

Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher

Imam Riadi ⁽¹⁾, Abdul Fadlil ⁽²⁾, Fahmi Auliya Tsani ^{(3)*}

¹ Sistem Informasi, Fakultas Sains dan Teknologi Terapan, Universitas Ahmad Dahlan, Yogyakarta

² Teknik Elektro, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta

³ Teknik Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta
e-mail : imam.riadi@is.uad.ac.id, fadlil@mti.uad.ac.id, fahmi1807048017@webmail.uad.ac.id.

* Penulis korespondensi.

Artikel ini diajukan 15 Juli 2021, direvisi 15 Desember 2021, diterima 15 Desember 2021, dan dipublikasikan 25 Januari 2022.

Abstract

Cryptography is one of the most popular methods in data security by making data very difficult to read or even unreadable. One of the well-known techniques or algorithms in cryptography is Vigenere Cipher. This classic algorithm is classified as a polyalphabetic substitution cipher-based algorithm. Therefore, this algorithm tends to only handle data in text form. By this research, a console-based application has been developed which is made from PHP programming language to be able to encrypt and decrypt digital image media using Vigenere Cipher. The encryption process is done by first converting a digital image into a base64 encoding format so that the encryption process can be carried out using the tabula recta containing the radix-64 letter arrangement used for base64 encoding. Conversely, the decryption process is carried out by restoring the encrypted file using radix-64 letters, so we get the image file in the base64 encoding format. Then, the image with the base64 encoding format is decoded into the original file. The encryption process took less than 0,2 seconds and 0.19 seconds for the decryption process and 33.34% for average file size addition on the encrypted file from the original file size. Testing on ten different images with different sizes and dimensions showed a 100% success rate which means this research was successfully carried out.

Keywords: Digital Image Encryption, Vigenere Cipher, Classical Cryptography, Base64 Encoding, Data Security

Abstrak

Kriptografi merupakan salah satu metode populer dalam pengamanan data dengan cara membuat data sulit atau bahkan tidak bisa dibaca. Salah satu teknik atau algoritma yang terkenal dalam kriptografi adalah Vigenere Cipher. Algoritma kriptografi klasik ini termasuk dalam kategori algoritma berbasis *polyalphabetic substitution cipher*. Oleh karena itu, algoritma ini cenderung hanya bisa menangani data dalam bentuk teks. Pada penelitian ini, dikembangkan aplikasi berbasis konsol yang dibuat dalam bahasa pemrograman PHP dengan tujuan agar bisa melakukan enkripsi dan dekripsi pada media citra digital menggunakan Vigenere Cipher. Proses enkripsi dilakukan dengan terlebih dahulu mengubah suatu citra digital menjadi format *encoding* base64, sehingga bisa dilakukan proses enkripsi dengan memakai tabula recta yang berisi susunan huruf radix-64 yang digunakan untuk proses encoding base64. Sebaliknya, proses dekripsi dilakukan dengan mengembalikan *file* yang sudah dienkripsi menggunakan susunan huruf radix-64, sehingga didapatkan *file* citra dalam format *encoding* base64. Lalu, citra berformat *encoding* base64 ini di-*decode* menjadi *file* asli. Proses enkripsi membutuhkan waktu kurang dari 0,2 detik dan 0,19 detik untuk proses dekripsi serta mengalami penambahan ukuran rata-rata sebesar 33,34% pada *file* hasil enkripsi dari ukuran *file* semula. Pengujian pada sepuluh citra digital dengan ukuran dan dimensi berbeda-beda menunjukkan tingkat keberhasilan sebesar 100%, hal ini berarti bahwa penelitian berhasil dilakukan.

Kata Kunci: Enkripsi Citra Digital, Vigenere Cipher, Kriptografi Klasik, Pengkodean Base64, Keamanan Data



1. PENDAHULUAN

Keamanan atau *security* merupakan salah satu aspek penting yang seharusnya dipenuhi dari suatu informasi atau data. Keamanan sangat penting karena berhubungan dengan data sensitif dengan cara melindungi dari akses yang tidak sah, pengubahan, maupun penghapusan (Awad et al., 2019). Ada beberapa aspek dalam keamanan data antara lain *authentication*, *confidentiality/privacy*, *integrity*, dan *non-repudiation*. Beberapa poin ini bisa diselesaikan dengan menggunakan teknik kriptografi (Munir, 2006). Hermansa et al. (2019) mendefinisikan bahwa kriptografi merupakan teknik yang digunakan untuk mengamankan suatu data melalui proses enkripsi sehingga data menjadi sulit dibaca atau dibuka oleh seseorang yang tidak berwenang karena tidak memiliki kunci untuk melakukan dekripsi. Dengan kata lain, kriptografi mampu mengubah isi suatu data menjadi data lain yang acak (Fadlil et al., 2020b).

Secara garis besar, kriptografi dibedakan menjadi dua yaitu kriptografi klasik dan kriptografi modern. Salah satu algoritma atau teknik dalam kriptografi klasik yang populer adalah Vigenere Cipher. Algoritma ini mengimplementasikan teknik substitusi yaitu proses penyandian dengan mengubah isi suatu data berdasarkan kunci yang digunakan agar tidak terbaca maknanya (Setiadi et al., 2018). Vigenere Cipher menggunakan bujur sangkar Vigenere dalam melakukan proses enkripsi maupun dekripsi, sehingga membuat algoritma ini dikenal mudah dipahami dan diimplementasikan (Munir, 2006). Contoh bujur sangkar Vigenere bisa dilihat pada Gambar 1.

	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 1. Contoh tabel bujur sangkar Vigenere.

Saat ini, kriptografi tidak hanya digunakan untuk data-data berjenis teks saja namun juga sangat memungkinkan untuk diaplikasikan pada jenis data yang lain seperti citra, video, dan suara (Sinaga et al., 2018). Suatu algoritma kriptografi bisa dikatakan bagus jika mampu mempertahankan aspek kerahasiaan dari pesan yang dienkripsi dan tidak mudah dipecahkan oleh orang yang tidak berhak untuk mengakses data tersebut (Anwar et al., 2019).

Beberapa penelitian terdahulu sudah banyak yang mengangkat tema pengaplikasian Vigenere Cipher ini untuk mengamankan berbagai jenis data. (Gerhana et al., 2016) dalam penelitiannya



mengangkat tema pengaplikasian Vigenere Cipher pada media citra digital dengan melakukan substitusi kode warna pada setiap pikselnya berdasarkan kunci yang dimasukkan. Sebagai hasilnya, terbentuk citra lain dengan warna yang acak.

Gunadhi & Sudrajat (2016) mengimplementasikan Vigenere Cipher yang sudah dimodifikasi untuk melakukan pengamanan pada data rekam medis pasien, sehingga menjadikan data rekam medis pasien lebih aman dari serangan para *cryptanalyst*.

Penelitian lain dilakukan oleh (Mandal & Deepti, 2016) dengan mengimplementasikan skema enkripsi *multi level*. Metode yang digunakan yaitu dengan menggunakan kunci yang memiliki panjang karakter sama dengan *plain text* sehingga menghasilkan *cipher text* pertama. Tidak berhenti sampai di sini, *cipher text* pertama ini lalu dienkripsi lagi dengan kunci yang sama dengan *cipher text* pertama sehingga dihasilkan *cipher text* kedua. Sebagai kesimpulannya, dibandingkan dengan beberapa algoritma kriptografi lainnya (AES, Blowfish, dan RC5) metode ini memiliki hasil yang sulit dipecahkan oleh *cryptanalyst* dan juga memiliki kompleksitas komputasi yang lebih rendah sehingga cocok digunakan untuk aplikasi yang ringan dan memiliki *resource* yang terbatas.

Soofi et al. (2016) mencoba melakukan sedikit modifikasi pada tabel bujur sangkar Vigenere dengan mengganti urutan setiap karakternya dan menambahkan satu karakter "&" sebagai pengganti karakter spasi (*white space*). Dengan metode ini, dihasilkan algoritma Vigenere yang lebih kuat terhadap serangan dengan metode Kasiski dan Friedman.

Beberapa penelitian mengenai Vigenere Cipher dilakukan dengan menggabungkan Vigenere Cipher dengan teknik-teknik lain. Nasution et al. (2017) menggabungkan Vigenere Cipher dengan teknik kompresi Goldbach Codes. Hasil penggabungan ini membuahkan *cipher text* yang susah diprediksi meskipun menggunakan serangan metode Kasiski, hal ini dikarenakan kumpulan karakter yang dihasilkan berbeda dengan karakter yang digunakan pada *plain text*.

Maruf et al. (2015) melakukan penelitian dengan menggabungkan Vigenere Cipher dengan XTEA (*Extended Tiny Encryption Algorithm*) *block cipher*. XTEA dipilih karena sudah teruji kekuatannya dalam mengamankan data berjenis teks. Penggabungan dua teknik ini diberi nama VixTEA dan terbukti meningkatkan keamanan berdasarkan beberapa pengujian yang dilakukan yaitu analisis frekuensi, analisis nilai entropi, dan analisis serangan *brute force*. Hasil pengujian bahkan juga menunjukkan bahwa konsep ini tidak mempengaruhi performa dari algoritma itu sendiri.

Rojali et al. (2016) dalam penelitiannya menggabungkan beberapa metode sebagai langkah untuk mengamankan data. Beberapa metode yang digunakan yaitu enkripsi, pembangkitan kunci, kompresi data, dan steganografi. Enkripsi yang digunakan yaitu Vigenere Cipher yang sudah dimodifikasi menggunakan komposisi bujur sangkar Vigenere sesuai dengan susunan huruf, angka, dan simbol yang ada pada *keyboard*. Sedangkan *key* yang digunakan dibangkitkan melalui *chaos function*. Proses selanjutnya yaitu melakukan kompresi pada data yang sudah dienkripsi menggunakan *Dictionary Based Compression*. Sebagai Langkah terakhir, data yang telah dikompres disembunyikan ke dalam suatu citra digital menggunakan steganografi dengan metode *Least Significant Bit* (LSB).

Masih dengan media *plain text*, Saputra et al. (2017) mengimplementasikan Vigenere Cipher dengan memanfaatkan citra *grayscale* berukuran 5 x 5 piksel sebagai kunci. Kunci citra *grayscale* ini dikonversi menjadi karakter ASCII, sehingga menjadi susunan karakter yang bisa diolah ke dalam Vigenere Cipher.

Subandi et al. (2018) dalam penelitiannya melakukan enkripsi citra digital dengan melakukan dua kali proses enkripsi menggunakan Vigenere Cipher dan mengadopsi *expansion key* menggunakan algoritma RC6 pada media teks. Penelitian ini memiliki tujuan untuk mengetahui perbandingan perbedaan ukuran suatu data sebelum dan sesudah dienkripsi (*avalanche effect*) pada beberapa skenario seperti penggunaan Vigenere Cipher secara standar, penggabungan dengan *expansion key* RC6, dan lain-lain.



Serupa dengan penelitian dari Subandi et al. (2018) yang bertujuan untuk mengetahui perbandingan *avalanche effect*, Rihartanto et al. (2020) menggunakan Vigenere Cipher yang sudah dimodifikasi dengan cara memperluas jangkauan karakter yang bisa diakomodasi menjadi 128 buah sesuai dengan jumlah karakter ASCII standar serta melakukan rotasi matriks bujur sangkar. Implementasi dari proses tersebut menghasilkan nilai *avalanche effect* sekitar 45% hingga 49%.

Fadlil et al. (2020b) melakukan pendekatan yang berbeda pada penelitiannya mengenai implementasi Vigenere Cipher yaitu dengan mengombinasikan Jaringan Syaraf Tiruan (JST) dengan Vigenere Cipher. Penelitian ini menggunakan JST sebagai generator kunci dengan memasukkan parameter *hidden neurons* (K), *input neurons* (N), dan bobot (L) sehingga dihasilkan karakter acak yang bisa digunakan dalam proses enkripsi dan dekripsinya. Melalui pendekatan ini diklaim memiliki sedikit kemungkinan memunculkan kunci yang sama meskipun memasukkan nilai parameter yang sama berulang kali.

Prabowo & Hangga (2015) juga mengimplementasikan metode pembangkitan kunci untuk digunakan di Vigenere Cipher. Caesar Cipher dipilih sebagai pembangkit kunci, dengan kata lain parameter kunci yang dimasukkan oleh pengguna akan dienkripsi terlebih dahulu menggunakan Caesar Cipher, sehingga dihasilkan *encrypted key* yang akan digunakan untuk proses enkripsi-dekripsi menggunakan Vigenere Cipher. Metode ini dipilih karena dari contoh yang digunakan memperlihatkan bahwa Vigenere Cipher dalam kondisi standar berpotensi menghasilkan pengulangan kata saat menggunakan kunci berulang dengan panjang kunci yang cukup pendek. Sebagai hasil dari penelitian ini, disimpulkan bahwa metode yang digunakan mampu mengurangi potensi pengulangan kata bahkan tidak ditemukan adanya pengulangan kata.

Hernawandra et al. (2018) melibatkan citra digital dalam penelitiannya dalam mengamankan data berupa teks dengan terlebih dahulu melakukan proses enkripsi menggunakan Vigenere Cipher dan substitusi. *Cipher text* yang dihasilkan dari proses enkripsi kemudian disembunyikan pada media citra digital dengan menggunakan teknik steganografi LSB 4 bit. Keluaran dari penelitian ini berupa aplikasi yang berjalan pada platform Android. Penelitian ini menghasilkan kesimpulan bahwa aplikasi yang dibangun mampu mengamankan pesan melalui metode steganografi LSB 4 bit yang digabungkan dengan enkripsi substitusi dan Vigenre Cipher serta memiliki *avalanche effect* rata-rata sebesar 12,77%.

Penelitian mengenai kriptografi menggunakan algoritma Vigenere Cipher yang telah dilakukan sebelumnya banyak yang berfokus pada pengamanan data jenis teks. Penelitian yang berfokus pada data jenis citra digital masih sangat jarang ditemukan. Padahal, citra digital merupakan salah satu jenis media yang sangat populer digunakan untuk berkomunikasi baik secara daring maupun langsung (Zebua & Ndruru, 2017). Oleh sebab itu, penelitian ini akan mengembangkan pengamanan data jenis citra digital menggunakan metode Vigenere Cipher. Pembuktian validitas hasil penelitian dengan membandingkan nilai *hash file* asli dengan nilai *hash file* hasil dekripsi. Penelitian ini juga akan menyajikan data mengenai waktu yang dibutuhkan untuk proses enkripsi dan dekripsi serta menghitung persentase rata-rata perubahan ukuran *file* yang dihasilkan dengan cara membandingkan ukuran *file* asli dengan ukuran *file* setelah dienkripsi. Hasil pengujian akan dibandingkan dengan penelitian sejenis yang menggunakan algoritma Arnold's Cat Map seperti yang dilakukan oleh (Rachmawanto, dkk., 2019) dan algoritma Elgamal dengan mode Electronic Code Book (ECB) seperti yang dilakukan oleh (Rizal, dkk., 2016). Penelitian ini diharapkan dapat memberikan wawasan mengenai pentingnya pengamanan data atau *file*, terutama data jenis citra digital.

2. METODE PENELITIAN

Data atau sistem yang tidak aman tentu akan berdampak buruk (Riadi et al., 2020). Salah satu metode yang dapat digunakan untuk mempertahankan kerahasiaan suatu data adalah dengan mengubahnya menjadi data tersandi yang tidak bermakna, proses ini bisa biasa disebut sebagai kriptografi (Yunita et al., 2019). Menurut terminologinya, kriptografi merupakan ilmu dan seni yang



digunakan untuk mengamankan pesan ketika pesan dikirim dari suatu sumber ke tempat tujuan. Proses ini terdiri dari tiga fungsi dasar antara lain (Ariyus, 2006):

- Enkripsi, proses mengubah pesan asli menjadi berbentuk kode-kode yang susah atau bahkan tidak bisa dimengerti.
- Dekripsi, proses kebalikan dari enkripsi yaitu mengubah pesan yang sudah terenkripsi menjadi pesan asli.
- Kunci, sekumpulan parameter yang digunakan dalam proses enkripsi maupun dekripsi.

Schneier dan Menezes (seperti yang diacu dalam Munir, 2006) menerangkan bahwa kriptografi memiliki beberapa tujuan pada beberapa aspek keamanan sebagai berikut:

- Kerahasiaan (*confidentiality*), bertujuan agar pesan tidak bisa dibaca oleh pihak-pihak yang tidak berhak.
- Integritas data (*data integrity*), bertujuan agar mendapat jaminan bahwa pesan masih asli/utuh dan tidak dimanipulasi saat pengiriman.
- Otentikasi (*authentication*), bertujuan untuk mengidentifikasi kebenaran pihak-pihak yang saling berkomunikasi maupun mengidentifikasi kebenaran pesan.
- Nirpenyangkalan (*non-repudiation*), bertujuan agar tidak ada penyangkalan oleh pihak-pihak yang berkomunikasi.

Penelitian ini mengimplementasikan algoritma Vigenere Cipher yang sudah dimodifikasi dan menghasilkan *output* berupa aplikasi berbasis *console*. Modifikasi yang dilakukan berupa pelebaran *range* karakter sesuai dengan karakter-karakter yang digunakan oleh algoritma *encoding* base64. *Encoding* base64 pada aplikasi ini digunakan untuk mengubah citra digital yang merupakan data *binary* menjadi berbentuk karakter-karakter tertentu sesuai dengan format karakter yang disediakan oleh *encoding* base64.

2.1. Vigenere Cipher

Vigenere Cipher merupakan hasil pengembangan lebih lanjut dari Caesar Cipher dan termasuk dalam kategori *polyalphabetic substitution cipher* (Prabowo & Hangga, 2015). Vigenere Cipher dapat dilakukan dengan dua cara yaitu dengan cara manual memakai bujur sangkar vigenere (*tabula recta*) seperti pada Gambar 1 maupun dengan cara substitusi angka (matematis). Secara matematis, enkripsi dan dekripsi menggunakan Vigenere Cipher dalam kondisi standar dapat dituliskan seperti Pers. (1), sedangkan untuk dekripsi bisa dituliskan seperti Pers. (2).

$$C_i = (P_i + K_i) \bmod 26 \quad (1)$$

$$P_i = (C_i - K_i) \bmod 26 \quad (2)$$

Berikut ini kami sajikan contoh penggunaan Vigenere Cipher dengan berpedoman pada susunan alfabet seperti pada Gambar 2.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 2. Indeks susunan huruf alfabet.



Plaintext : UINSUNANKALIJAGA
 Key : VIGENERECIPHERVI
 Ciphertext : PQTWHRRMIAPNRBI

Penelitian ini menggunakan susunan huruf yang digunakan pada *encoding* base64 sebanyak 64 karakter ditambah dengan tiga karakter tambahan yaitu “:”, “;”, dan “,” karena berkas citra digital yang sudah di-*encode* menggunakan metode base64 memerlukan informasi tambahan berupa susunan *string mime type* sebagai penanda jenis berkas yang di-*encode*. Oleh karena itu, rumus matematis yang digunakan untuk proses enkripsi dan dekripsi juga berubah. Rumus persamaan untuk proses enkripsi sebagaimana tertulis pada Pers. (3). Sedangkan untuk proses dekripsi persamaan matematisnya sebagaimana tertulis pada Pers. (4).

$$C_i = (P_i + K_i) \bmod 67 \quad (3)$$

$$P_i = (C_i - K_i) \bmod 67 \quad (4)$$

2.2. Base64

Base64 merupakan salah satu skema *encoding binary-to-text* yang merepresentasikan data *binary* menjadi susunan karakter berformat ASCII, dengan menerjemahkannya ke dalam susunan radix-64 (Wen & Dang, 2018). Base64 merupakan suatu algoritma *block cipher* yang beroperasi dalam lingkup bit, hanya saja lebih mudah diimplementasikan dibandingkan algoritma yang lain. Karakter-karakter dalam radix-64 ini terdiri dari huruf “A-Z”, “a-z”, “0-9”, dan dua karakter terakhir yaitu “/” dan “+” (Sumartono et al., 2016). Daftar karakter dalam radix-64 dapat dilihat pada Tabel 1.

Tabel 1. Susunan karakter untuk encoding base64.

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	/
15	P	31	f	47	v	63	+

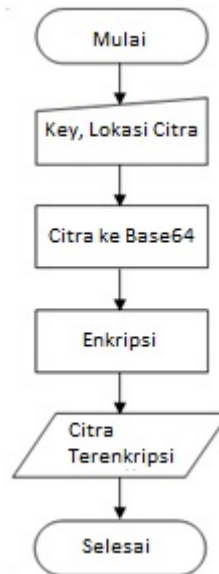
Berikut ini adalah contoh potongan *string* citra digital yang di-*encode* menggunakan base64 lengkap beserta dengan *mime type*:

```
data:image/png;base64,iVBORw0KGgoAAAANSUHEUgAAAQAAAAEACAYAAABccqhAAAA
GXRFWHRTb2Z0d2FyZQBmZG9iZSBBZWFuZGVyZWZvYXQAAAMtJREFUeNrsfXtsHeeV35m
Z ...
```

2.3. Proses Enkripsi

Enkripsi merupakan proses untuk mengubah data asli menjadi data tersandi (Munir, 2006). Proses enkripsi tersaji dalam bentuk *flowchart* seperti yang terlihat pada Gambar 3.



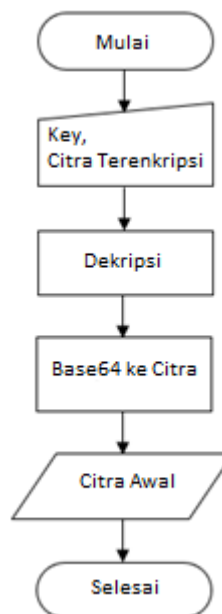


Gambar 3. Diagram alir proses enkripsi.

Langkah awal untuk melakukan proses enkripsi adalah dengan cara memasukkan *key/password* dan *path* lokasi *file* citra digital yang akan dienkripsi. Selanjutnya aplikasi akan melakukan konversi citra digital menjadi *encoded string* dengan metode base64. Kemudian aplikasi akan melakukan proses enkripsi dengan menerapkan Vigenere Cipher yang menggunakan susunan tabel Vigenere berdasarkan radix-64 ditambah tiga karakter lain dan *key* yang sudah dimasukkan. Sampai tahap tersebut, proses enkripsi selesai dilakukan dan hasilnya dikeluarkan menjadi berkas yang memiliki ekstensi *.vig.

2.4. Proses Dekripsi

Dekripsi merupakan proses untuk mengembalikan data yang sudah dienkripsi menjadi data asli (Munir, 2006). Proses dekripsi tersaji dalam bentuk *flowchart* seperti terlihat pada Gambar 4.



Gambar 4. Diagram alir proses dekripsi.



Langkah awal untuk melakukan dekripsi adalah pengguna memasukkan *key* dan *path* lokasi *file* yang akan didekripsi. Kemudian aplikasi akan melakukan proses dekripsi sebagaimana proses enkripsinya, yaitu menerapkan Vigenere Cipher menggunakan susunan tabel Vigenere berdasarkan radix-64 dengan tiga karakter tambahan dan *key* yang sudah dimasukkan. Selanjutnya aplikasi akan mengembalikan berkas citra digital yang dienkrpsi menjadi *encoded string* berbasis base64. Kumpulan *string* tersebut akan di-*decode* dan dikeluarkan menjadi berkas citra digital sesuai dengan format aslinya berdasarkan *mime type*-nya.

3. HASIL DAN PEMBAHASAN

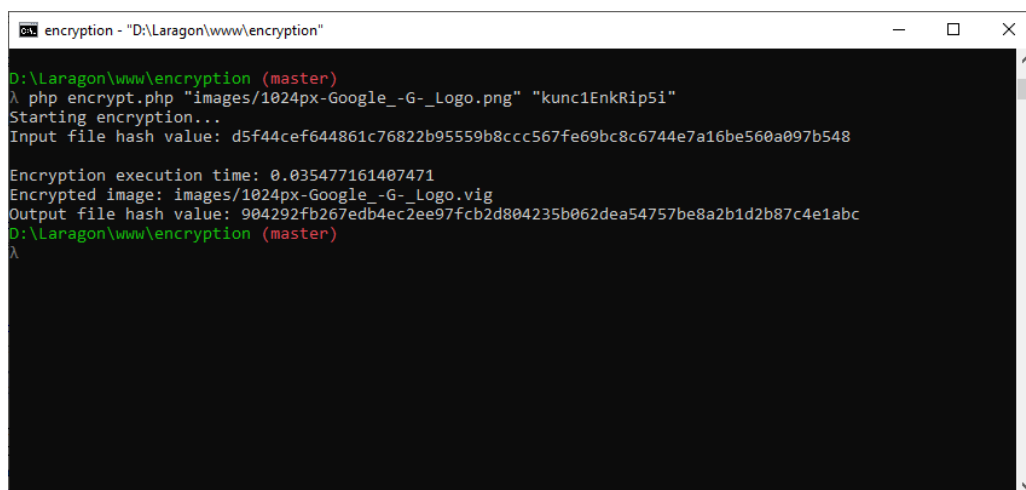
3.1. Modifikasi Vigenere Cipher

Penelitian ini menggunakan Vigenere Cipher yang sudah dimodifikasi. Modifikasi yang dilakukan terbatas pada pelebaran *support* karakter dari yang semula hanya 26 karakter alfabet menjadi 64 karakter yang terkandung dalam *list* radix-64 ditambah dengan karakter “.”, “,”, “,” sehingga berjumlah 67 karakter. Berikut adalah susunan karakter yang digunakan pada modifikasi Vigenere Cipher ini:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ  
abcdefghijklmnopqrstuvwxyz  
0123456789  
+/,;
```

3.2. Implementasi

Penelitian ini menghasilkan *output* berupa aplikasi berbasis konsol dengan kata lain dijalankan melalui *terminal/command prompt* dan dibangun menggunakan bahasa pemrograman PHP versi 7.2.19 di atas platform Windows 10 Pro 64-bit. Aplikasi ini terdiri dari dua *file* utama yaitu *encrypt.php* dan *decrypt.php*, penamaan *file* ini sesuai dengan fungsi utama yang diusungnya. Sedangkan *core* utama untuk proses enkripsi-dekripsi menggunakan satu *file* saja yaitu *VigenereCipher.php* yang berada di dalam *folder source*. Contoh tampilan dalam proses enkripsi dan format *command* yang dijalankan seperti yang terlihat pada Gambar 5.

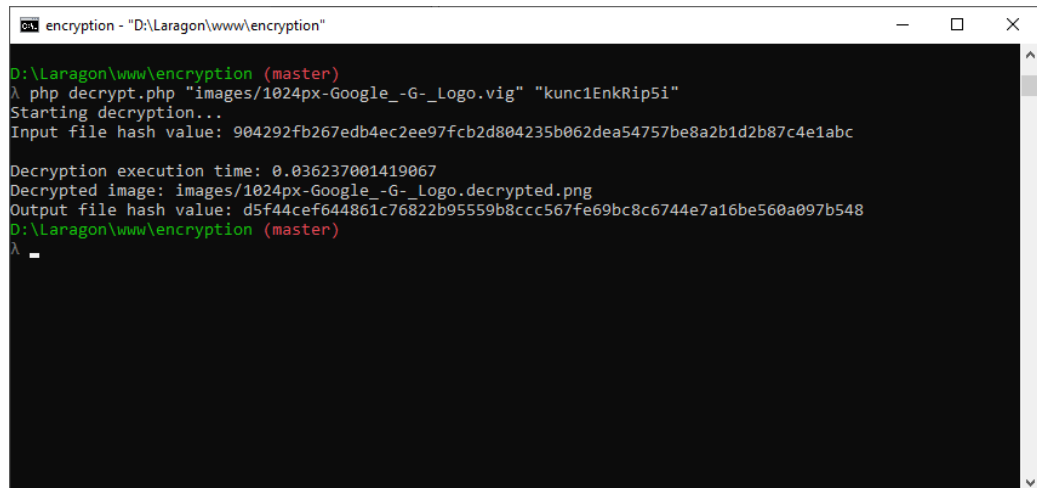


```
encryption - "D:\Laragon\www\encryption"  
  
D:\Laragon\www\encryption (master)  
λ php encrypt.php "images/1024px-Google_-G_Logo.png" "kunc1EnkRip5i"  
Starting encryption...  
Input file hash value: d5f44cef644861c76822b95559b8ccc567fe69bc8c6744e7a16be560a097b548  
  
Encryption execution time: 0.035477161407471  
Encrypted image: images/1024px-Google_-G_Logo.vig  
Output file hash value: 904292fb267edb4ec2ee97fcb2d804235b062dea54757be8a2b1d2b87c4e1abc  
D:\Laragon\www\encryption (master)  
λ
```

Gambar 5. Tampilan proses enkripsi.

Terdapat dua *arguments* atau parameter yang wajib diisi saat menjalankan aplikasi ini, baik dalam proses enkripsi maupun dekripsi. Parameter pertama yaitu *string* yang berisi lokasi *file* baik yang akan dienkrpsi maupun yang akan didekripsi. Parameter kedua yaitu *string* yang berisi *key* yang digunakan. Contoh tampilan dalam proses dekripsi mirip dengan tampilan pada proses enkripsi seperti yang terlihat pada Gambar 6.





```

D:\Laragon\www\encryption (master)
λ php decrypt.php "images/1024px-Google_-G-_Logo.vig" "kunc1EnkRip5i"
Starting decryption...
Input file hash value: 904292fb267edb4ec2ee97fcb2d804235b062dea54757be8a2b1d2b87c4e1abc

Decryption execution time: 0.036237001419067
Decrypted image: images/1024px-Google_-G-_Logo.decrypted.png
Output file hash value: d5f44cef644861c76822b95559b8ccc567fe69bc8c6744e7a16be560a097b548
D:\Laragon\www\encryption (master)
λ

```

Gambar 6. Tampilan proses dekripsi.

Aplikasi yang dihasilkan secara khusus hanya menerima input *file* citra digital dengan format png. Hasil dari proses enkripsi dikeluarkan ke dalam *file* dengan format ekstensi .vig, sedangkan hasil dari proses dekripsi dikeluarkan ke dalam *file* dengan format ekstensi .decrypted.png. Selain menghasilkan *output* berupa *file*, aplikasi ini juga menampilkan *output* nilai *hash* dari *file* yang akan dienkripsi, *file* yang sudah dienkripsi, dan *file* hasil dekripsi. Nilai *hash* ini digunakan untuk pengujian akurasi proses enkripsi dan dekripsi.

3.3. Pengujian

Pengujian dilakukan dengan menggunakan notebook Lenovo seri V14-ARE dengan spesifikasi *hardware* seperti yang ditunjukkan pada Tabel 2.

Tabel 2. Spesifikasi hardware untuk pengujian.

Perangkat	Spesifikasi
Processor	AMD Ryzen 7 4700U with Radeon Graphics (8 CPUs), ~2.0GHz
Memory/RAM	1228 MB RAM
Display	AMD Radeon(TM) Graphics
Harddisk	1 TB
SSD	512 MB

Validitas hasil penelitian diuji dengan cara membandingkan nilai *hash file* asli sebelum dienkripsi dengan nilai *hash file* hasil dekripsi menggunakan SHA256. Pengujian dilakukan pada sepuluh *file* ctra digital yang berbeda dengan hasil seperti yang terlihat pada Tabel 3. *File* dengan format ekstensi .png atau .jpg merupakan *file* asli, sedangkan *file* dengan format ekstensi .vig merupakan *file* hasil enkripsi. *File* dengan format ekstensi .dec.png atau .dec.jpg merupakan *file* hasil dekripsi.

Perbandingan nilai *hash file* asli dengan nilai *hash file* hasil dekripsi selalu menunjukkan tingkat kemiripan sebesar 100%. Hal ini berarti bahwa proses enkripsi dan dekripsi berhasil dengan baik dan akurat dalam mengamankan *file* citra digital.



Tabel 3. Pengujian tingkat akurasi.

No	Nama File	Nilai Hash
1.	1024px.png	d5f44cef644861c76822b95559b8ccc567fe69bc8c6744e7a16be560a097b548
	1024px.vig	904292fb267edb4ec2ee97fcb2d804235b062dea54757be8a2b1d2b87c4e1abc
	1024px.dec.png	d5f44cef644861c76822b95559b8ccc567fe69bc8c6744e7a16be560a097b548
	Kemiripan	100%
2.	768px.png	9bb8b08d1d5dbbbc0cf1b81d5cad5e94bd05631370971a9fe8334ed97b0d8cfc
	768px.vig	a5f57fc69fef9b04bc36175a7354163017fbc34019d933903ddfb8d703dd8945
	768px.dec.png	9bb8b08d1d5dbbbc0cf1b81d5cad5e94bd05631370971a9fe8334ed97b0d8cfc
	Kemiripan	100%
3.	600px.png	6c4bb7f7ebf1e5531eb622421750eddc87d5c240f61e5960a70bb3bb9ac4ce43
	600px.vig	5efd0374b39c3d20fa4c38323bf2c24d018d68fcc5080145b675db6ffd79ef6f
	600px.dec.png	6c4bb7f7ebf1e5531eb622421750eddc87d5c240f61e5960a70bb3bb9ac4ce43
	Kemiripan	100%
4.	480px.png	77c2b739c04e67a345016430efd6831a084f65bcd300681cc0014c405b4c3a3d
	480px.vig	2e978fba910bc613d62f8f222d7cd14ebbd9dec0a0bdc3385631ab90dc980e7f
	480px.dec.png	77c2b739c04e67a345016430efd6831a084f65bcd300681cc0014c405b4c3a3d
	Kemiripan	100%
5.	240px.png	463be7410c34f9e9b7e078f832a73d91c69de520c6b3e162394658c8838be0b2
	240px.vig	df0ce75f56bba5ee7a90c1a51244217c6c541d8800dbbcc00c49276810ab3487
	240px.dec.png	463be7410c34f9e9b7e078f832a73d91c69de520c6b3e162394658c8838be0b2
	Kemiripan	100%
6.	jpeg1.jpg	67c0e8280d2d48a291d289784a6eb6d60782d87092200231079f119cbaf1169a
	jpeg1.vig	a06f1d7663447395f4a5b4c62872183cec30315338d2296f5a558b5f0faee6ec
	jpeg1.dec.jpg	67c0e8280d2d48a291d289784a6eb6d60782d87092200231079f119cbaf1169a
	Kemiripan	100%
7.	jpeg2.jpg	63fdb834976b4e7e74b0b1dbc18c9c5fa254916c922cdc43a30c611e41619cb
	jpeg2.vig	b23068d3a94950a1c3cf0a1beea18acfd2073f5188a112ea1237b685609594f
	jpeg2.dec.jpg	63fdb834976b4e7e74b0b1dbc18c9c5fa254916c922cdc43a30c611e41619cb
	Kemiripan	100%
8.	jpeg3.jpg	cc6d678810c48d8521864a456f28785170c52d76ff144dc7e34c7b2cfc2f090a
	jpeg3.vig	5363c0df7f3cb611961d6b97bd5b2b466bea0eb727d701f0505dc6bf699e0263
	jpeg3.dec.jpg	cc6d678810c48d8521864a456f28785170c52d76ff144dc7e34c7b2cfc2f090a
	Kemiripan	100%
9.	jpeg4.jpg	7ecd178674861ef3074a820f94bed5fb09894ff0115dfb704516afce1283233f
	jpeg4.vig	de5cc10114a879b01d098d56af3c26c510d1285f7d0d4d00c978c81d37c81fc3
	jpeg4.dec.jpg	7ecd178674861ef3074a820f94bed5fb09894ff0115dfb704516afce1283233f
	Kemiripan	100%
10.	jpeg5.jpg	5fd792469110989c8f332270726773cc90f649b22ea4649e4e6f6e0298d0d3fc
	jpeg5.vig	83b48381294265614017aa30dacc737a740437981827fdef39bd45fb8ff0fa62
	jpeg5.dec.jpg	5fd792469110989c8f332270726773cc90f649b22ea4649e4e6f6e0298d0d3fc
	Kemiripan	100%

Tabel 4 menyajikan hasil pengujian lain yang dilakukan yaitu penghitungan persentase rata-rata perubahan ukuran *file* yang dihasilkan dari membandingkan ukuran *file* asli dengan ukuran *file* setelah dienkripsi. Pengujian yang dilakukan pada sepuluh *file* citra digital yang berbeda-beda baik dari segi ukuran *file* maupun dimensi menunjukkan bahwa terjadi penambahan ukuran *file* rata-rata sebesar 33,34%.

Penambahan ukuran rata-rata sebesar 33,34% ini tentu tidaklah buruk jika dibandingkan penggunaan algoritma Elgamal dengan mode operasi Electronic Code Book (ECB) untuk melakukan enkripsi citra digital seperti yang dilakukan oleh (Rizal, dkk., 2016).



Tabel 4. Pengujian perubahan ukuran file hasil enkripsi.

No	Nama File	Dimensi	Ukuran File	Ukuran Cipher
1.	1024px.png	1024 x 1024	41,1 KB	54,9 KB
2.	768px.png	768 x 768	39,8 KB	53,1 KB
3.	600px.png	600 x 600	29,5 KB	39,3 KB
4.	480px.png	480 x 480	22,6 KB	30,1 KB
5.	240px.png	240 x 240	10,0 KB	13,4 KB
6.	jpeg1.jpg	1280 x 853	239 KB	318 KB
7.	jpeg2.jpg	1280 x 870	180 KB	240 KB
8.	jpeg3.jpg	1920 x 1020	89 KB	118 KB
9.	jpeg4.jpg	1280 x 854	309 KB	413 KB
10.	jpeg5.jpg	2480 x 1388	401 KB	535 KB

Pengujian lain dilakukan dengan mengukur lama proses enkripsi dan dekripsi. Hasil uji lama proses enkripsi dan dekripsi tersaji pada Tabel 5.

Tabel 5. Pengujian lama proses enkripsi dan dekripsi.

No	Nama File	Dimensi	Lama Enkripsi	Lama Dekripsi
1.	1024px.png	1024 x 1024	0,036212921142578	0,041611194610596
2.	768px.png	768 x 768	0,036642074584961	0,038815975189209
3.	600px.png	600 x 600	0,028040885925293	0,026721954345703
4.	480px.png	480 x 480	0,020203828811646	0,020391941070557
5.	240px.png	240 x 240	0,010972023010254	0,0097010135650635
6.	jpeg1.jpg	1280 x 853	0,12175107002258	0,11409497261047
7.	jpeg2.jpg	1280 x 870	0,0935959815979	0,088201999664307
8.	jpeg3.jpg	1920 x 1080	0,046401023864746	0,043292999267578
9.	jpeg4.jpg	1280 x 854	0,15549278259277	0,1446430683136
10.	jpeg5.jpg	2480 x 1388	0,19454002380371	0,18740081787109

Pengujian yang dilakukan pada sepuluh *file* yang berbeda-beda baik dari segi ukuran *file* maupun dimensi menunjukkan bahwa proses enkripsi dilakukan dengan cepat dan membutuhkan waktu kurang dari 0,2 detik. Begitu pula dengan waktu yang digunakan untuk proses dekripsi yang tak terpaut jauh dengan proses enkripsi yaitu kurang dari 0,19 detik. Hal ini tentu saja merupakan hasil yang bagus jika dibandingkan dengan penggunaan algoritma Arnold's Cat Map oleh (Rachmawanto, dkk., 2019).

4. KESIMPULAN

Beberapa kesimpulan yang bisa didapatkan dari penelitian ini antara lain:

- Implementasi algoritma Vigenere Cipher untuk proses enkripsi *file* citra digital berhasil dilakukan. Hal ini dapat dibuktikan dari hasil uji validitas yang selalu memperoleh skor kemiripan sebesar 100% antara *file* citra digital asli dengan *file* citra digital hasil dekripsi.
- Proses enkripsi dan dekripsi *file* citra digital menggunakan algoritma Vigenere Cipher ini dilakukan dengan sangat cepat, terlihat dari proses enkripsi dan dekripsi yang memakan waktu tidak sampai dengan satu detik pada sepuluh sampel *file* uji.
- File* hasil enkripsi yang dihasilkan memiliki ukuran yang lebih besar rata-rata sebesar 33,34% dibanding dengan ukuran *file* aslinya.

Penggunaan *encoding* base64 sangat membantu menjembatani kekurangan algoritma Vigenere Cipher yang semula hanya mampu menangani data berupa teks. Penggunaan *encoding* ini dapat membantu proses enkripsi-dekripsi menggunakan algoritma Vigenere Cipher untuk *file* citra digital. Penelitian selanjutnya dapat dilakukan mengimplementasikan algoritma Vigenere Cipher ini untuk *file* dengan format yang beragam. Ide lain yang bisa dilakukan yaitu membandingkan kecepatan proses enkripsi maupun dekripsi dari algoritma Vigenere Cipher dengan algoritma kriptografi yang lain, termasuk dengan algoritma kriptografi modern.



DAFTAR PUSTAKA

- Anwar, F., Rachmawanto, E. H., Atika Sari, C., & Ignatius Moses Setiadi, D. R. (2019). StegoCrypt Scheme using LSB-AES Base64. *2019 International Conference on Information and Communications Technology (ICOIACT)*, July, 85–90. <https://doi.org/10.1109/ICOIACT46704.2019.8938567>
- Ariyus, D. (2006). *Kriptografi: Keamanan Data dan Komunikasi*. Graha Ilmu.
- Awad, M., Ali, M., Takruri, M., & Ismail, S. (2019). Security vulnerabilities related to web-based data. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 17(2), 852. <https://doi.org/10.12928/telkomnika.v17i2.10484>
- Fadlil, A., Riadi, I., & Nugrahantoro, A. (2020a). Kombinasi Sinkronisasi Jaringan Syaraf Tiruan dan Vigenere Cipher untuk Optimasi Keamanan Informasi. *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi*, 11(1), 81–95. <https://doi.org/10.31849/digitalzone.v11i1.3945>
- Fadlil, A., Riadi, I., & Nugrahantoro, A. (2020b). Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology. *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, 11(3), 155. <https://doi.org/10.24843/LKJITI.2020.v11i03.p04>
- Gerhana, Y. A., Insanudin, E., Syarifudin, U., & Zulmi, M. R. (2016). Design of digital image application using vigenere cipher algorithm. *2016 4th International Conference on Cyber and IT Service Management*, 1–5. <https://doi.org/10.1109/CITSM.2016.7577571>
- Gunadhi, E., & Sudrajat, A. (2017). Pengamanan Data Rekam Medis Pasien Menggunakan Kriptografi Vigenere Cipher. *Jurnal Algoritma*, 13(2), 295–301. <https://doi.org/10.33364/algoritma/v.13-2.295>
- Hermansa, Umar, R., & Yudhana, A. (2019). Analisis Sistem Keamanan Teknik Kriptografi dan Steganografi Pada Citra Digital (Bitmap). *Seminar Nasional Teknologi Fakultas Teknik Universitas Krisnadwipayana*, 520–528.
- Hernawandra, P., Supriyadi, S., & Lenggana, U. T. (2018). Aplikasi Steganografi Menggunakan LSB 4 Bit Sisipan dengan Kombinasi Algoritme Substitusi dan Vigenere Berbasis Android. *Jurnal Teknologi Dan Sistem Komputer*, 6(2), 44–50. <https://doi.org/10.14710/jtsiskom.6.2.2018.44-50>
- Mandal, S. K., & Deepti, A. R. (2016). A Cryptosystem Based On Vigenere Cipher By Using Multilevel Encryption Scheme. *International Journal of Computer Science and Information Technologies*, 7(4), 2096–2099.
- Maruf, F., Riadi, I., & Prayudi, Y. (2015). Merging of Vigenere Cipher with XTEA Block Cipher to Encryption Digital Documents. *International Journal of Computer Applications*, 132(1), 27–33. <https://doi.org/10.5120/ijca2015907262>
- Munir, R. (2006). *Kriptografi*. 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), 360–363.
- Prabowo, H. E., & Hangga, A. (2015). Enkripsi Data Berupa Teks Menggunakan Metode Modifikasi Vigenere Cipher. *Seminar Nasional Aplikasi Teknologi Informasi (SNATi)*, 1–4.
- Rachmawanto, E. H., Irawan, C., Studi, P., Informatika, T., Komputer, F. I., Dian, U., Semarang, N., & Digital, C. (2019). Enkripsi Dan Dekripsi Citra RGB Menggunakan Algoritma Arnold's Cat Map. *Prosceeding SENDI U*, 44–49.
- Riadi, I., Yudhana, A., & W, Y. (2020). Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, 7(4), 853. <https://doi.org/10.25126/jtiik.2020701928>
- Rihartanto, R., Ningsih, R. K., Gaffar, A. F. O., & Utomo, D. S. B. (2020). Implementation of vigenere cipher 128 and square rotation in securing text messages. *Jurnal Teknologi Dan Sistem Komputer*, 8(3), 201–209. <https://doi.org/10.14710/jtsiskom.2020.13476>
- Rizal, D., Sutojo, T., & Rahayu, Y. (2016). Implementasi Kriptografi Gambar Menggunakan Kombinasi Algoritma Elgamal Dan Mode Operasi ECB (Electronic Code Book). *Techno.COM*, 15(3), 231–240. <https://doi.org/10.33633/tc.v15i3.1240>
- Rojali, Salman, A. G., & George. (2017). Website-based PNG image steganography using the modified Vigenere Cipher, least significant bit, and dictionary based compression methods. *International Conference on Mathematics: Pure, Applied and Computation*, 020059. <https://doi.org/10.1063/1.4994462>
- Saputra, I., Hasibuan, N. A., Aan, M., & Rahim, R. (2017). Vigenere Cipher Algorithm with



- Grayscale Image Key Generator for Secure Text File. *International Journal of Engineering Research & Technology (IJERT)*, 6(1), 266–269.
- Setiadi, D. R. I. M., Jatmoko, C., Rachmawanto, E. H., & Sari, C. A. (2018). Kombinasi Cipher Substitusi (Beaufort Dan Vigenere) pada Citra Digital. *Prosceeding SENDI U*, 52–57.
- Sinaga, D., Umam, C., Setiadi, D. R. I. M., & Rachmawanto, E. H. (2018). Teknik Super Enkripsi Menggunakan Transposisi Kolom Berbasis Vigenere Cipher Pada Citra Digital. *Dinamika Rekayasa*, 14(1), 57. <https://doi.org/10.20884/1.dr.2018.14.1.198>
- Soofi, A. A., Riaz, I., & Rasheed, U. (2016). An Enhanced Vigenere Cipher For Data Security. *International Journal of Scientific & Technology Research*, 5(03), 141–145.
- Subandi, A., Lydia, M. S., Sembiring, R. W., Zarlis, M., & Efendi, S. (2018). Vigenere cipher algorithm modification by adopting RC6 key expansion and double encryption process. *IOP Conference Series: Materials Science and Engineering*, 420, 012119. <https://doi.org/10.1088/1757-899X/420/1/012119>
- Sumartono, I., Siahaan, A. P. U., & Arpan. (2016). Base64 Character Encoding and Decoding Modeling. *International Journal of Recent Trends in Engineering & Research (IJRTER)*, 02(12), 63–68. <https://doi.org/10.31227/osf.io/ndzqp>
- Wen, S., & Dang, W. (2018). Research on Base64 Encoding Algorithm and PHP Implementation. *2018 26th International Conference on Geoinformatics*, 1–5. <https://doi.org/10.1109/GEOINFORMATICS.2018.8557068>
- Yunita, S., Hasan, P., & Ariyus, D. (2019). Modifikasi Algoritma Hill Cipher dan Twofish Menggunakan Kode Wilayah Telepon. *SISFOTENIKA*, 9(2), 213. <https://doi.org/10.30700/jst.v9i2.489>
- Zebua, T., & Ndruru, E. (2017). Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma RC4. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, 4(4), 275–282. <https://doi.org/10.25126/jtiik.201744474>

