SAIN TEKOM
ISSN 2088-1770 (Print)
ISSN 2503-3247 (Online)

JURNAL
SAINTEKOM
Sains, Teknologi, Komputer, dan Manajemen

PENERAPAN KOMBINASI METODE *VIGENERE CIPHER*, *CAESAR CIPHER* DAN SIMBOL BACA DALAM MENGAMANKAN PESAN

Veny Cahya Hardita [1], Eka Wahyu Sholeha [2]
[1)]Teknik Informatika, STMIK Palangka Raya
Jl. G. Obos No.114, Palangka Raya, Kalimantan Tengah
[2)]Teknologi Informasi, Politeknik Negeri Tanah Laut
Jl. A. Yani No.Km.06, Kec. Pelaihari, Kabupaten Tanah Laut, Kalimantan Selatan
Email: : vencahya@gmail.com, ekawahyus@politala.ac.id

ABSTRACT

The concept that an important information cannot be known by parties who don't have rights can be done by making the confidentiality of data using cryptography. Safety in vigenere ciphers depends on the number of keys used, the more the number of keys, the wider the key space. While Caesar Cipher or often also called caesar code is a classic coding system based on simple substitution. This study uses a combination of Vigenere Cipher and Caesar Cipher algorithms so that the security of the contents of the message is protected stronger and safer so that if the message sent is tapped by someone who is not responsible then the hijacker has difficulty knowing contents of the message. So that the confidentiality and authenticity of message is up to the recipient. In this study successfully implemented both methods and has an output in the form of a reading symbol, not letters.

***Keyword** : Crypthography, Vigenere Cipher, Caesar Cipher.*

ABSTRAK

Konsep agar sebuah informasi penting tidak dapat diketahui oleh pihak yang tidak memiliki hak dapat dilakukan dengan cara membuat kerahasiaan data menggunakan kriptografi. Keamanan pada vigenere cipher bergantung pada jumlah kunci yang digunakan semakin banyak jumlah kunci maka semakin luas ruang kunci. Sedangkan caesar cipher atau sering disebut juga sandi caesar adalah sistem persandian klasik yang berbasis substitusi sederhana. Penelitian ini menggunakan kombinasi algoritma Vigenere Cipher dan Caesar Cipher agar keamanan isi pesan terproteksi lebih kuat dan aman sehingga apabila pesan yang dikirimkan dibajak ataupun disadap oleh orang yang tidak bertanggung jawab maka si pembajak kesulitan utnuk mengetahui isi pesannya. Sehingga kerahasiaan dan keaslian pesan terjaga sampai kepada penerima. Keunggulan dari penelitian ini yaitu menerapkan kombinasi vigenere cipher dan caesar cipher pada vigenere cipher tidak hanya menggunakan satu kunci saja tetapi menggunakan dua kunci dalam pengamanannya serta menggunakan hasil keluaran berupa simbol bukan huruf untuk memperkuat pengamanan isi pada suatu pesan.

Kata kunci : Kriptografi**,** *Vigenere Cipher, Caesar Cipher.*

1. PENDAHULUAN

Teknologi informasi digunakan di hampir semua aspek kehidupan manusia modern saat ini. Kemajuan teknologi memungkinkan dalam hal bertukan informasi, berbagi cerita, tatap muka secara online, hingga melakukan penyimpanan menggunakan media digital melalui jaringan internet. Dalam proses pertukaran informasi dengan melalui jaringan internet dapat meningkatkan resiko penyadapan informasi penting (Silangen, 2017)

Salah satu cara menjaga informasi agar tidak diketahui oleh siapapun kecuali pihak yang memiliki akses dapat dilakukan dengan cara membuat konsep kerahasiaan data. Untuk menjaga keamaanan data dapat menggunakan kriptografi. Menurut bahasa Yunani kata kriptografi dibagi menjadi dua, yaitu kripto dan graphia. Kripto sendiri memiliki arti *secret* (rahasia) dan graphia berarti *writing* (tulisan) (Kurniawan, 2014).

Enkripsi merupakan salah satu cabang ilmu dari kriptografi. Enkripsi merupakan suatu proses merubah suatu data atau informasi teks kedalam bentuk teks lain yang tidak dapat dipahami. Pada proses enkripsi dapat menggunkan kunci simetris dan kunci asimetris. Ada beberapa algoritma yang dapat digunakan untuk enkripsi menggunakan kunci simetris, tiga diantaranya yaitu *Caesar Cipher*, *Vigenere Cipher* dan *affine Cipher*.

Pada penelitian (Silangen & Pardede, 2018) aplikasi yang bisa digunakan sebagai pengaman pada pesan teks yang bersifat rahasia. Pada penelitian kunci dan pesan teks dienkripsi terlebih dahulu, dimana kunci dienkripsi menggunakan metode *vigenere* sedangkan pesan teks dienkripsi dengan menggunakan metode *triple columner*. Dengan adanya kombinasi dua metode tersebut maka pesan rahasia bisa dikirimkan dengan aman.

Penelitian (Gupta & Kumar, 2019) menyebutkan bahwa agar data dapat dibuat lebih aman dengan menerapkan teknik lipatan berlipat ganda untuk mengubah teks biasa menjadi sandi teks dan kemudian menanamkannya ke media lain dengan menerapkan teknik steganografi. Penelitian yang dilakukan menetapkan pendekatan *ensemble yang* dapat membuat fitur keamanan lebih kuat.

Penelitian (Susanto & Solichin, 2018) mengimplementasikan algoritma kriptografi *Caesar Cipher* dan Vigenere Cipher ke database sistem penggajian untuk mengamankan data rahasia

perusahaan dan pegawai yang nantinya akan digunakan oleh PT. Kemasindo Cepat Nusantara untuk mengurangi kemungkinan terjadinya pencurian data atau informasi.

Penelitian (Nasution, et al., 2017) membahas keamanan dengan vigenere ciphertext, lalu ciphertext yang diproduksi akan diproses lagi menggunakan algoritma Goldbach kode. Dengan menerapkan algoritma, Goldbach mengkode hasil dari jalannya pengamanan data menggunakan *Vigenere Cipher* menjadi lebih sulit menebak teks aslinya meskipun menggunakan metode kasiski yang akan didapat adalah pesan dari karakter yang berbeda.

Berdasarkan beberapa referensi penelitian diatas, maka penulis tertarik menggabungkan dua algoritma menggunakan kunci simetris yaitu *Caesar Cipher* dengan *Vigenere Cipher* dan simbol baca. Dengan tujuan agar sebuah informasi yang dikirim dapat dibuat lebih aman dan mengurangi kemungkinan terjadinya pencurian informasi. Penelitian yang dibuat untuk mengimplementasikan dan menggabungkan dua metode dengan *output* berupa simbol baca. Pesan yang diambil hanya sebagai contoh pengimplementasian untuk membuktikan bahwa pesan tersebut bisa dijadikan sebuah pesan rahasia yang tidak bisa dipecahkan oleh orang-orang biasa.

2. METODE

Metode yang digunakan dalam penelitian ini adalah sebagai berikut :

a. Studi Pustaka

Penelitian ini menggunakan metode studi pustaka yaitu tinjauan literatur untuk mendapatkan referensi tentang kriptografi, dan metode-metode seperti Vigenere Cipher dan Caesar Cipher.

b. *Action Planning*

Action planning merupakan suatu kegiatan dalam menentukan metode yang akan diambil dalam proses enkripsi kriptografi pada penelitian ini. Metode yang akan diambil adalah kombinasi *Vigenere Cipher* dan *Caesar Cipher*.

Sandi vigenere atau disebut juga *Vigenere Cipher* merupakan sistem sandi poli-alphabetik yang mengenkripsi sekaligus sebuah teks yang terdiri dari beberapa huruf. Layaknya *Caesar Cipher*, *vigenere cipher* juga menggunakan substitusi fungsi *shift.* Keamanan pada vigenere cipher bergantung pada jumlah kunci yang digunakan, semakin banyak jumlah kunci maka semakin luas ruang

kunci. Kelemahan sandi ini mencari terlebih dahulu panjang kunci vigenere dengan mencari rangkaian karakter yang berulang atau sering disebut pengujian (Sadikin, 2012).

Caesar Cipher atau sering disebut juga sandi caesar adalah sistem persandian klasik yang berbasis substitusi sederhana. Enkripsi dan dekripsi sistem persandian caesar menggunakan operasi shift yang mensubtitusi suatu huruf menjadi huruf pada daftar alfabet berada di –k sebelah kanan atau sebelah kiri huruf tersebut.

c. *Action Taking*

Action taking merupakan kegiatan dalam mengimplementasikan metode yang diambil ke dalam program kriptografi.

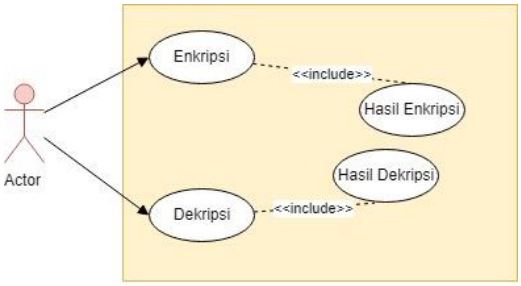
d. *Evaluating*

Evaluasi merupakan proses penyimpulan terhadap penelitian yang dilakukan

3. HASIL DAN PEMBAHASAN

a. *USE CASE DIAGRAM*

Dalam penelitian ini menggunakan *use case diagram* untuk mendefinisikan tentang fitur yang akan digunakan pada sistem. *Use case diagram* digunakan untuk menggambarkan hal apa saja yang dapat dilakukan oleh aktor/pengguna dari sistem. Pada Gambar 1 akan ditunjukan sebuah use case dari sistem kriptografi penelitian ini.



Gambar 1. *Use Case Diagram* Sistem Kriptografi

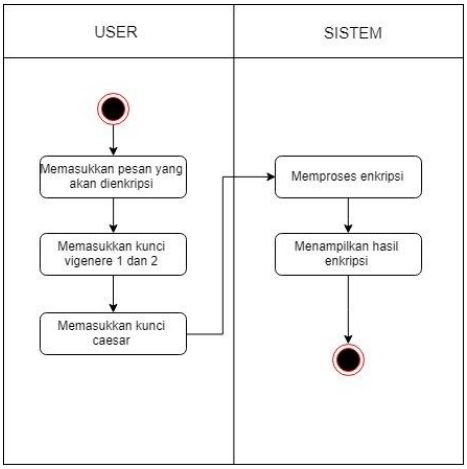
Pada Gambar 1 menggambarkan *use case diagram* dari sistem kriptografi yang dibangun. Dijelaskan bahwa aktor merupakan pengguna dari sistem, pengguna sistem dapat mengakses sistem secara keseluruhan. Hal yang dapat dilakukan oleh aktor adalah enkripsi dan dekripsi. Setelah melakukan enkripsi atau dekripsi, sistem akan menampilkan hasil dari enkripsi atau dekripsi yang telah dilakukan oleh si aktor.

b. *ACTIVITY DIAGRAM*

Activity diagram merupakan pemodelan dari proses-proses yang terjadi pada sistem. Berikut merupakan activity diagram dari sistem kriptografi penelitian ini :

1) *Activity Diagram* Enkripsi

Activity Diagram enkripsi menggambarkan proses dari enkripsi untuk metode Vigenere dan Caesar dengan alur seperti gambar 2.

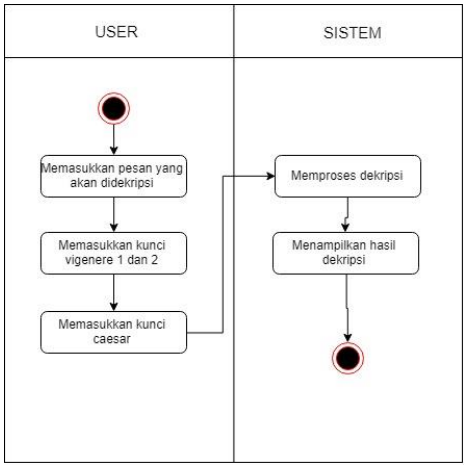


Gambar 2. *Activity Diagram* Enkripsi

Gambar 2 merupakan activity diagram enkripsi, dari Gambar 2 user dapat menginputkan pesan yang akan di enkripsi kemudian menginputkan kunci vigenere 1 dan 2 serta kunci caesar. Setelah itu sistem akan memproses enkripsi dan menampilkan hasil enkripsi berupa simbol-simbol dari tanda baca.

2) *Activity Diagram Dekripsi*

Activity Diagram dekripsi menggambarkan tentang activity diagram dari proses dekripsi. Gambaran proses dekripsi digambarkan pada Gambar 3.



Gambar 3. *Activity Diagram* Dekripsi

Pada Gambar 3 User dapat menginputkan pesan yang akan didekripsi dan menginputkan kunci vigenere dan kunci caesar. Setelah itu sistem akan melakukan proses dekripsi dan kemudian akan menampilkan hasil dari dekripsi sistem.

c. SIMBOL BACA

Simbol baca yang digunakan untuk menyamarkan pesan setelah pesan di enkripsi adalah seperti Tabel 1.

Tabel 1. Simbol Tanda Baca

A	0	1	2	3	4	5	6	7	8	9	10	11	12
S	!	"	#	$	%	&	(	*	+	)	-	.	/
A	13	14	15	16	17	18	19	20	21	22	23	24	25
S	<	,	?	@	`	:	=	>	[	;	^	]	~

d. *VIGENERE CIPHER*

Terdapat suatu data atau pesan yang akan disandikan dengan menggunakan algoritma Vigenere. Teks data atau pesan awal yang akan di sandikan yaitu HABIS GELAP TERBITLAH TERANG dengan kunci

pertama KARTINI dan kunci kedua WANITA. Berikut adalah proses Enkripsinya dengan algoritma vigenere.

Teks awal (plaintext) = HABIS GELAP TERBITLAH TERANG

Kunci (*Key*) 1 = KARTINI

Kunci (*Key*) 2 = WANITA

1) Enkripsi *Vigenere Cipher*

Enkripsi *vigenere cipher* merupakan proses yang pertama untuk menjadkan kalimat "HABIS GELAP" menjadi sebuah simbol baca.

Tabel 2. Enkripsi Vigenere HABIS GELAP

PT	H	A	B	I	S	G	E	L	A	P
PA	7	0	1	8	18	6	4	11	0	15
K	K	A	R	T	I	N	I	K	A	R
PA	10	0	17	19	8	13	8	10	0	17
+	17	0	18	27	26	19	12	21	0	32
K 2	W	A	N	I	T	A	W	A	N	I
PA	22	0	13	8	19	0	22	0	13	8
+	39	0	31	35	45	19	34	21	13	40
M	13	0	5	9	19	19	8	21	13	14
CS	<	!	&	)	=	=	+	[	<	,

Enkripsi Vigenere Cipher dengan kalimat "TERBITLAH TERANG" digambarkan dengan Tabel 3.

PT	T	E	R	B	I	T	L	A	H	T	E	R	A	N	G
PA	19	4	17	1	8	19	11	0	7	19	4	17	0	13	6
K	T	I	N	I	K	A	R	T	I	N	I	K	A	R	T
PA	19	8	13	8	10	0	17	19	8	13	8	10	0	17	19
+	38	12	30	9	18	19	28	19	15	32	12	27	0	30	25
K 2	T	A	W	A	N	I	T	A	W	A	N	I	T	A	W
PA	19	0	22	0	13	8	19	0	22	0	13	8	19	0	22
+	57	12	52	9	31	27	47	19	37	32	25	35	19	30	47
M	5	12	0	9	5	1	21	19	11	6	25	9	19	4	21
CS	&	/	!	)	&	"	[	=	.	(	~	)	=	%	[

Tabel 3. Enkripsi Vigenere TERBITLAH TERANG

Pada Tabel 2 dan Tabel 3 merupakan proses perhitungan Enkripsi dengan menggunakan *Vigenere Cipher*. Dengan hasil akhir Enkripsi:

<!&)==+[<,&/!)&"[=.(~)=%[

Keterangan Tabel:

PT : *Plain Text*

PA : Posisi Abjad

K : *Key*

M : *Mod*

CS/CT : *Cipher Symbol/Cipher Text*

2) Dekripsi *Vigenere Cipher*

Dekripsi *Vigenere Cipher* untuk kalimat "HABIS GELAP" digambarkan oleh Tabel 4:

Tabel 4. Dekripsi *Vigenere Cipher* HABIS GELAP

CS	<	!	&	)	=	=	+	[	<	,
M	13	0	5	9	19	19	8	21	13	14
K2	W	A	N	I	T	A	W	A	N	I
PA	22	0	13	8	19	0	22	0	13	8
K	K	A	R	T	I	N	I	K	A	R
PA	10	0	17	19	8	13	8	10	0	17
-	-19	0	-25	-18	-8	6	-22	11	0	-11
M	7	0	1	8	18	6	4	11	0	15
PT	H	A	B	I	S	G	E	L	A	P

Pada Tabel 4 menunjukkan bahwa dekripsi dari hasil enkripsi dari HABIS GELAP dan memiliki hasil yang sama.

Dekripsi *Vigenere Cipher* untuk kalimat "TERBITLAH

TERANG" digambarkan oleh Tabel 5.

Tabel 5. Dekripsi *Vigenere Cipher*
TERBITLAH TERANG

CS	&	/	!	)	&	"	[	=	.	(	~	)	=	%	[
M	5	12	0	9	5	1	21	19	11	6	25	9	19	4	21
K2	T	A	W	A	N	I	T	A	W	A	N	I	T	A	W
PA	19	0	22	0	13	8	19	0	22	0	13	8	19	0	22
K	T	I	N	I	K	A	R	T	I	N	I	K	A	R	T
PA	19	8	13	8	10	0	17	19	8	13	8	10	0	17	19
-	-33	4	-35	1	-18	-7	-15	0	-19	-7	4	-9	0	-13	-20
M	-7		-9		8	19	11		7	19		17		13	6
PT	T	E	R	B	I	T	L	A	H	T	E	R	A	N	G

Pada Tabel 5 menunjukkan bahwa dekripsi dari hasil enkripsi dari HABIS GELAP dan memiliki hasil yang sama.

e. *CAESAR CIPHER*

Setelah dilakukan enkripsi dengan *vigenere cipher*, langkah selanjutnya adalah menyandikan lagi dengan *Caesar Cipher*. Diketahui teks hasil enkripsi vigenere adalah:

<!&)==+[<,&/!)&"[=.(~)=%[

Maka proses enkripsi dengan sandi caesar:

1) Enkripsi *Caesar Cipher* :

Rumus : E(P)=C, C=P+K Mod 26 (1)

Pada persamaan 1 memiliki keterangan sebagai berikut:

E(P) : Enkripsi

P : *Plaintext* (Teks awal)

K :*Key* (Jumlah pergeseran)

Teks Awal :

<!&)==+[<,&/!)&"[=.(~)=%[

Kunci (*Key*) : 7

Tabel 6. Enkripsi *Caesar Cipher*

CT	<	!	&	)	=	=	+	[	<	,
PA	13	0	5	9	19	19	8	21	13	14
K7+	20	7	12	16	26	26	15	28	20	21
M	20	7	12	16	0	0	15	2	20	21
CS2	>	*	/	@	!	!	?	#	>	[

Proses enkripsi *Caesar Cipher* dengan Ciphertext &/!)&"[=.(~)=%[digambarkan oleh Tabel 7.

Tabel 7. Enkripsi *Caesar Cipher*

CT	&	/	!	)	&	"	[	=	.	(	~	)	=	%	[
PA	5	12	0	9	5	1	21	19	11	6	25	9	19	4	21
K7+	12	19	7	16	12	8	28	26	18	13	32	16	26	11	28
M	12	19	7	16	12	8	2	0	18	13	6	16	0	11	2
CS2	/	=	*	@	/	+	#	!	:	<	(	@	!	.	#

Tabel 6 dan Tabel 7 merupakan hasil dari enkripsi *Caesar Cipher* yang sebelumnya sudah di enkripsikan dengan *Vigenere Cipher*. Jadi hasil dari kedua tabel tersebut merupakan hasil yang sudah di proses dengan menggunakan dua metode.

Hasil Enkripsi *Caesar Cipher* :

>*/ @ ! ! ? # > [/ = * @ /+#!:(@!.#

2) Proses Dekripsi :

Rumus : D(C)=P, P=C-K mod 26 (2)

D(C) : Dekripsi

C : *Ciphertext* (Teks akhir)

K : *Key* (Kata / Kalimat)

Ciphertext 2 :

>*/ @ ! ! ? # > [/ = * @ /+#!:(@!.

Kunci (*Key*) : 7

Hasil dekripsi seperti pada tabel 8.

Tabel 8. Dekripsi *Caesar Cipher*

CT2	>	*	/	@	!	!	?	#	>	[
M	20	7	12	16	0	0	15	2	20	21
K7	13	0	5	9	-7	-7	8	-5	13	14
PM	13	0	5	9	19	19	8	21	13	14
CT1	<	!	&	)	=	=	+	[	<	,

Hasil Dekripsi seperti pada tabel 9.

Tabel 9. Dekripsi *Caesar Cipher*

CT2	/	=	*	@	/	+	#	!	:	<	(	@	!	.	#
M	12	19	7	16	12	8	2	0	18	13	6	16	0	11	2
K7	5	12	0	9	5	1	-5	-7	11	6	-1	9	-7	4	-5
PM	5	12	0	9	5	1	21	19	11	6	25	9	19	4	21
CT1	&	/	!	)	&	“	[	=	.	(	~	)	=	%	[

Pada Tabel 8 dan Tabel 9 merupakan hasil dekripsi yang telah didapatkan dari proses dekripsi *Vigenere Cipher*. Hasil dekripsi :

<!&)==+[<,&/!)&”[=.(~)=%[

f. IMPLEMENTASI PROGRAM

Berikut merupakan hasil implementasi sistem kriptografi yang berhasil dibangun dengan menggunakan bahasa pemrograman PHP.

1) Tampilan *Input* Enkripsi

Tampilan *input* enkripsi menampilkan antarmuka awal kriptografi bagian enkripsi. Tampilan seperti pada gambar 4.

Gambar 4. Tampilan *Input* Kriptografi Enkripsi

Pada Gambar 4 tampilan ini user dapat memasukkan pesan teks yang akan dienkripsi beserta kata kunci dan panjang kunci. Pada *button* “enkripsi”, pesan dan kunci yang telah dimasukkan akan diproses oleh sistem dan menghasilkan sebuah pesan yang telah dienkripsikan yaitu *ciphertext*.

2) Tampilan *Output* Enkripsi

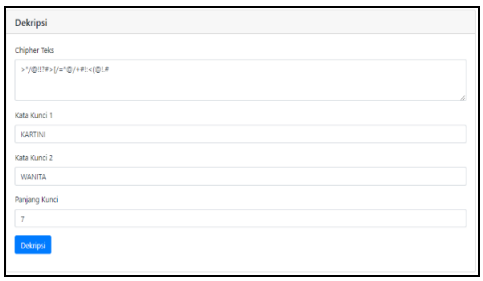
Tampilan *output* enkripsi menampilkan antarmuka *output* dari proses enkripsi sebelumnya. Tampilan seperti pada gambar 5.

Gambar 5. Tampilan *Output* Kriptografi Enkripsi

Pada Gambar 5 hasil output menghasilkan *ciphertext* berupa simbol baca.

3) Tampilan *Input Dekripsi*

Proses dekripsi merupakan proses pengembalian *ciphertext* ke teks awal. Tampilan seperti pada gambar 6.



Gambar 6. Tampilan *Input* Kriptografi Dekripsi

Pada Gambar 6 menampilkan antarmuka untuk mengembalikan pesan yang telah dienkripsi ke pesan awal. Dengan memasukkan pesan yang telah dienkripsi serta kuncinya, maka pesan akan diproses menuju pengembalian pesan awal. Tampilan *Output* Dekripsi

Tampilan *output* dekripsi menampilkan antarmuka dari *output* dekripsi. Tampilan seperti pada gambar 7.

Gambar 7. Tampilan *Output* Kriptografi

Pada Gambar 7 pesan yang telah diproses dekripsinya akan ditampilkan seperti pada gambar 7.

4. SIMPULAN

Dalam menjaga kerahasiaan suatu pesan dapat digunakan kombinasi algoritma Vigenere Cipher dan Caesar Cipher agar keamanan isi pesan terproteksi lebih kuat dan aman sehingga apabila pesan yang dikirimkan dibajak ataupun disadap oleh orang yang tidak bertanggung jawab maka si pembajak kesulitan untuk mengetahui isi pesannya. Pesan yang telah di dekripsi dari kombinasi vigenere cipher dan caesar cipher dapat dibaca dan dipahami oleh penerima pesan. Hanya pengirim dan penerima pesan yang mengetahui kunci dari pesan tersebut. Sehingga kerahasiaan dan keaslian pesan terjaga sampai kepada penerima.

Dari contoh proses kriptografi menggunakan kalimat “HABIS GELAP TERBITLAH TERANG” didapatkan suatu hasil yaitu >*/@!!?#>[/=*@/+#!:<(@!# sehingga orang lain yang tidak berhak untuk menerima pesan rahasia tersebut kesulitan dalam membaca pesannya. Dan hanya penerima yang bisa membaca pesan tersebut dengan melalui proses Dekripsi.

Keunggulan dari penelitian ini yaitu menerapkan kombinasi vigenere cipher dan caesar cipher, pada vigenere cipher tidak hanya menggunakan 1 kunci saja tetapi menggunakan 2 kunci dalam pengamanannya serta menggunakan hasil keluaran berupa

simbol bukan huruf untuk memperkuat pengamanan isi pada suatu pesan.

DAFTAR PUSTAKA

Gupta, A. & Kumar, A., 2019. *Information Security Using the Ensemble Approach of Steganography and Cryptography.* India, Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), pp. 66-73.

Kurniawan, Y. M., 2014. *Kriptografi: Keamanan Internet dan Jaringan Komunikasi.* Bandung: Informatika.

Nasution, S. D., Ginting, G. L., Syahrizal, M. & Rahim, R., 2017. Data Security Using Vigenere Cipher and Goldbach Codes Algorithm. *International Journal of Engineering Research & Technology (IJERT),* 6(1), pp. 360-363.

Sadikin, R., 2012. *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java.* Yogyakarta: Andi.

Silangen, M., 2017. *Enkripsi dan Penyembunyian Data Dalam File Audio Menggunakan Triple Des dan Parity Coding,* Yogyakarta: Universitas Gajah Mada.

Silangen, M. & Pardede, A. M. H., 2018. Pengamanan File Teks Menggunakan Kombinasi Algoritma Viginere Cipher dan Triple Columner. *Jurnal Ilmiah Behongang,* 1(2), pp. 38-42.

Susanto, I. A. & Solichin, A., 2018. Enkripsi Data Penggajian Dengan Algoritma Caesar Cipher dan Vigenere Cipher Pada PT. Kemasindo Cepat Nusantara. *SKANIKA,* 1(1), pp. 399-404.