p-ISSN 2087-1716
e-ISSN 2548-7779

ILKOM Jurnal Ilmiah Volume 11 Nomor 3 Desember 2019
Terakreditasi peringkat 3 SK. No.28/E/KPT/2019

PENGAMANAN *FILE* DOKUMEN MENGGUNAKAN KOMBINASI METODE SUBTITUSI DAN *VIGENERE CIPHER*

Sarwo Budi[1], Arif Budimansyah Purba[2], Jajang Mulyana[3]
[1]sarwobudi58@gmail.com, [2]arifbudimansyahpurba@gmail.com, [3]ja2ngm@gmail.com
[1,2,3]STMIK Kharisma Karawang

Abstrak

Kriptografi adalah metode pengamanan data menggunakan algoritma yang banyak dikembangkan secara berkelanjutan hingga sekarang, kriptografi menawarkan keamanan berupa kerahasiaan data, misalnya kerahasiaan data yang dihasilkan melalui algoritma enkripsi yang mengacak informasi pribadi sehingga tidak dapat terbaca maupun dipecahkan oleh pihak yang tidak berkepentingan. Salah satunya adalah algoritma subtitusi dan *vigenere cipher* merupakan metode klasik yang digunakan untuk pengamanan data. Kombinasi metode algoritma tersebut menjadi solusi untuk keamanan ganda sebagai proteksi file, Dengan menggunakan aplikasi kriptografi pengamanan data kombinasi algoritma dua metode tersebut menghasilkan file data yang memberikan keamanan lebih pada file teks sehingga tidak mudah dan sulit untuk dipecahkan.
Kata kunci: Kriptografi, *Subtitusi*, *Vigenere cipher*, *SDLC Waterfall*

Abstract

Cryptography is a method of securing data using algorithms that have been developed continuously until now. Cryptography offers security in the form of data confidentiality, for example the confidentiality of data generated through encryption algorithms that scrambles personal information so that it cannot be read or solved by unauthorized parties. One of them is the substitution algorithm and the vigenere cipher is a classic method used for data security. The combination of these algorithm methods becomes a solution for double security as file protection. By using a cryptographic application for data security, the combination of the two method algorithms produces a data file that provides more security to the text file so that it is not easy and difficult to solve.
Keywords: Cryptography, Subtitution, Vigenere cipher, SDLC Waterfall

1. Pendahuluan

Kemajuan teknologi *internet*, media digital seperti gambar, audio, video dan file teks dapat dibagi dan dikirimkan melalui Internet dengan lebih mudah dengan bermacam media. Salah satu tantangan utama dalam berbagi dan mentransmisikan semua jenis informasi melalui saluran publik adalah keamanan data [1]. Muncul kebutuhan untuk melindungi informasi yang akan dikirimkan dari penyadap dan pihak yang tidak berwenang. Proses dalam melindungi suatu informasi tersebut dapat dilakukan dengan ilmu atau teknik menyembunyikan pesan dengan suatu cara tertentu sehingga selain si pengirim dan si penerima, tidak ada orang lain yang mengetahui atau menyadari adanya suatu pesan rahasia. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi [2].

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi [3]. Metode kriptografi adalah alat untuk menawarkan keamanan data. Kriptografi menyediakan fitur seperti kerahasiaan, keaslian, dan integritas data. Misalnya, kerahasiaan data dihasilkan melalui algoritma enkripsi yang mengacak/mencampur informasi pribadi sehingga menjadi tidak dapat dibaca oleh pihak selain penerima yang dimaksud [4]. Enkripsi merupakan proses konversi data dari data biasa menjadi data baru yang disandikan, sedangkan deskripsi yaitu proses pengembalian data yang sudah disandikan menjadi data semula atau data asli [5]. Salah satu metode kriptografi adalah *Vigener chiper* yang merupakan metode untuk proses membuat kata sandi dari sebuah teks berdasarkan huruf-huruf pada kata kunci deretan sandi Caesar [6] dan sandi *Vigenère* sebenarnya merupakan pengembangan dari sandi Caesar. Pada sandi Caesar, setiap huruf teks terang digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalnya pada sandi Caesar dengan geseran 3, A menjadi D, B menjadi E and dan seterusnya. Sandi *Vigenère* terdiri dari beberapa sandi Caesar dengan nilai geseran yang berbeda [7].

Metode ini tidak menjamin data akan aman apabila mendapatkan dengan jenis serangan *brute force attack*, maka perlu adanya proteksi keamanan lebih untuk keamanan data tersebut yaitu

DOI: https://doi.org/10.33096/ilkom.v11i3.477.222-230

menggunakan metode Subtitusi. Metode substitusi merupakan proses dimana sebuah data diubah menjadi data baru yang bersifat acak [8][9]. Tahap pertama pesan yang disisipkan akan disandikan dengan algoritma substitusi. Untuk mengacak pesan menggunakan algoritma substitusi dimana proses enkripsi tersebut akan sama dilakukan menggunakan perhitungan enkripsi substitusi sampai karakter terakhir. Kemudian dilanjutkan dengan tahap kedua yaitu pengacakan menggunakan algoritma *vigenere cipher*. Selanjutnya *vigenere cipher* menggabungkan *plaintext* (*ciphertext-1*) dengan kunci sehingga menghasilkan ciphertext yang baru (*ciphertext-2*).

Dalam penelitian ini pengamanan data menggunakan penggabungan dua metode kriptogafi, dapat menghasilkan keamanan data yang lebih maksimal untuk proteksi data. Untuk perancangan sistem dalam penelitian ini menggunakan metode *System Development Life Cycle* (SDLC) *Waterfall* [10]. Dengan menggunakan dua metode kriptografi sebagai pengamanan data, maka diharapkan hal ini dapat menjadi solusi terhadap serangan kriptanalisis. Berdasarkan hal ini maka penelitian ini akan melakukan pengamanan file dokumen menggunakan kombinasi metode subtitusi dan *vigenere cipher.*

2. Metode

Untuk membangun aplikasi Kriptografi Pengamanan data menggunakan penggabungan metode subtitusi dam *vigenere cipher* ini menggunakan metode SDLC *Waterfall* dimana dalam penelitian ini hanya akan digunakan empat tahapan dari kelima tahapan pada metode SDLC *Waterfall* yaitu tahap perencanaan projek, tahap analisis, tahap perancangan dan tahap implementasi. Tahapan SDLC *Waterfall* adalah sebagai berikut:

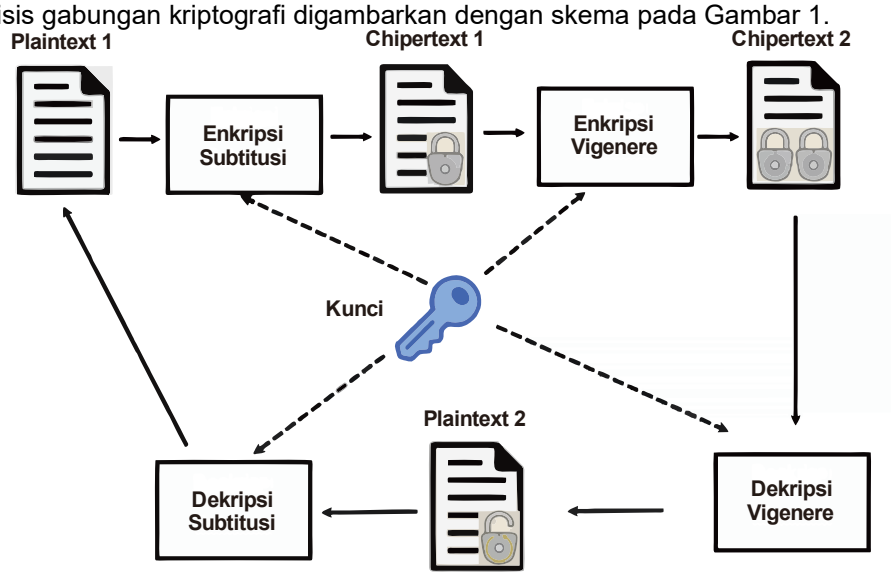
Tahap Perencanaan Projek

Pada tahapan ini dilakukan penelitian terlebih dahulu untuk menyaring data serta informasi yang terkait. Teknik pengumpulan data yang dilakukan adalah dengan melakukan studi literatur/pustaka baik melalui buku ataupun jurnal dan wawancara terhadap bagian pelayanan terkait. Pada tahapan ini, terdapat beberapa aktifitas yang harus dilakukan,diantaranya: Definisikan Masalah, Pengumpulan Data, Menganalisis Teori, Pembuatan Jadwal, Mencari Solusi dan Mendefinisikan kebutuhan.

Tahap Analisis

1. Analisis Proses

Analisis gabungan kriptografi digambarkan dengan skema pada Gambar 1.



Gambar 1. Skema kombinasi metode subtitusi dan vigenere kriptografi

Proses enkripsi terdiri dari sebuah algoritme dan sebuah kunci dengan nilai yang terlepas dari pesan asli (*plaintext*) dan mengontrol algoritme yang dipakai. Penerapan algoritme akan menghasilkan output yang berbeda sesuai dengan kunci yang digunakan. Mengubah kunci berarti mengubah output dari algoritme yang dipakai. Setelah *chipertext* dihasilkan, *chipertext* tersebut dapat diubah kembali menjadi pesan asli dengan algoritme dekripsi dan dengan kunci yang sama seperti yang digunakan pada saat enkripsi [11][12].

DOI: https://doi.org/10.33096/ilkom.v11i3.477.222-230

2. Analisis Sistem

Analisis sistem aplikasi kriptografi menggunakan *Object Oriented Analysis* (OOA) yaitu :

1. *System Activities* (*Actor Description and Use Case Description, Use Case Diagram, Scenario Use Case*).
2. *Class Diagram (Class Definition, Class Relation).*
3. *Object Interaction (Sequence Diagram).*
4. *Object Behavior (Activity Diagram).*

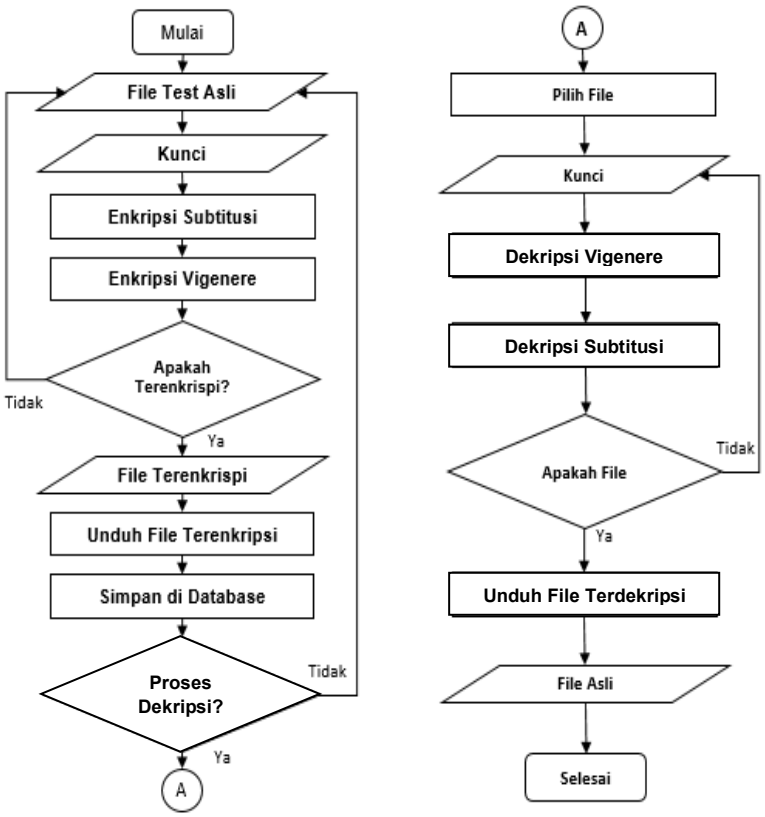
Tahap Perancangan

Tahapan perancangan yang dilakukan oleh peneliti adalah desain berbasis *Object Oriented Design* (OOD) yang terdiri dari :

1. Desain Proses

   Rancangan logika pemrosesan data yang akan disajikan menggunakan *flowchart* dalam menggambarkan urutan pada aplikasi ini [13].

   Berikut Gambar 2. diagram *flowchart* proses kriptografi dengan dua metode :



Gambar 2. *Flowchart* Kriptografi

2. Desain Antarmuka

   Aplikasi biasanya berupa perangkat lunak yang berbentuk *software* yang berisi kesatuan perintah atau program yang dibuat untuk melaksanakan sebuah pekerjaan yang diinginkan [14]. Untuk itu diperlukan rancangan tampilan aplikasi yang akan dioperasikan oleh pengguna (*user*).

Tahap Implementasi

Tahapan implementasi merupakan tahap pembuatan program termasuk penulisan kode program. Pada Tahapan ini meliputi:

1. Instalasi Sistem
2. Pelatihan Prosedural
3. Pengujian Sistem (pengujian *whitebox* dan *blackbox).*

   Software testing merupakan sebuah alat yang menjamin kualitas perangkat lunak yang diterapkan untuk mengontrol kualitas produk perangkat lunak sebelum penyerahan atau instalasi ditempat pengguna. *Software* testing dapat diklasifikasikan berdasarkan konsep pengujian, yaitu *black box* (fungsional) testing dan *whitebox* (struktural) testing [15].

DOI: https://doi.org/10.33096/ilkom.v11i3.477.222-230

3. Hasil dan Pembahasan

Dalam penelitian kriptografi dengan media pesan file teks format *txt* sebagai *Plaintext* yang di acak dengan algoritma kriptografi substitusi dan *vigenere cipher*. Pesan teks (*plaintext)* akan dienkripsi menggunakan algoritma substitusi *menghasilkan ciphertext* yang akan dienkripsi lagi menggunakan *vigenere cipher* dengan kunci tertentu menghasilkan ciphertext-2. Hasil dari *ciphertext-*2 dan selanjutnya di simpan di dalam file *database.*

Sesuai dengan alur diagram *flowchart* analisis untuk pengamanan file, maka pesan asli akan diacak (enkripsi) terlebih dulu menjadi pesan tersandi (*ciphertext*). Dengan hasil analisis sebagai berikut :

Pesan asli : STMIK Kharisma 92 (17 karakter).
Kunci : karawang (8 karakter).

Untuk *index* karakter pesan asli dapat dilihat pada Tabel 1. *Index* karakter pesan asli berikut:

Tabel 1. *Index* Karakter Pesan Asli

***Index* ke-i**	**Pesan asli (P)**	**Desimal dalam ASCII 128 bit**
P_1	S	83
P_2	T	84
P_3	M	77
P_4	I	73
P_5	K	75
P_6	(spasi)	32
P_7	K	75
P_8	h	104
P_9	a	97
P_{10}	r	114
P_{11}	i	105
P_{12}	s	115
P_{13}	m	109
P_{14}	a	97
P_{15}	(spasi)	32
P_{16}	9	57
P_{17}	2	50

Untuk *index* karakter kunci dapat dilihat pada Tabel 2. *Index* karakter kunci berikut:

Tabel 2. *Index* Karakter Kunci

***Index* ke-i**	**Kunci (K)**	**Desimal dalam ASCII 128 bit**
K_1	k	107
K_2	a	97
K_3	r	114
K_4	a	97
K_5	w	119
K_6	a	97
K_7	n	110
K_8	g	103

p-ISSN 2087-1716
e-ISSN 2548-7779

ILKOM Jurnal Ilmiah Volume 11 Nomor 3 Desember 2019
Terakreditasi peringkat 3 SK. No.28/E/KPT/2019

Proses penyisipan pesan sebagai berikut:

Enkripsi Algoritma Substitusi

Pesan yang disisipkan akan disandikan dengan algoritma substitusi. Untuk mengacak pesan menggunakan algoritma substitusi, perhitungannya sebagai berikut:

$C_i = (P_i + K) \bmod 128$ (1)

Dimana,

C_i	=	*Ciphertext* ke-i
P_i	=	*Plaintext* ke-i
K	=	Panjang kunci asli
mod 128	=	ASCII 128 bit

Enkripsi Algoritma Substitusi:
Untuk P_1 = S, maka:

$C_1 = (P_i + K) \bmod 128$
$= (83 + 17) \bmod 128$
$= 100 \bmod 128$
$= 100$
$=$ **d** (konversi karakter dari ASCII)

Proses enkripsi akan sama dilakukan menggunakan perhitungan enkripsi substitusi sampai karakter terakhir yaitu P_{17} = 2. Hasil enkripsi dapat dilihat pada Tabel 3. Hasil enkripsi substitusi berikut:

Tabel 3. Hasil Enkripsi Subtitusi

Plaintext (P)	**Desimal dalam ASCII 256 bit**	**P_i + N mod 128**	***Ciphertext (C)***
S	83	100	d
T	84	101	e
M	77	100	d
I	73	101	e
K	75	94	^
(spasi)	32	90	Z
K	75	92	\
h	104	49	1
a	97	92	\
r	114	121	y
i	105	114	r
s	115	3	(null)
m	109	122	z
a	97	4	(null)
(spasi)	32	126	~
9	57	114	r
2	50	49	1

Pesan hasil enkripsi substitusi (*ciphertext-1*) adalah **de^Z\1\yr z ~r1JC**.

Enkripsi Algoritma Vigenere *Cipher*

Setelah tahap pertama pengacakan pesan akan dilanjutkan dengan tahap kedua yaitu pengacakan menggunakan algoritma *vigenere cipher*. Vigenere *cipher* menggabungkan *plaintext* (*ciphertext-1*) dengan kunci sehingga menghasilkan *ciphertext* yang baru (*ciphertext-2*). Untuk

DOI: https://doi.org/10.33096/ilkom.v11i3.477.222-230

mengacak pesan menggunakan perhitungan berikut:

$C_i = (P_i + K_i) \bmod 128$ (2)

Dimana,

C_i = *Ciphertext* ke-i
P_i = *Plaintext* ke-i
K_i = Kunci ke-i
mod 128 = ASCII 128 bit

Enkripsi Vigenere *Cipher* :
Untuk P_1 = S dan K_1 = k, maka:

$C_1 = (P_i + K_i) \bmod 128$
$= (100 + 107) \bmod 128$
$= 207 \bmod 128$
$= 79$
= **O** (konversi karakter dari ASCII)

Proses enkripsi akan sama dilakukan menggunakan perhitungan enkripsi *vigenere* sampai karakter terakhir yaitu P_{17} = 2 dan perulangan kunci K_{17} = k. Hasil enkripsi dapat dilihat pada Tabel 4. Hasil enkripsi *vigenere cipher* berikut:

Tabel 4. Hasil Enkripsi Vigenere *Cipher*

Plaintext (P)	**Desimal dalam ASCII**	**Kunci (K)**	**Desimal dalam ASCII**	**$P_i + K_i$ mod 128**	***Ciphertext (C)***
d	100	k	107	79	O
e	101	a	97	70	F
^	94	r	114	80	P
Z	90	a	97	59	;
\	92	w	119	83	S
1	49	a	97	18	(null)
\	92	n	110	74	J
y	121	g	103	96	`
r	114	k	107	93	]
f	131	a	97	100	d
z	122	r	114	108	l
„	132	a	97	101	e
~	126	w	119	117	u
r	114	a	97	83	S
1	49	n	110	31	(null)
J	74	g	103	49	1
C	67	k	107	46	.

Pesan hasil enkripsi Vigenere (*ciphertext-2*) adalah **OFP;S J`]dleuS 1.**

Dekripsi Algoritma *Vigenere*

Setelah tahap pengambilan pesan akan dilanjutkan dengan tahap dekripsi menggunakan algoritma Vigenere *cipher*. Vigenere *cipher* ini menggunakan kunci yang sama pada enkripsi yaitu "karawang". Untuk dekripsi pesan menggunakan perhitungan berikut:

$P_i = (C_i + K_i) \bmod 128$ (3)

DOI: https://doi.org/10.33096/ilkom.v11i3.477.222-230

Dimana,
C_i = *Ciphertext* ke-i
P_i = *Plaintext* ke-i
K_i = Kunci ke-i
mod 128 = ASCII 128 bit

Dekripsi Vigenere *Cipher* :
Untuk C_1 = O dan K_1 = k, maka:
$\mathbf{P_1}$ = $(C_i - K_i)$ mod 128
= (207 - 107) mod 128
= 100 mod 128
= 100
= **d** (konversi karakter dari ASCII)

Proses dekripsi akan sama dilakukan menggunakan perhitungan dekripsi *vigenere* sampai karakter terakhir yaitu C_{17} = 1 dan perulangan kunci K_{17} = k. Hasil dekripsi untuk seluruh karakter dapat dilihat pada Tabel 5. Hasil dekripsi vigenere *cipher* berikut:

Tabel 5. Hasil Dekripsi Vigenere C*ipher*

Ciphertext (C)	Desimal dalam ASCII	Kunci (K)	Desimal dalam ASCII	$C_i - K_i$ mod 128	*Plaintext (P)*
O	79	k	107	100	d
F	70	a	97	101	e
P	80	r	114	94	^
;	59	a	97	90	Z
S	83	w	119	92	\
(null)	18	a	97	49	1
J	74	n	110	92	\
`	96	g	103	121	y
]	93	k	107	114	r
d	100	a	97	3	(null)
l	108	r	114	122	z
e	101	a	97	4	(null)
u	117	w	119	126	~
S	83	a	97	114	r
(null)	31	n	110	49	1
1	49	g	103	74	J
-	46	k	107	67	C

Pesan hasil dekripsi Vigenere adalah **de^Z\1\yr z ~r1JC.**

Dekripsi Algoritma Substitusi

Pesan hasil dekripsi Vigenere akan didekripsikan lagi menggunakan algoritma substitusi untuk memperoleh pesan asli. Untuk dekripsi pesan menggunakan algoritma substitusi, perhitungannya berikut:

$P_i = (C_i - N) \bmod 128$ (4)

Dimana,
C_i = *Ciphertext* ke-i
P_i = *Plaintext* ke-i

DOI: https://doi.org/10.33096/ilkom.v11i3.477.222-230

N = Panjang pesan
mod 128 = ASCII 128 bit

Dekripsi algoritma substitusi:
Untuk P_1 = d, maka :
P_1 = $(C_i - N) \bmod 128$
= $(100 - 17) \bmod 128$
= $83 \bmod 128$
= 83
= **S** (konversi karakter dari ASCII)

Proses dekripsi akan sama dilakukan menggunakan perhitungan dekripsi substitusi sampai karakter terakhir yaitu C_{17} = C. Hasil dekripsi dapat dilihat pada Tabel 6. Hasil dekripsi substitusi berikut:

Tabel 6. Hasil Dekripsi Subtitusi

Plaintext (P)	Desimal ASCII	C_i - N mod 128	*Plaintext (P)*
d	100	83	S
e	101	84	T
^	94	77	M
Z	90	73	I
\	92	75	K
1	49	32	(spasi)
\	92	75	K
y	121	104	h
r	114	97	a
(null)	3	114	r
z	122	105	i
(null)	4	115	s
~	126	109	m
r	114	97	a
1	49	32	(spasi)
J	74	57	9
C	67	50	2

Pesan hasil dekripsi substitusi adalah **STMIK Kharisma 92**.

4. Kesimpulan dan Saran

Berdasarkan hasil penelitian dan pembahasan yang dilakukan maka diperoleh kesimpulan bahwa aplikasi kriptografi ini dapat diimplementasikan pada *software database MySQL* menggunakan sistem operasi *linux* maupun sistem operasi berlisensi sebagai keamanan data file dokumen dengan metode kombinasi algoritma substitusi dan *vigenere cipher* ini menghasilkan file yang terenkrip atau rahasia dalam format file txt yang secara kualitas tidak berbeda dan memiliki ukuran yang sama dari ukuran file text awal. Untuk pengembangan aplikasi ini disarankan agar media kriptografi dapat berupa multimedia seperti keamanan data file yang berisi gambar dan format file text yang bervariasi seperti format odt, docx atau format yang lain. Pesan yang dienkripsi maupun di deskripsi tidak hanya berupa file teks, dapat dikembangkan dengan pesan suara, gambar atau multimedia lain.

Daftar Pustaka

[1] Widianto, Septian Rheno. *Desain Algoritma Steganografi dengan Metode Spread Spectrum Berbasis PCMK (Permutasi Chaotic Multiptaran Mengecil dan Membesar) Yang Tahan Terhadap Gangguan*. Prodi Teknologi Rekayasa Perangkat Lunak Politeknik Enjinering Indorama Kembang Kuning Ubrug Jatiluhur, Purwakarta. p- ISSN: 2407 – 184 e ISSN: 2460 –8416, 2018.

[2] Irawan, Muhammad Dedi., *Implementasi Kriptografi Vigenere Chiper Dengan PHP.* Program Studi Teknik Informatika. Universitas Asahan. Jurnal Teknologi Informasi (JurTI) Volume 1, Nomor 1, P-ISSN 2580-7927. 2017

[3] Sa'id, Fauzus., Wijanarto. *Implementasi Algoritma Vigenere dan Metode LSBMR Pada Citra Diam*. Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro. Techno.COM, Vol. 14, No. 3: 189-197. Agustus 2015.

[4] Rohmanu, Ajar. *Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma Des dan Metode End of File*. Teknik Informatika, STMIK Cikarang. Jurnal Informatika SIMANTIK Vol.1 No.2 ISSN: 2541-3244. Maret 2017.

[5] Maesyaroh, Siti.. *Enkripsi Data dengan Menggunakan Metode Subtitusi*. Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Kuningan (UNIKU). Jurnal Buffer Informatika, Volume 3 Nomor 1, ISSN 2527-4856. 2017

[6] M. Azman Maricar dan Nyoman Putra Sastra. *Efektivitas Pesan Teks dengan Cipher Substitusi, Vigenere Cipher, dan Cipher Transposisi*. Majalah Ilmiah Teknologi Elektro, Vol. 17, No. 1,Januari -April 2018. p- ISSN:1693 – 2951; e-ISSN: 2503-2372. 2018

[7] Efrandi, Asnawati, Yupiyanti. *Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Chiper.* Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu. Jurnal Media Infotama Vol. 10 No. 2, ISSN 1858 – 2680, September 2014.

[8] Hernawandra, Priyagung., Supriyadi, Lenggana, U. Tresna. Aplikasi Steganografi Menggunakan LSB 4 Bit Sisipan dengan Kombinasi Algoritma Substitusi dan Vigenere Berbasis Android. Program Studi Informatika, STMIK Kharisma Karawang. Jurnal Teknologi dan Sistem Komputer, 6(2, 44-50. E-ISSN:2338-0403, 2018

[9] Setiadi, et al, *Kombinasi Chiper Subtitusi (Beaufort Dan Vigenere) Pada Citra Digital.* Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang. Prosiding SENDI_U. ISBN: 978-979-3649-99-3. 2018

[10] Satzinger, John W., Jackson, Robert B., Burd, Stephen D. *System Analysis and Design in a Changing World, Fourth Edition, Thomson Course Technology.* Canada. ISBN-13: 9781423902287, ISBN- 10: 1-4239-0228-9. 2010.

[11] Albert Ginting, R. Rizal Isnanto, Ike Pertiwi Windasari., *Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email.* Program Studi Sistem Komputer Fakultas Teknik Universitas Diponegoro. Semarang. Jurnal Teknologi dan Sistem Komputer, Vol 3, No. 2, April. e-ISSN: 2338-0403. 2015

[12] *Ebook Teori dan Aplikasi Kriptografi.Sentot Kromodimoeljo Desember 2009.ISBN 978-602-96233-0-7.* Penerbit SPK IT Consulting. 2009 SPK IT Consulting.

[13] Anwar, et al, *Implementasi Kriptografi Dengan Enkripsi Shift Vigenere Chiper Serta Checksum Menggunakan CRC32 Pada Data Text*. Jurusan Magister Ilmu Komputer, Universitas Budi Luhur. Jurnal Sistem Informasi Volume.2, ISSN: 2406-7768. 2015

[14] Rojali Soni Afandi dan Erik Hadi Saputra., *Aplikasi Mobile Informasi Kafe 24 Jam Di Yogyakarta Berbasis Android., Jurnal Ilmiah DASI Vol. 14 No. 04, pp: ISSN: 1411-3201. Desember 2013.*

[15] Galin, Daniel. *Software Quality Assurance from Theory to Implementation. England, Addison-Wesley*. ISBN 0201 70945 7. 2004.

