	36	\$	84	T	131	À	177	⌘	223	⌘
4	End of transmit	37	%	85	U	132	Á	178	⌘	224	⌘
5	Enquiry	38	&	86	V	133	Â	179	⌘	225	⌘
6	Acknowledge	39	'	87	W	134	Ã	180	⌘	226	⌘
7	Audible bell	40	<	88	X	135	Ä	181	⌘	227	⌘
8	Backspace	41	>	89	Y	136	Å	182	⌘	228	⌘
9	Horizontal tab	42	*	90	Z	137	Æ	183	⌘	229	⌘
10	Line feed	43	+	91	[	138	Ç	184	⌘	230	⌘
11	Vertical tab	44	,	92	\	139	È	185	⌘	231	⌘
12	Form feed	45	-	93	]	140	É	186	⌘	232	⌘
13	Carriage return	46	.	94	^	141	Ê	187	⌘	233	⌘
14	Shift out	47	/	95	_	142	Ë	188	⌘	234	⌘
15	Shift in	48	0	96	`	143	Ì	189	⌘	235	⌘
16	Data link escape	49	1	97	a	144	Í	190	⌘	236	⌘
17	Device control 1	50	2	98	b	145	Ï	191	⌘	237	⌘
18	Device control 2	51	3	99	c	146	Ï	192	⌘	238	⌘
19	Device control 3	52	4	100	d	147	Ò	193	⌘	239	⌘
20	Device control 4	53	5	101	e	148	Ó	194	⌘	240	⌘
21	Neg. acknowledge	54	6	102	f	149	Ô	195	⌘	241	⌘
22	Synchronous idle	55	7	103	g	150	Õ	196	⌘	242	⌘
23	End trans. block	56	8	104	h	151	Ö	197	⌘	243	⌘
24	Cancel	57	9	105	i	152	Ù	198	⌘	244	⌘
25	End of medium	58	:	106	j	153	Ú	199	⌘	245	⌘
26	Substitution	59	;	107	k	154	Û	200	⌘	246	⌘
27	Escape	60	<	108	l	155	Ü	201	⌘	247	⌘
28	File separator	61	=	109	m	156	Ý	202	⌘	248	⌘
29	Group separator	62	>	110	n	157	ÿ	203	⌘	249	⌘
30	Record separator	63	?	111	o	158	ÿ	204	⌘	250	⌘
31	Unit separator	64	@	112	p	159	ÿ	205	⌘	251	⌘
32	Blank space	65	A	113	q	160	ÿ	206	⌘	252	⌘
		66	B	114	r	161	ÿ	207	⌘	253	⌘
		67	C	115	s	162	ÿ	208	⌘	254	⌘
		68	D	116	t	163	ÿ	209	⌘	255	⌘
		69	E	117	u	164	ÿ	210	⌘		
		70	F	118	v	165	ÿ	211	⌘		
		71	G	119	w	166	ÿ	212	⌘		
		72	H	120	x	167	ÿ	213	⌘		
		73	I	121	y	168	ÿ	214	⌘		
		74	J	122	z	169	ÿ	215	⌘		
		75	K	123	[	170	ÿ	216	⌘		
		76	L	124	\	171	ÿ	217	⌘		
		77	M	125	]	172	ÿ	218	⌘		
		78	N	126	~	173	ÿ	219	⌘		
		79	O	127	Δ						
		80	P								

Gambar 1. Tabel Kode Ascii 0-255

[11]

## 2. METODE PENELITIAN

### 2.1 Deskripsi Data

Penelitian ini dilakukan untuk mengembangkan teori pengamanan data yang berbentuk teks. Penelitian ini merupakan penelitian murni dan penelitian terapan. Dikatakan penelitian murni dikarenakan penelitian yang penulis buat adalah untuk mengembangkan teori yang sudah ada dan dikatakan penelitian terapan dikarenakan penelitian ini hasilnya dapat langsung diterapkan untuk memecahkan sebuah permasalahan (Moedjiono 2012) dalam

hal ini adalah aplikasi ini dapat digunakan dalam menyembunyikan sebuah pesan dan dapat digunakan kembali untuk mengembalikan pesan yang disembunyikan sebelumnya.

Dalam implementasinya penelitian ini menggunakan bahasa pemrograman Python yang dapat menguji sistem keamanan data dengan pengembangan rumus dan metode algoritma *Vigenère*. Penelitian ini dalam pengembangannya sistemnya menggunakan metode prototype serta analisis dan

perancangan sistem dengan pendekatan berorientasi objek (*object oriented*).

## 2.2 Metode Pengumpulan Data

Penelitian ini menggunakan metode pengumpulan data sebagai berikut :

### 2.2.1 Metode Observasi

Observasi adalah metode ini melakukan kegiatan pengawasan dan pengamatan terhadap objek atau metode yang akan diteliti[Sugiyono 2012].

Observasi pada penelitian ini adalah dengan melakukan pengamatan terhadap Algoritma Vigenère yang merupakan salah satu algoritma kriptografi dan algoritma ini dapat diterapkan untuk melakukan pengamatan data yang berbentuk teks.

### 2.2.2 Metode Studi Pustaka

Metode studi pustaka dalam penelitian ini adalah kegiatan mempelajari, meneliti, dan membaca jurnal, buku, tesis, skripsi, baik hardcopy maupun softcopy yang berhubungan atau memiliki relevansi mengenai sistem keamanan data dan algoritma Vigenère.

### 2.3 Rumus Pengembangan Vigenere Key

Kode ASCII (Standard Code for Information Interchange) pada implementasi ini mencakup seluruh angka, huruf, dan simbol yang terdapat pada keyboard(ASCII bit ke-32 sampai bit ke-126) untuk nilai yang jatuh pada ASCII bit ke-0 sampai bit ke-31 pada saat enkripsi akan disubstitusi dengan kunci spesial. Berikut tabel ASCII dari bit ke-0 sampai bit ke-127:

Desimal	Karakter	Desimal	Karakter	Desimal	Karakter	Desimal	Karakter
0	NUL	32	Space	64	@	96	`
1	SOH	33	!	65	A	97	a
2	STX	34	"	66	B	98	b
3	ETX	35	#	67	C	99	c
4	EOT	36	\$	68	D	100	d
5	ENO	37	%	69	E	101	e
6	ACK	38	&	70	F	102	f
7	BEL	39	'	71	G	103	g
8	BS	40	(	72	H	104	h
9	TAB	41	)	73	I	105	i
10	LF	42	*	74	J	106	j
11	VT	43	+	75	K	107	k
12	FF	44	,	76	L	108	l
13	CR	45	-	77	M	109	m
14	SO	46	.	78	N	110	n
15	SI	47	/	79	O	111	o
16	DLE	48	0	80	P	112	p
17	DC1	49	1	81	Q	113	q
18	DC2	50	2	82	R	114	r
19	DC3	51	3	83	S	115	s
20	DC4	52	4	84	T	116	t
21	NAK	53	5	85	U	117	u
22	SYN	54	6	86	V	118	v
23	ETB	55	7	87	W	119	w
24	CAN	56	8	88	X	120	x
25	EM	57	9	89	Y	121	y
26	SUB	58	:	90	Z	122	z
27	ESC	59	;	91	[	123	{
28	FS	60	<	92	\	124	
29	GS	61	=	93	]	125	}
30	RS	62	>	94	^	126	~
31	US	63	?	95	_	127	DEL

Gambar 2. Tabel Kode Ascii 0-255 [12]

### 2.3.1 Rancangan Enkripsi

Rumus Pengembangan Enkripsi Vigenere :

$$\text{Kalkulasi} = (\text{Pi} + \text{Ki})$$

Jika Kalkulasi < 127, maka  $\text{Ci} = (\text{Pi} + \text{Ki}) - 1 \text{ mod } 127$

Jika Kalkulasi  $\geq 127$ , maka  $\text{Ci} = (\text{Pi} + \text{Ki}) - 1 - 127$

Keterangan :

Pi : Plain Text

Ki : Key Text

Kalkulasi : perhitungan penjumlahan nilai desimal Plain Text dan Key Text

Rancangan Sistem Enkripsi

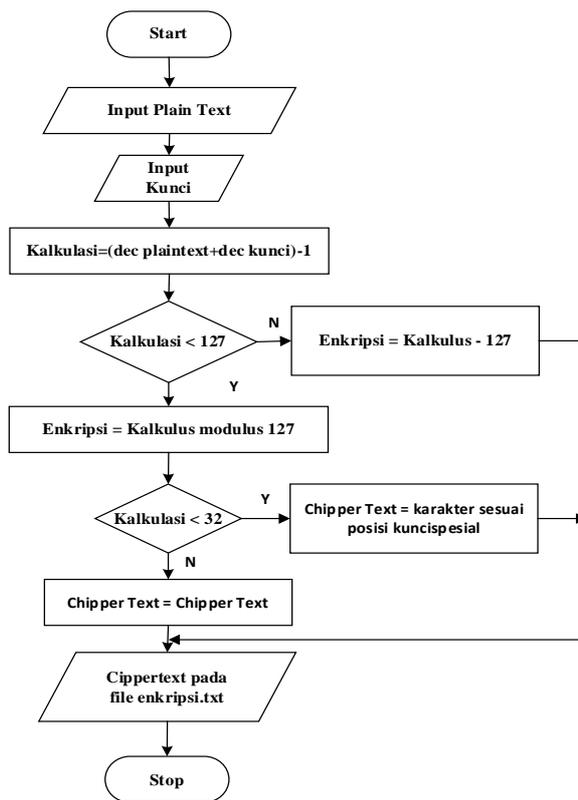
1. Pengguna memasukan pesan kedalam textbox "Pesan Rahasia" dengan (Plain Text).
2. Pengguna memasukan kunci pada textfield "KUNCI" dengan teks kunci bersifat dinamis, yaitu kunci enkripsi dapat berubah dari proses pertama dengan proses berikutnya.
3. Aplikasi akan melakukan kalkulasi dengan rumus sebagai berikut untuk setiap huruf:

- (nilai desimal plaintext + nilai desimal kunci)-1
4. Jika kalkulasi < 127 maka hasil kalkulasi modulus 127 tetapi jika tidak maka hasil kalkulasi dikurang 127.
  5. Jika kalkulasi < 32 maka tuliskan karakter dari list kuncispesial pada urutan sesuai kalkulasi kedalam ciphertext tetapi Jika tidak maka

tuliskan karakter dengan nilai desimal ASCII sesuai dengan kalkulasi kedalam ciphertext.

Kuncispesial berisikan karakter 'ÿ', 'þ', 'ý', 'ü', 'ù', 'ú', 'û', 'ø', '÷', 'ö', 'õ', 'ô', 'ó', 'ò', 'ñ', 'ð', 'í', 'î', 'ï', 'è', 'é', 'ê', 'ë', 'ç', 'æ', 'à', 'ä', 'ã', 'â', 'á', 'à', 'á', 'â', 'Û', 'Ü'.

6. Hasil enkripsi ditampilkan pada textbox "HASIL ENKRIPSI" yang berisi Chipertext dan dimasukan ke dalam file bernama "enkripsi.txt" yang dihasilkan pada root folder aplikasi.



Gambar 3. Flowchart Enkripsi

### 2.3.2 Rancangan Dekripsi

Rumus Pengembangan Dekripsi Vigenere :

Jika Ci ada didalam kuncispesial, maka

$$\text{kalkulasi} = ((\text{posisispesial} - K_i) \bmod 127) + 1,$$

– jika kalkulasi=0 maka jangan tulis apa-apa pada hasil dekripsi,

– jika nilai kalkulasi < 0 maka tulis karakter dari kuncispesial pada elemen ke-1,

– jika tidak maka tulis karakter ASCII pada desimal senilai kalkulasi.

Jika Ci tidak ada dalam kuncispesial maka

$$\text{kalkulasi} = ((C_i - K_i) \bmod 127) + 1,$$

– jika kalkulasi=0 maka jangan tulis apa-apa pada hasil dekripsi

– jika nilai kalkulasi < 0 maka tulis karakter dari kuncispesial pada elemen ke-1

– jika tidak maka tulis karakter ASCII pada desimal senilai kalkulasi.

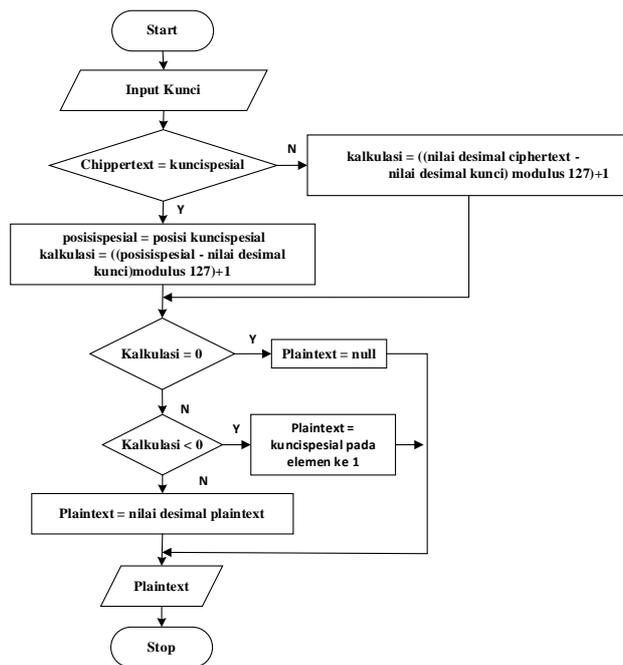
Keterangan :

Ci : Chipertext

kalkulasi : perhitungan terhadap posisispesial dan Kunci

posisispesial : posisi kunci spesial

kuncispesial :



Gambar 4. Flowchart Dekripsi

### 3. HASIL DAN PEMBAHASAN

#### 3.1 Deskripsi Data

Pada penelitian ini akan menggunakan 15 data Plain text yang akan di uji dalam proses enkripsi.

Tabel 1: Tabel Data Plaintext

No	Plain Text	Key Text	Ukuran Data
1	qwertyuiopasdfghjklz xcvbnmQWERTYUIO PASDFGHJKLZXCVBN M,./;'\[]\<>?:'"} `1234 567890- =~!@#\$\$%^&*()_+`	UJICOBA	94bytes
2	Apa kabar hari ini?	Rahasia	19bytes
3	testing 123 aman	kunci123	19bytes
4	Dia berkata: malam ini hujan deras!	hujan	35bytes
5	email@emailprovider.com	email	23bytes
6	mulai dalam 1..2..3..	hitung	21bytes
7	semoga beruntung kawan	kawan	22bytes
8	Hari ini adalah hari yang yang cerah untuk pergi	c3Rah	48bytes
9	Jangan menilai buku dari sampulnya	@123	34bytes
10	berkumpul jam 7:30 malam	kumpul0	24bytes

No	Plain Text	Key Text	Ukuran Data
11	belajar bersama di rumah saya nanti	b3l4j4r	35bytes
12	jangan mudah menyerah tetap bekerja keras	keras	41bytes
13	mencoba berkali-kali hingga berhasil	cobaterus	36bytes
14	perjuangan hampir selesai tetapi masih ada lagi tantangan didepan	panjang	65bytes
15	semoga berhasil dan beruntung.	00re	30bytes

### 3.2 Pembahasan

Bagian ini memuat pembahasan dari data hasil penelitian yang telah disajikan.

*chippertext*, durasi proses enkripsi, besar file enkripsi.txt sebagai hasil output *chippertext*.

#### 3.2.1 Enkripsi

Dari data Plaintext dilakukan proses enkripsi dengan mendapatkan data-data

Tabel 2: Tabel Hasil Enkripsi

No	Plain Text	Key Text	Ukuran Data	Chippertext	Durasi Enkripsi (sec)	Ukuran File enkripsi .txt
1	qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM,./;'\<>?:"{} `1234567890- =~!@#\$%^&*()_+`	UJICOPA	94bytes	FaN5c[V>YY\$bFG<RS.[\Y8`K1\38â<=ãD+0%+<ø5))à55âG%7è86nâîã{EFà+đód@kBíøââw%ææñâéýmü!wññ!êóö}lë	1.855 35502 43377 686	94bytes
2	Apa kabar hari ini?	Rahasia	19bytes	ìQlþ^Jc3S÷IT[JqJVJ2	1.816 93959 23614 502	19bytes
3	testing 123 aman	kunci123	19bytes	_ZaWRàæRã'!üJàl!	2.034 17348 86169 434	19bytes
4	Dia berkata: malam ini hujan deras!	hujan	35bytes	,^KþPMgUBbl/öNO TVWþWV^ðIcRVXþRMgKTð	0.568 12095 64208 984	35bytes
5	email@emailprovider.com	email	23bytes	JZBRX%RNJUQ]SXbNQF[âH\N	0.851 83858 87145 996	23bytes

No	Plain Text	Key Text	Ukuran Data	Chipertext	Durasi Enkripsi (sec)	Ukuran File enkripsi .txt
6	mulai dalam 1..2..3..	hitung	21byte s	U^`VWøLJ`V[øæè""ä êäè"	0.522 11666 10717 773	21bytes
7	semoga beruntung kawan	kawan	22byte s	^FdPULpYF`OkV\R pbBeLO	0.380 91349 60174 5605	22bytes
8	Hari ini adalah hari yang yang cerah untuk pergi	c3Rah	48byte s	+ëDJ÷L!;plGë>BPüä 3SQü,300ü,300üé 7SIKRG0\XáqQMUä ;	1.390 87486 26708 984	48bytes
9	Jangan menilai buku dari sampulnya	@123	34byte s	õí à!àQ %àää!âQê5ä'R\$í\$ã_ \$ì 0&á!9í	0.399 61576 46179 199	34bytes
10	berkumpul jam 7:30 malam	kumpul0	24byte s	MZ_[jY`aòZVYO"/ êYíWVZ	0.467 45705 60455 322	24bytes
11	belajar bersama di rumah saya nanti	b3l4j4r	35byte s	DçXêTêdyêQ&]ê_CR Pâö&gOêTS]êkCRZê X([	0.483 34813 11798 0957	35bytes
12	jangan mudah menyerah tetap bekerja keras	keras	41byte s	UF`HTYú_VWLMíNX Y^WSTSúffgLUíCXV JdKTôPWST^	1.456 21705 05523 682	41bytes
13	mencoba berkali-kali hingga berhasil	cobaterus	36byte s	PTPDcGSêUHAMB`N à`TOXýl]SY`TüQGS\ Fe^_	0.458 81485 93902 588	36bytes
14	perjuangan hampir selesai tetapi masih ada lagi tantangan didepan	panjang	65byte s	`F`TVOUWB\õIOT`J` õTSSUTOSpbLdB^Sp [HcJVöBRHíMOQJñ[ QObKOUH^pRSESW QO	0.449 12195 20568 8477	65bytes
15	semoga berhasil dan beruntung.	00re	30byte s	#ê_TëíGê"ZF#æ^úë î`úíêdZá\$gSè]	0.476 20987 89215 088	30bytes

### 3.2.2 Dekripsi

Hasil Enkripsi (Chipertext) akan di dekripsi (proses menjadi plaintext kembali), berikut hasil pengujian proses dekripsi :

Tabel 3: Tabel Hasil Dekripsi

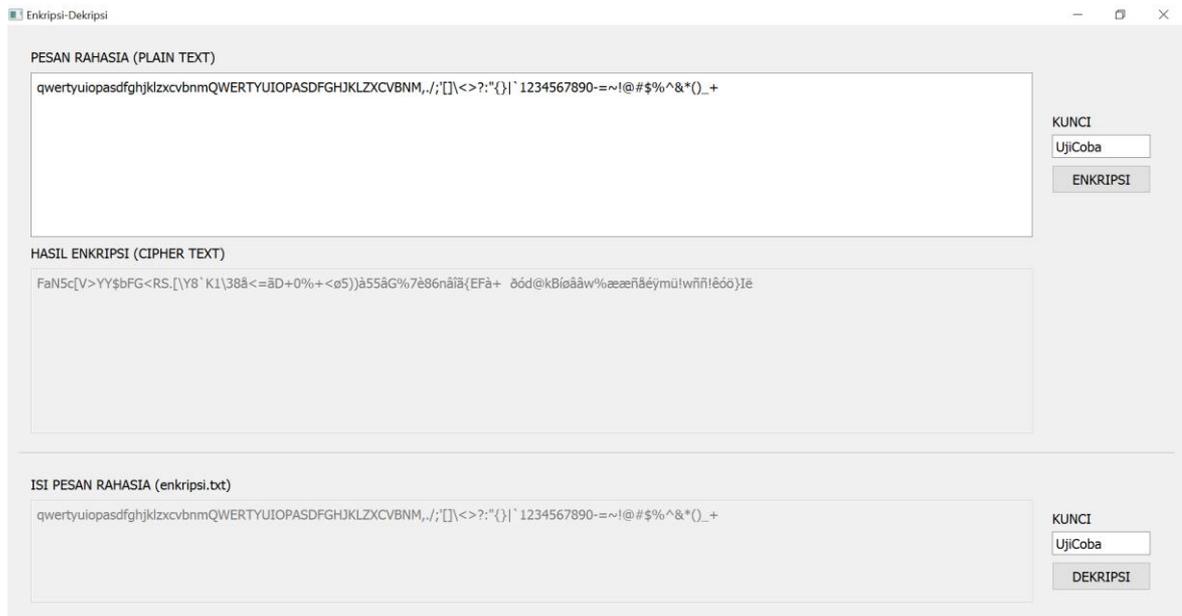
No	Chipertext	Key Text	Ukuran File enkripsi.txt	Plain Text	Durasi Dekripsi (sec)	Ukuran Data
1	FaN5c[V>YY\$bfG<RS.[\Y8`K1\38â<=ãD+0%+<ø5))à55âG%7è86nâîã{EFà+ đód@kBíøââw%ææñâ éÿmü!wññ!êóó}lë	UjiCoba	94 bytes	qwertyuiopasdfghjklzcvbnmQWERTYUIOPA SDFGHJKLZXCVBNM,./;[]\<>?:"{} `1234567890-=~!@#%&^*()_+	2.393 6431 4079 2846 7	94 bytes
2	ìQlp^JC3S÷IT[JqJVJ2	Rahasia	19bytes	Apa kabar hari ini?	1.816 9395 9236 1450 2	19bytes
3	_ZaWRàæRã'!úJái!	kunci123	16bytes	testing 123 aman	2.256 1337 9478 4546	19bytes
4	,^KþPMgUBbl/ðNOTVWþWV^ðicRVXþRMgKTð	hujan	35bytes	Dia berkata: malam ini hujan deras!	2.994 4682 1212 7685 5	35bytes
5	JZBRX%RNJUQ]SXbNQF[âH\N	Email	23bytes	email@emailprovider.com	1.540 8160 6864 9292	23bytes
6	U^`VWøL`V[øæè""ãêã è"	hitung	21bytes	mulai dalam 1..2..3..	2.358 5455 4176 3305 7	21bytes
7	^FdPULþYF`OkV\RþbbELO	kawan	22bytes	semoga beruntung kawan	0.429 8810 9588 6230 47	22bytes
8	+ëDJ÷Ll;þlGë>BPüä3S Qü,300ü,300üé7SIKR GO\XáqQMUâ;	c3Rah	48bytes	Hari ini adalah hari yang yang cerah untuk pergi	0.728 8463 1156 9213 9	48bytes
9	õí â!àQ %ààà!âQê5â'R\$í\$ã_šì O&á!9í	@123	34bytes	Jangan menilai buku dari sampulnya	0.495 6841 4688 1103 5	34bytes
10	MZ_[jY`aòZVYO"/ èYiWVZ	kumpul0	24bytes	berkumpul jam 7:30 malam	0.800 4124 1645	24bytes

No	Chipertext	Key Text	Ukuran File enkripsi.txt	Plain Text	Dura si Dekripsi (sec)	Ukuran Data
					81299	
11	DçXêTêdyêQ&]ê_CRPâ õ&gOëTS]êkCRZêX([	b3l4j4r	35bytes	belajar bersama di rumah saya nanti	0.5895669460296631	35bytes
12	UF`HTYú_VWLMíNXY^ WSTSúfGLUíCXVJdKTô PWST^	keras	41bytes	jangan mudah menyerah tetap bekerja keras	0.4988059997558594	41bytes
13	PTPDcGSêUHAMB`Nà`TOXýi]SY`TüQGS\Fe^_	cobaterus	36bytes	mencoba berkali-kali hingga berhasil	0.4608943462371826	36bytes
14	`F`TVOUWB\öIOT`J`öt SSUTOSpbLdB^Sp[HcJV öBRHiMOQñ[QObKO UH^pRSESWQO	panjang	65bytes	perjuangan hampir selesai tetapi masih ada lagi tantangan didepan	0.5263767242431641	65bytes
15	#ê_TèîîGê"ZF#æ^úëî`ú íêdZá\$gSè]	00re	30bytes	semoga berhasil dan beruntung.	0.4553852081298828	30bytes

### 3.2.3 Tampilan Aplikasi Kriptografi

Berikut tampilan aplikasi Vigenère cipher yang dikembangkan berikut dengan hasil enkripsi

dan dekripsi yang mencakup seluruh huruf, karakter, dan simbol yang terdapat pada keyboard QWERTY



Gambar 5. Tampilan Layar Aplikasi

#### 4. KESIMPULAN

Dari penelitian ini didapatkan kesimpulan bahwa aplikasi ini dapat melakukan enkripsi semua karakter yang berada pada tombol keyboard QWERTY dan uji coba didapatkan lama durasi proses enkripsi berdasarkan data uji pada Tabel 1 yaitu selama rata-rata 0.907407824198403 detik dengan ukuran data rata-rata sebesar 36.4 Byte, adapun hasil uji coba memiliki akurasi 100% sehingga plaintext yang dibuat menjadi ciphertext dapat dikembalikan menjadi plaintext kembali tanpa mengubah isi pesan, sehingga aplikasi yang dibuat dapat dikatakan berhasil karena dapat melakukan proses enkripsi-dekripsi dengan benar.

#### 5. SARAN

Saran untuk penelitian selanjutnya:

1. Memperbaiki tampilan UI sehingga lebih user friendly dan modern
2. Memungkinkan user untuk membuat kunci spesial sendiri
3. menambahkan karakter tidak hanya untuk ascii saja tetapi huruf lain seperti aksara mandarin, huruf dengan nada, dsb.

#### DAFTAR PUSTAKA

[1] Databoks, "Databoks. Chatting, Aplikasi Paling Digemari Masyarakat Indonesia.," Internet: <https://databoks.katadata.co.id/datapu>

[blish/2018/02/21/chatting-aplikasi-paling-digemari-masyarakat-indonesia](https://databoks.katadata.co.id/datapublish/2018/02/21/chatting-aplikasi-paling-digemari-masyarakat-indonesia) [26 Feb 2021].

- [2] Apriandala, Rio, 2013, "Sistem Keamanan Menggunakan Rubik Dengan Algoritma Kriptografi Encryption", Tugas Besar I Makalah Kriptografi, Universitas Bengkulu. 375 Hal
- [3] Y. Efrand, Asnawati, "Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher," J. Media Infotama, 2014.
- [4] Doni dan Abu Walad, "Caesar Cipher Vs Vigenère", Jurnal Komputer Bisnis, vol. 1, no. 3, Des 2012.
- [5] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," Inform. Mulawarman J. Ilm. Ilmu Komput., 2016, doi: 10.30872/jim.v10i1.23.
- [6] E. L. Hakim, Khairil, and F. H. Utami, "Aplikasi Enkripsi Dan Deskripsi Data Menggunakan Algoritma Rc4 Dengan Menggunakan Bahasa Pemrograman Php," J. Media Infotama, 2014.
- [7] Basri, "KRIPTOGRAFI SIMETRIS DAN ASIMETRIS DALAM PERSPEKTIF KEAMANAN DATA DAN KOMPLEKSITAS KOMPUTASI," J. Ilm. Ilmu Komput., 2016.
- [8] Hallim, Abd, "Pembuatan Perangkat Lunak Media Pembelajaran Kriptografi

Klasik”, Surabaya: Politeknik Elektronika Negeri, 2010, Hal. 11.

- [9] I. M. Arrijal, R. Efendi, and B. Susilo, “Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks,” *Pseudocode*, 2016, doi: 10.33369/pseudocode.3.1.69-82.
- [10] D. Hamdani and J. Junaidi, “Modifikasi Karakter Kode Pada Cipher Hill Menggunakan Kode ASCII,” *Eig. Math. J.*, 2020, doi: 10.29303/emj.v1i2.54.
- [11] PCMAG. *Definition of ASCII Chart* [Online]. Available: <https://www.pcmag.com/encyclopedia/term/ascii-chart>
- [12] Kuswari Hernawati, 2012, Implementasi Cipher Vigenere pada kode ASCII dengan Memanfaatkan Digit Desimal Bilangan Euler, Lumbung Pustaka UNY