Vol. 4, No. 1, April 2023, hal. 182-192

p-ISSN: 2723-567X
e-ISSN: 2723-5661

Jurnal Computer Science and Information Technology (CoSciTech)

http://ejurnal.umri.ac.id/index.php/coscitech/index

Kombinasi algoritma kriptografi vigenere cipher dengan metode zig-zag dalam pengamanan pesan teks

Faris Apriliano Eka Fardianto*[1], Febi Yanto[2], Iwan Iskandar[3], Pizaini[4]
Email: [1]11850112401@students.uin-suska.ac.id, [2]febiyanto@uin-suska.ac.id, [3]iwan.iskandar@uin-suska.ac.id, [4]pizaini@uin-suska.ac.id

[1,2,3,4] Fakultas Sains dan Teknologi, Teknik Informatika, UIN Sultan Syarif Kasim, Riau, Indonesia

Diterima: 31 Maret 2023 | Direvisi: 14 April 2023 | Disetujui: 30 April 2023

Abstrak

Perkembangan teknologi yang begitu pesat semakin memudahkan dalam mendapatkan informasi secara cepat dan mudah. Ada informasi yang bersifat publik dan ada juga yang bersifat rahasia. Informasi yang bersifat rahasia tentunya memerlukan keamanan dalam menjaga kerahasiaanya oleh pihak yang tidak berkepentingan terhadap informasi tersebut. Ada banyak macam bentuk informasi rahasia, salah satunya informasi yang berbentuk teks. Untuk memberikan pengamanan pada pesan teks dapat dilakukan dengan teknik kriptografi. Teknik kriptografi bekerja dengan cara mengenkripsikan pesan asli (*plaintext*) menjadi teks yang susah dipahami (*ciphertext*), yang biasanya *ciphertext* tersebut tidak mengandung makna. Penelitian ini menggunakan kriptografi klasik yang dimana teknik enkripsi menggunakan kunci dekripsi yang digunakan sama dengan kunci enkripsi pada saat penyandian. Penelitian ini menggunakan algoritma kriptografii *vigenere cipher* dan *zig-zag cipher*. Algoritma *vigenere cipher* merupakan salah satu teknik kriptografi yang menggunakan suatu kata atau kalimat dengan panjang kunci menyesuaikan dengan plaintext-nya. Sedangkan *zig-zag* cipher menggunakan teknik transposisi dari kolom dan baris. Penggunaan dua algoritma kriptografi sekaligus dimaksudkan agar memberikan keamanan super enkripsi dengan kunci berlapis dan *cryptnalayst* akan kesulitan dalam memecahkan informasi yang telah disandikan. Pengujian dilakukan dengan melakukan perhitungan matematis dari algoritma *vigenere* maupun *zig-zag* terlebih dahulu yang digunakan sebagai dasar untuk diimplementasikan ke dalam sistem simulasi penyandian teks. Pada sistem yang telah dibuat memberikan hasil yang sama dengan perhitungan matematis. Pada pengujian pemecahan *ciphertext* dengan menggunakan sistem Boxentrix tidak dapat mengembalikan *plaintext* tanpa adanya kunci yang telah ditentukan. Sedangkan pada pengujian performa waktu bergantung pada jumlah karakter yang digunakan, semakin banyak jumlah karakter maka waktu enkripsi dan dekripsi juga semakin bertambah.

Kata kunci: *kriptografi, enkripsi, dekripsi, vigenere, zig-zag*

Combination of vigenere cipher cryptographic algorithm with zigzag method in securing text messages

Abstract

The rapid development of technology makes it easier to get information quickly and easily. Some information is public and some are confidential. Confidential information certainly requires security in maintaining confidentiality by parties not interested in the information. There are many forms of personal information, one of which is information in the form of text. Providing security to text messages can be done with cryptographic techniques. Cryptographic techniques work by encrypting the original message (plaintext) into text that is difficult to understand (ciphertext), which usually contains no meaning. This research uses classical cryptography where the encryption technique uses the decryption key used the same as the encryption key at the time of encoding. This research uses vigenere cipher and zigzag cipher cryptographic algorithms. Vigenere cipher algorithm is a cryptographic

technique that uses a word or sentence with the length of the key adjusting to the plaintext. In comparison, zigzag ciphers use transposition techniques from columns and rows. The use of two cryptographic algorithms at once is intended to provide super security, encryption with layered keys and cryptanalysts will be difficult in cracking the information that has been encoded. Testing is carried out by performing mathematical calculations from vigenere and zigzag algorithms first which are used as a basis for implementation into text encoding simulation systems. On the system that has been created gives the same result as mathematical calculations. In ciphertext cracking tests using the Boxentrix system cannot return plaintext in the absence of a predefined key. While in performance testing the time depends on the number of characters used, the more the number of characters, the encryption and decryption time also increases.

Keywords: *cryptography, decryption, encryption, vigenere, zig-zag*

1. PENDAHULUAN

Pada era digital saat ini kemajuan teknologi jaringan dan internet berkembang begitu pesat. Hal ini membuat komunikasi menjadi lebih cepat dan mudah [1]. Keamanan informasi merupakan hal yang harus diperhatikan dalam upaya melindungi informasi yang bersifat pribadi dan rahasia. Berkembangnya teknik pengambilan informasi secara illegal sering menyebabkan terjadinya pencurian informasi yang bukan haknya. Untuk mengamankan informasi tersebut, diperlukan teknik yang baik dalam merubah informasi dari pesan asli menjadi pesan yang tidak bisa dipahami oleh orang yang tidak berhak atas informasi tersebut. Salah satu cara yang bisa digunakan yaitu dengan mengacak data sehingga menjadi tidak jelas isinya, sehingga informasi yang tersimpan bisa terjaga kerahasiannya. Teknik penyandian dengan mengubah dan mengacak bentuk asli dari suatu informasi disebut dengan kriptografi [2].

Kriptografi merupakan teknik enkripsi yang mengubah teks asli (*plaintext*) yang diacak dengan menggunakan kunci enkripsi menjadi teks acak yang sulit untuk dibaca informasinya (*ciphertext*) oleh seseorang yang tidak memiliki kunci dekripsi [1], [3]. [1], [3]. Dekripsi dipecahkan dengan menggunakan kunci dekripsi untuk mendapatkan informasi data asli [3], [4]. Kriptografi berkaitan erat dengan keamanan dengan bentuk solusi berupa kata kunci. Semakin sulit kata kunci yang digunakan, maka kerahasiaan data akan semakin lebih besar peluangnya dibandingkan menggunakan kata kunci yang mudah sehingga tingkat keamanan cenderung rendah [4]. Kriptografi masa kini sudah banyak diterapkan pada berbagai media seperti teks [4], video [5], pesan chat [6], dan lainnya. Pada penelitian ini menggunakan kriptografi diterapkan pada pesan teks dengan menggunakan algoritma *vigenere cipher* dan metode *zig-zag cipher*.

Vigenere cipher merupakan algoritma kriptografi klasik dengan menerapkan kode abjad majemuk dengan teknik subtitusi atau mengganti teks asli (*plaintext*) menjadi teks kode (*ciphertext*) [2], [7]. Dalam melakukan proses enkripsi dan deskripsi *vigenere* menggunakan bujur sangkar *vigenere*. Penelitian *vigenere cipher* telah banyak dilakukan pada berbagai media, salah satunya pada citra digital [8] yaitu dengan mengubah file citra digital menjadi format *encoding* base 64. Hasil penelitian menunjukkan kemiripan 100% antara file citra digital asli dengan file citra digital yang sudah didekripsi. Penerapan *vigenere* juga pernah diterapkan pada transmisi media teks [9]. Metode *vigenere* bekerja dengan cara mengganti karakter *plaintext* dengan karakter yang ada pada tabel ASCII dengan menggeser tiap karakter dengan sebuah kunci. Pada proses enkripsi nilai dari tiap karakter *plaintext* dijumlahkan dengan nilai kunci dari *plaintext* ASCII untuk menghasilkan *ciphertext.* Pada proses dekripsi *ciphertext* yang dihasilkan dapat dikembalikan menjadi *plaintext* dengan mengurangkan nilai kunci dari *ciphertext* dan *ciphertext* ASCII. Selain itu, algoritma *vigenere cipher* juga pernah diimplementasikan pada keamanan resep obat [10] pada Puskesmas Metroyudan 1. Hasil implementasi memberikan kemudahan bagi dokter, apoteker, dan pasien serta dapat melindungi penyalahgunaan data obat yang tidak diinginkan.

Metode *vigenere cipher* tidak lagi dianggap sebagai *cipher* yang aman dan kurang populer digunakan. Hal ini disebabkan karena semakin meningkatnya keterampilan *cryptanalytic* (orang yang bisa memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci yang digunakan) dalam memecahkan kata yang telah disandikan [11]. Untuk menyiasati hal tersebut algoritma *vigenere cipher* dapat ditingkatkan keamanannya dengan cara melakukan kombinasi minimal dua atau lebih algoritma kriptografi klasik [7].

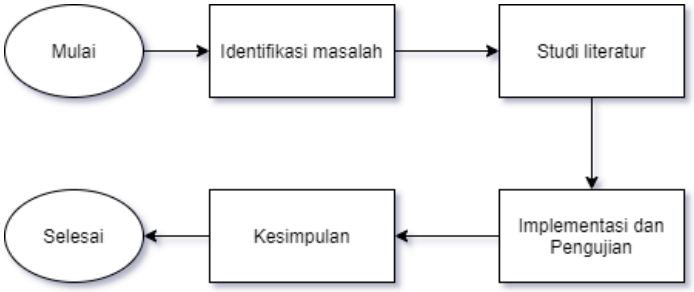
Metode *zig-zag cipher* merupakan algoritma kriptografi klasik dengan teknik transposisi yang menggunakan permutasi karakter [12]. Hanya orang yang memiliki kunci untuk dapat mengembalikan pesan yang sudah dienkripsi menjadi ke bentuk semula. Metode *zig-zag* memiliki kelebihan dimana proses penulisan *plaintext* menjadi *ciphertext* dapat dilakukan dari baris mana saja. Penerapan metode *zig-zag* pernah dilakukan pada pengamanan file video [5] dengan menggunakan bahasa pemrogaman *visual basic net* 2008. Sampel video yang digunakan berukuran 9 x 4 dengan format video hanya yang bertipe ekstensi *.mp4. Hasil akhir dari file video yang telah dienkripsikan membuat video menjadi buram sehingga objek yang ditampilkan tidak jelas. Dalam penerapannya *zig-zag cipher* sering dikombinasikan dengan metode kriptografi lainnya [13][14], hal ini dikarenakan algoritma ini hanya melakukan perubahan posisi pada kolom dan baris.

Pada penelitian ini melakukan kombinasi dari algoritma kriptografi *vigenere cipher* dengan metode *zig-zag cipher* yang bertujuan untuk meningkatkan keamanan pada sebuah pesan. Pesan teks asli dienkripsi dahulu dengan menggunakan algoritma *vigenere cipher*, kemudian hasil dari enkripsi *vigenere cipher* yaitu *ciphertext* dienkripsi lagi dengan menggunakan metode *zig-zag cipher*. Tahapan enkripsi yang dilakukan dua kali dimaksudkan agar meningkatkan keamanan informasi terhadap teks yang disandikan. Hasil penelitian ini diharapkan dapat memberikan solusi terhadap masalah keamanan informasi yang bersifat pribadi dan rahasia agar informasi yang tersimpan dapat terjaga agar tidak disalahgunakan oleh pihak yang tidak berkepentingan.

2. METODE PENELITIAN

2.1 Tahapan Penelitian

Metodologi penelitian adalah tahapan demi tahapan yang dilakukan di dalam penelitian secara terstruktur dan tersistematis agar penelitian yang dilakukan dapat memberikan hasil sesuai yang diharapkan. Berikut adalah kerangka penelitian pada Gambar 1 berikut:



Gambar 1. Kerangka Penelitian

a. Identifikasi Masalah
   Tahapan identifikasi masalah merupakan tahap awal yang dilakukan untuk mengetahui permasalahan agar dapat menemukan penyebab permasalahan serta solusi yang bisa dilakukan untuk menyelesaikan permasalahan tersebut. Penelitian ini dilakukan untuk meningkatkan keamanan pada pesan teks dengan mengombinasikan dua algoritma kriptografi klasik yaitu algoritma *vigenere cipher* dan *zig-zag cipher*. Penggunaan dua algoritma sekaligus dimaksudkan agar dapat memberikan keamanan super enkripsi dimana pesan teks yang disandikan dari tahap enkripsi maupun dekripsi sulit untuk dipecahkan oleh seseorang yang tidak memiliki kunci pesan tersebut.
b. Studi Literatur
   Tahapan studi literatur adalah tahapan yang dilakukan dalam menemukan informasi terkait, teori yang relevan, serta materi-materi yang berhubungan dengan penelitian yang dilakukan. Pada penelitian ini studi literatur yang digunakan berdasarkan penelitian-penelitian pada jurnal-jurnal terdahulu baik dari jurnal internasional maupun jurnal nasional. Selain itu ditambahkan juga dari beberapa sumber lain seperti buku, internet, dan sumber lainnya.
c. Implementasi dan Pengujian
   Tahapan implementasi merupakan tahapan pengaplikasian menggunakan *coding* pada algoritma yang digunakan pada penelitian yaitu metode *vigenere cipher* dan *zig-zag cipher*. Adapun pengujian yang digunakan yaitu pada performa waktu yang dibutuhkan dalam proses enkripsi maupun dekripsi.
d. Kesimpulan
   Tahapan kesimpulan merupakan tahap akhir yang menjelaskan kesimpulan dari penelitian yang telah dilakukan. Pada kesimpulan dapat dilihat keberhasilan suatu penelitian atau tidak.

2.2 Kriptografi

Kriptografi merupakan sebuah ilmu dalam keamanan informasi dengan cara mengenkripsikan dokumen asli *(plaintext*) menjadi informasi yang sulit (*ciphertext*) untuk dipahami [3], [12]. Adapun dokumen yang telah dienkripsikan dapat menjadi dokumen semula melalui tahapan dekripsi. Dalam tahapan dekripsi menggunakan kata kunci (*key*) yang berfungsi sebagai converter data [15], [16]. Pihak yang tidak mempunyai kunci memiliki kemungkinan yang sangat kecil untuk mengetahui teks asli yang telah disandikan [17], [9]. Dalam sejarahnya, kriptografi terbagi menjadi dua yaitu kriptografi klasik dan kriptografi modern [2], [7], [18]. Teknik kriptografi klasik digunakan sebelum adanya era komputerisasi dan teknik kunci yang digunakan yaitu teknik kunci simetris, dimana kunci dekripsi yang digunakan sama dengan kunci enkripsi pada saat penyandian. Pada kriptografi modern menggunakan pengolahan symbol biner pada komputer digital dengan tingkat kesulitan yang lebih kompleks. Kriptografi memiliki 4 komponen utama [19] yaitu *plaintext* (pesan asli), *ciphertext* (pesan sandi), *key* (kunci), dan algoritma yang digunakan. Penelitian ini menggunakan kriptografi klasik dengan teknik dasar yang biasa digunakan pada kriptografi klasik yaitu teknik subtitusi (pengganti) dan teknik transposisi [17]. Ada banyak macam algoritma dalam teknik kriptograpi klasik yaitu *vigenere cipher* [9], *zig-zag cipher* [14], *blowfish* [20], dan algoritma kriptografi lainnya.

2.3 *Vigenere Cipher*

Algoritma *vigenere cipher* diperkenalkan pada tahun 1586 untuk pertama kalinya oleh kriptologis asal Prancis yaitu Blaise De Vigenere. Algoritma *vigenere* dalam penerapannya menggunakan teknik subtitusi dimana kata asli teks yang disandikan diubah berdasarkan kunci yang telah ditentukan. Algoritma ini merupakan salah satu algoritma klasik yang tidak membutuhkan komputasi yang tinggi. Selain itu, *vigenere cipher* termasuk algoritma yang *simple* sehingga mudah dan cepat dalam proses pengenkripsianya. *Vigenere cipher* sendiri dalam prosesnya menggunakan alfabet yang biasanya disebut dengan tabel bujur sangkar *vigenere cipher* [3]. Tabel bujur sangkar tersebut digunakan untuk memudahkan dalam melakukan proses enkripsi maupun dekripsi. Adapun tabel bujur sangkar *vigenere* dapat dilihat pada Gambar 2 berikut.

KEY \ PLAINTEXT	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
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
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	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 2. Bujur Sangkar *Vigenere*

Tabel bujur sangkar *vigenere* berisi huruf alfabet yang berjumlah 26 yang dimulai dari A-Z. Adapun untuk penentuan nomor dari index tersebut dimulai dari index 0 yaitu pada huruf A dan seterusnya. Adapun dalam perhitungan matematika untuk proses enkripsi dapat dilihat pada persamaan (1) dan dekripsi pada persamaan (2).

$$C_i = (P_i + K_i) \; mod \; 26 \qquad (1)$$

$$P_i = (C_i - K_i) \; mod \; 26 \qquad (2)$$

Keterangan:

C_i = *Ciphertext* index ke-$_{i(0, 1, 2, ..i)}$

P_i = *Plaintext* index ke-$_{i(0, 1, 2, ..i)}$

K = *Key*

2.4 *Zig-Zag Cipher*

Algoritma *zig-zag* merupakan algoritma kriptogtafi klasik dengan teknik transposisi [11]. Teknik transposisi merupakan teknik merubah posisi setiap karakter sehingga informasi yang rahasia menjadi sebuah kata yang sudah diacak dan tidak bermakna.. Secara sederhana algoritma ini dapat digambarkan mirip seperti anagram [21] seperti pada kata “jurnal” menjadi “rnalju”, tetapi untuk perpindahan tiap karakter *cipher* tentunya memiliki rumus tertentu untuk dipecahkan kepada kata aslinya. Pada algoritma ini menggunakan parameter kunci sebagai baris pada pola *zig-zag*. Algoritma ini dapat digambarkan seperti pada Tabel 1 berikut.

Tabel 1. Contoh Tabel *Zig-Zag*

x		**x**		**x**	
	x		**x**		**x**

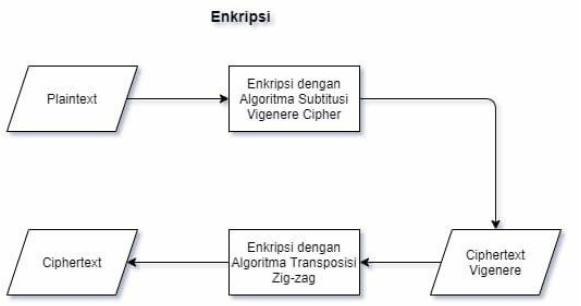
Pada Tabel 1 tersebut dapat dilihat nilai “x” berada di posisi *zig-zag*. Baris pada tabel tersebut adalah 2 yang melambangkan kunci yang digunakan yaitu 2. Untuk jumlah kolom yang digunakan disesuaikan dengan jumlah karakter. Misalnya kata “sukses” terdiri dari 6 karakter, maka jumlah kolom yang digunakan yaitu 6 kolom.

3. HASIL DAN PEMBAHASAN

Algoritma *vigenere cipher* dan *zig-zag cipher* merupakan algoritma simetris atau klasik yang dalam penerapannya menggunakan kunci yang sama baik dalam proses enkripsi maupun dekripsi. Penerapan kombinasi kedua algoritma tersebut dilakukan dengan

dua cara yaitu subtitusi dan transposisi. Pada *vigenere cipher* menggunakan teknik subtitusi yaitu mengganti karakter-karakter pada kata yang digunakan sesuai dengan kuncinya tanpa mengubah urutannya. Sedangkan pada *zig-zag cipher* menggunakan teknik transposisi yaitu dengan cara memindahkan posisi huruf-huruf sesuai dengan jumlah kunci yang digunakan.

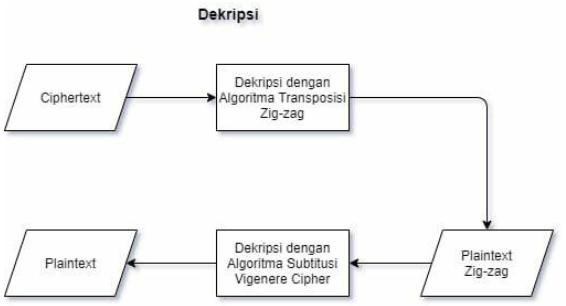
Adapun tahapan enkripsi menggunakan *vigenere cipher* yang dikombinasikan dengan *zig-zag cipher* dapat dijelaskan pada Gambar 3 di bawah ini,



Gambar 3. *Flowchart* Enkripsi

Pada Gambar 3 di atas merupakan tahapan enkripsi yang dimulai dari mengenkripsikan *plaintext* dengan menggunakan algoritma *vigenere cipher* dengan cara mensubtitusikan tiap karakter dari *plaintext* agar menjadi sebuah kata baru yang disebut dengan *cipher vigenere. Cipher vigenere* yang telah didapatkan dienkripsi lagi dengan menggunakan algoritma *zig-zag cipher* dengan transposisi karakter yang mengubah posisi karakter pada *cipher vigenere.* Dari proses enkripsi *zig-zag* tersebut didapatkanlah *ciphertext* yang akan digunakan pada tahap dekripsi.

Setelah proses enkripsi berhasil dilakukan didapatkan *ciphertext* acak dari *plaintext* yang telah disandikan. Untuk mengembalikan *ciphertext* dapat dilakukan pada tahapan dekripsi dimana proses dekripsi merupakan kebalikan dari tahapan enkripsi. Proses dekripsi dapat dilihat pada Gambar 4 di bawah ini.



Gambar 4. *Flowchart* Dekripsi

Proses awal dekripsi dimulai dengan cara mendekripsikan *ciphertext* dengan menggunakan algoritma transposisi *zig-zag cipher*. Hasil dekripsi *zig-zag* tersebut menghasilkan *plaintext* zig-zag yang didekripsi kembali oleh *vigenere cipher* dengan mensubtitusikan *plain zig-zag.* Dari hasil subtitusi *vigenere* didapatkan *plaintext* atau kata asli pesan semula yang telah berhasil dilakukan proses enkripsi maupun dekripsi.

3.1 Tahapan Perhitungan Manual

Tahapan perhitungan manual merupakan acuan dalam mengimplementasikan algoritma yang digunakan dalam penelitian dengan menggunakan bahasa pemrogaman yang dimuat dalam sebuah sistem enkripsi dan dekripsi. Hasil dari perhitungan algoritma *vigenere cipher* dan *zig-zag cipher* menjadi acuan pada pembuatan sistem simulasi. Pada pehitungan manual ini dapat melihat adanya kesamaan dengan hasil yang disimulasikan sistem. Apabila terdapat perbedaan antara perhitungan manual dengan yang disimulasikan dalam sistem dapat menjadi acuan untuk dilakukan perbaikan pada sistem itu sendiri.

1. Enkripsi

A. Enkripsi Pesan Teks Menggunakan *Vigenere Cipher* dan *Zig-zag Cipher*

Adapun tahapan perhitungan pada proses enkripsi pesan teks dari pihak pengirim dengan menggunakan algoritma *vigenere ciphere*, yaitu:

1. *Plaintext* = FARDIANTO

   Dari *plaintext* atau teks asli tersebut dirubah menjadi nomor abjad dengan index dimulai dari 0.

F	A	R	D	I	A	N	T	O
5	0	17	3	8	0	13	19	14

2. Kunci *vigenere* = TIGA

   Kunci *vigenere* digunakan sebagai nilai dari K_i dengan jumlah abjad kata kunci kecil dari jumlah *plaintext* yang digunakan. Apabila kata kunci yang digunakan telah habis sebelum dapat memenuhi jumlah kata sesuai dengan *plaintext*, maka kunci diulang dari huruf pertama dan seterusnya sampai jumlah *plaintext* dan jumlah kata kunci benrilai sama. Sama halnya dengan *plaintext*, kunci juga dirubah sesuai dengan nomor abjad yang dimulai dari index 0.

T	I	G	A	T	I	G	A	T
19	8	6	0	19	8	6	0	19

3. Proses ekripsi *vigenere cipher* untuk menghasilkan *ciphertext* dari *plaintext* yang telah ditentukan, yaitu:

   $C_1 = (P_1 + K_1) \bmod 26$
   $= (5 + 19) \bmod 26$
   $= 24 \bmod 26$
   $= 24 =$ **Y**

   $C_2 = (P_2 + K_2) \bmod 26$
   $= (0 + 8) \bmod 26$
   $= 8 \bmod 26$
   $= 8 =$ **I**

   $C_3 = (P_3 + K_3) \bmod 26$
   $= (17 + 6) \bmod 26$
   $= 23 \bmod 26$
   $= 23 =$ **X**

   $C_4 = (P_4 + K_4) \bmod 26$
   $= (3 + 0) \bmod 26$
   $= 3 \bmod 26$
   $= 10 =$ **D**

   $C_5 = (P_5 + K_5) \bmod 26$
   $= (8 + 19) \bmod 26$
   $= 27 \bmod 26$
   $= 1 =$ **B**

   $C_6 = (P_6 + K_6) \bmod 26$
   $= (0 + 8) \bmod 26$
   $= 8 \bmod 26$
   $= 8 =$ **I**

   $C_7 = (P_7 + K_7) \bmod 26$
   $= (13 + 6) \bmod 26$
   $= 19 \bmod 26$
   $=19 =$ **T**

   $C_8 = (P_8 + K_8) \bmod 26$
   $= (19 + 0) \bmod 26$
   $= 19 \bmod 26$
   $=19 =$ **T**

   $C_9 = (P_9 + K_9) \bmod 26$
   $= (14 + 19) \bmod 26$
   $= 33 \bmod 26$
   $= 7 =$ **H**

   Dengan demikian, hasil enkripsi dari pesan FARDIANTO dengan menggunakan algoritma *vigenere cipher* adalah *ciphertext*_1 = **YIXDBITTH**. *Ciphertext* ini akan digunakan pada proses enkripsi pesan selanjutnya yaitu dengan menggunakan metode *zig-zag cipher*.

Enkripsi dengan menggunakan *zig-zag cipher* menggunakan *ciphertext* yang berasal dari enkripsi *vigenere cipher* sebelumnya. Adapun tahapan perhitungan pada proses enkripsi pesan teks dari pihak pengirim dengan menggunakan algoritma *zig-zag cipher*, yaitu:

1. *Ciphertext*_1 = **YIXDBITTH**
2. Kunci = 3

   Dari ciphertext tersebut dienkripsi menggunakan kunci 3 yang diterapkan sebagai baris pada tiap tingkatan. *Ciphertext* tersebut dipecah menjadi karakter-karakter yang dimulai dari karakter pertama.

Y	→		B	→		H
	I	→ D	→	I	→ T	
		X	→		T	

   Ciphertext ditulis dari baris pertama, yang selanjutnya turun ke baris berikutnya dengan kolom yang berbeda. Proses tersebut dilakukan sesuai dengan jumlah kunci yang digunakan. Setelah kunci yang digunakan habis dilakukan dengan naik dari baris terbawah. Proses dilakukan berulang sampai *ciphertext* yang digunakan habis. Dengan demuikian setelah dilakukan enkripsi dengan menggunakan *zig-zag cipher* didapatkan *ciphertext*_2 yaitu **YBHIDITXT.**

2. Dekripsi

B. Dekripsi Pesan Teks Menggunakan *Zig-zag Cipher* dan *Vigenere Cipher*

Dekripsi dengan menggunakan *zig-zag cipher* menggunakan *ciphertext*2 yang berasal dari enkripsi kedua dari algoritma *zig-zag cipher* sebelumnya. Adapun tahapan perhitungan pada proses dekripsi pesan teks dari pihak penerima dengan menggunakan algoritma *zig-zag cipher*, yaitu:

1. *Ciphertext*_2 = **TBGKBUG**
2. Kunci = 3

   Tahapan pertama yang dilakukan dalam proses pendekripsian pesan dengan algoritma *zig-zag* yaitu dengan membuat tabel acuan dengan jumlah kolom sepanjang jumlah karakter *cipher* yaitu 7 karakter dan jumlah baris disesuaikan dengan kuncinya yaitu 3. Adapun tabel tersebut dapat dituliskan seperti di bawah ini, yaitu:

X				X				X
	X		X		X		X	
		X				X		

Melalui Tabel “” di atas dapat dijelaskan pada baris pertama diisi oleh 3 karakter dari *ciphertext*_2, baris kedua mendapatkan 4 karakter berikutnya, dan baris ketiga diisi oleh 2 karakter terakhir. Berikut Tabel “” yang telah diisi dengan karakter dari *ciphertext*_2

Y			B				H
	I		D		I	T	
		X				T	

Adapun untuk mendapatkan hasil *ciphertext*_1 dibaca dari kolom pertama pada baris pertama. Selanjutnya dilakukan pada kolom berikutnya dan baris berikutnya dengan menggunakan pola *zig-zag* sampai dengan karakter terakhir, Hasil dari dekripsi menggunakan *zig-zag cipher* yaitu *ciphertext*_1: **YIXDBITTH**

Dekripsi dengan menggunakan *vigenere cipher* menggunakan *ciphertext*_1 yang berasal dari dekripsi pertama dari algoritma *zig-zag cipher* sebelumnya. Adapun tahapan perhitungan pada proses dekripsi pesan teks dari pihak penerima dengan menggunakan algoritma *vigenere cipher*, yaitu:

1. *Ciphertext*_1 = **YIXDBITTH**
   Dari *ciphertext*_1 tersebut dirubah menjadi nomor abjad dengan index dimulai dari 0.

Y	I	X	D	B	I	T	T	H
24	8	23	3	1	8	19	19	7

2. Kunci *vigenere* = TIGA
   Kunci vigenere digunakan sebagai nilai dari Ki dengan jumlah abjad kata kunci kecil dari jumlah *ciphertext*_1 yang digunakan. Kunci *vigenere* dapat dituliskan sebagai berikut:

T	I	G	A	T	I	G	A	T
19	8	6	0	19	8	6	0	19

3. Proses dekripsi vigenere cipher untuk menghasilkan *plaintext* dari *ciphertext_1*, yaitu:

$P_1 = (C_1 - K_1) \bmod 26$
$= (24 - 19) \bmod 26$
$= 5 \bmod 26$
$= 5 =$ **F**

$P_2 = (C_2 - K_2) \bmod 26$
$= (8 - 8) \bmod 26$
$= 0 \bmod 26$
$= 0 =$ **A**

$P_3 = (C_3 - K_3) \bmod 26$
$= (23 - 6) \bmod 26$
$= 17 \bmod 26$
$= 17 =$ **R**

$P_4 = (C_4 - K_4) \bmod 26$
$= (3 - 0) \bmod 26$
$= 3 \bmod 26$
$= 3 =$ **D**

$P_5 = (C_5 - K_5) \bmod 26$
$= (1 - 19) \bmod 26$
$= -18 \bmod 26$
$= 8 =$ **I**

$P_6 = (C_6 - K_6) \bmod 26$
$= (8 - 8) \bmod 26$
$= 0 \bmod 26$
$= 0 =$ **A**

$P_7 = (C_7 - K_7) \bmod 26$
$= (19 - 6) \bmod 26$
$= 13 \bmod 26$
$= 13 =$ **N**

$P_8 = (C_8 - K_8) \bmod 26$
$= (19 - 0) \bmod 26$
$= 19 \bmod 26$
$= 19 =$ **T**

$P_9 = (C_9 - K_9) \bmod 26$
$= (7 - 19) \bmod 26$
$= -12 \bmod 26$
$= 14 =$ **0**

3.2 Implementasi Pada Sistem

Dari perhitungan matematis di atas menjadi dasar untuk acuan dalam pengecekan hasil pada sistem. Sistem berikut merupakan simulasi proses enkripsi maupun dekripsi dengan menggunakan algoritma *vigenere cipher* dan *zig-zag cipher* dengan menggunakan bahasa pemrogaman PHP. Adapun untuk melakukan implementasi sistem memerlukan perangkat pendukung yaitu perangkat keras (*hardware*) dan perangkat lunak (*software*), yaitu:

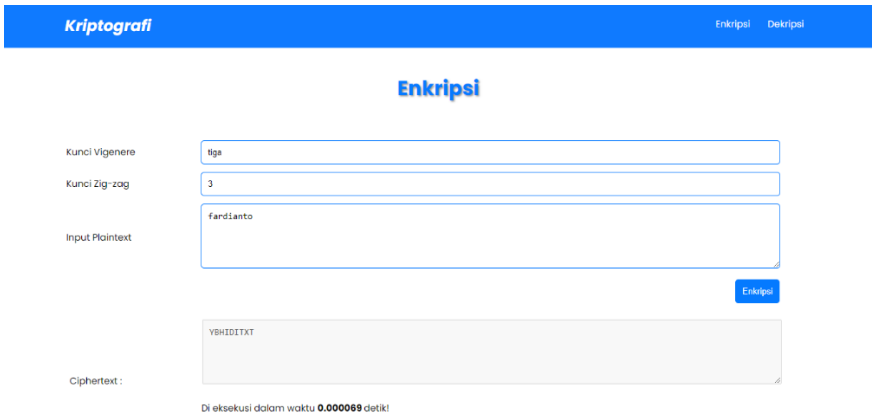
Perangkat keras (*hardware*):
1. *Processor* : Intel(R) Core (TM) i3-4030U CPU @ 1.90GHz (4 CPUs), ~1.9GHz
2. *Memory* : 8192. MB RAM
3. *Harddisk* : SSD Kingmax 240GB SATA

Perangkat lunak (*software*):
1. *Platform* : Windows 10
2. Bahasa Pemrograman : PHP
3. *Browser* : *Google Chrome*
4. *Server* : *localhost*
5. *Text Editor* : *Visual Studio Code*

Berikut merupakan tampilan dari sistem kombinasi kriptografi algoritma *vigenere cipher* dan *zig-zag cipher*.

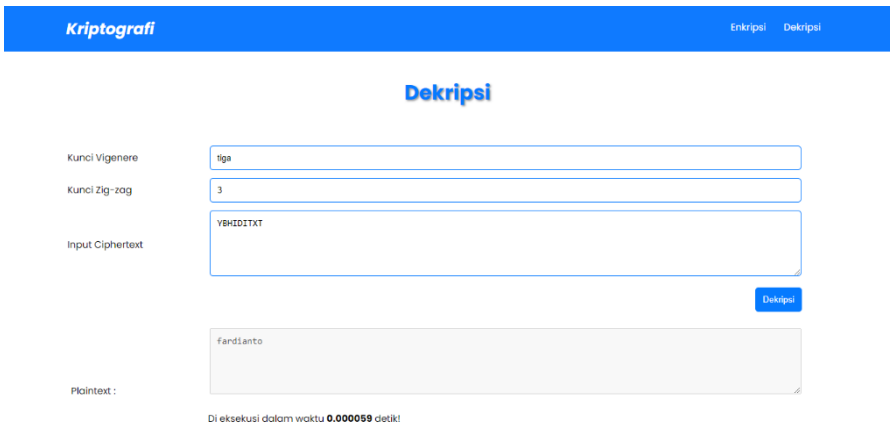
Gambar 5. Tampilan Awal Sistem Simulasi

Pada Gambar 5 di atas merupakan tampilan awal dari sistem simulasi sederhana kombinasi algoritma *vigenere cipher* dan *zig-zag cipher*. Pada sistem ini terdapat dua proses yaitu proses enkripsi dan proses dekripsi.



Gambar 6. Proses Enkripsi

Pada Gambar 6 di atas merupakan tahapan enkripsi. Teks yang digunakan yaitu “fardianto” dengan kunci *vigenere* “tiga” dan kunci zig-zag “3”. Dari proses enkripsi tersebut dihasilkan *ciphertext* “**YBHIDITXT**” dengan waktu eksekusi 0,000069 detik.



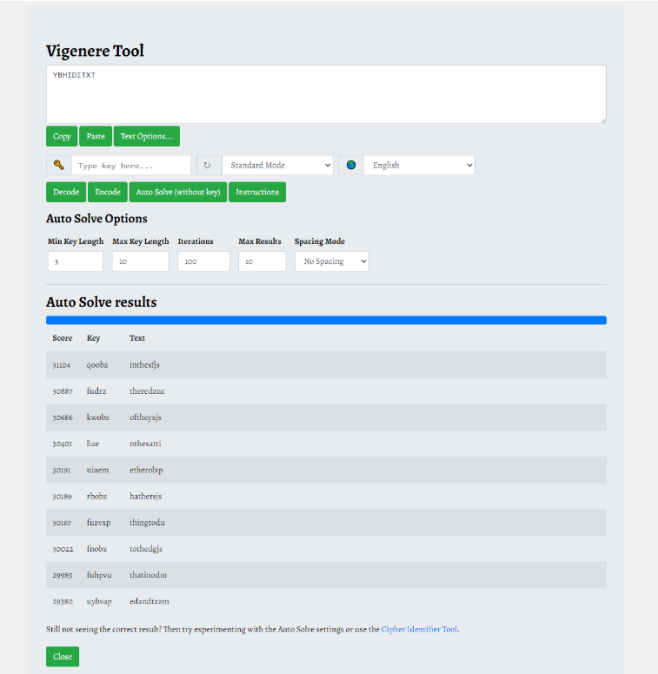
Gambar 7. Proses Dekripsi

Pada Gambar 7 di atas merupakan tahapan dekripsi. *Ciphertext* yang dihasilkan dari proses enkripsi sebelumnya digunakan pada teks yang ingin didekripsi yaitu “**YBHIDITXT**” dengan kunci *vigenere* “tiga” dan kunci *zig-zag* “3”. Dari proses dekripsi tersebut menghasilkan *plaintext* semula yaitu “**fardianto**” dengan waktu eksekusi 0,000059 detik.

Dari implementasi sistem tersebut memberikan hasil yang sama dengan perhitungan matematis baik dari proses enkripsi maupun dekripsi.

3.3 Pengujian *Ciphertext*

Pengujian ini dilakukan untuk menguji kekuatan *ciphertext* hasil kombinasi antara algoritma *vigenere cipher* dengan metode *zig-zag* yang dimana bisa dipecahkan atau tidak tanpa menggunakan kunci. Pengujian ini menggunakan sistem "Boxentrix" yaitu *vigenere cipher decoder and solver* untuk melakukan proses dekripsi dari *ciphertext* hasil kombinasi.

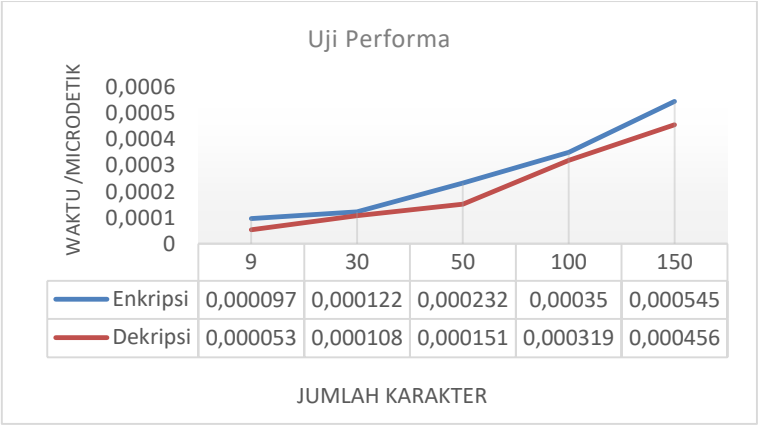


Gambar 8. Pengujian *Ciphertext*

Dari Gambar 8 tersebut menampilkan hasil dari *auto solve results* dengan 10 hasil. Dari 10 hasil yang ditampilkan tidak dapat mendekripsikan *ciphertext* menjadi *ciphertext*.

3.4 Pengujian Performa Waktu

Pengujian ini dilakukan untuk melihat waktu yang dibutuhkan dalam mengenkripsi dan mendekripsi pesan teks pada 5 kata dengan jumlah karakter yang berbeda-beda.



Gambar 9. Grafik Performa Waktu

Dari Gambar 9 tersebut dapat dilihat performa waktu dari 5 kata dengan jumlah karakter 9, 30, 50, 10, dan 150 yang digunakan pada tahap enkripsi maupun dekripsi mengalami kenaikan. Semakin banyak jumlah karakter yang digunakan, maka performa waktu dalam enkripsi maupun dekripsi bertambah.

4. KESIMPULAN

Berdasarkan dari penelitian yang telah dilakukan dapat disimpulkan, yaitu:

1. Algoritma *vigenere cipher* dan *zig-zag cipher* dapat digunakan untuk mengamankan pesan teks.

2. Algoritma *vigenere cipher* dan *zig-zag cipher* yang telah dikombinasikan mengasilkan *ciphertext* acak yang tidak bisa untuk didekripsi kembali tanpa mengetahui algoritma dan kunci yang digunakan.
3. Proses enkripsi dan dekripsi yang dilakukan secara manual maupun dengan menggunakan sistem mengasilkan hasil yang sama.
4. *Ciphertext* tidak dapat dipecahkan menjadi *plaintext* tanpa adanya kunci setelah diuji coba dengan sistem "Boxentrix".
5. Semakin banyak jumlah kata yang digunakan, maka waktu enkripsi dan dekripsi yang diperlukan semakin bertambah.

DAFTAR PUSTAKA

[1] N. Uniyal, G. Dobhal, A. Rawat, and A. Sikander, "A Novel Encryption Approach Based on Vigenère Cipher for Secure Data Communication," *Wirel. Pers. Commun.*, vol. 119, no. 2, pp. 1577–1587, 2021, doi: 10.1007/s11277-021-08295-5.

[2] M. Ziaurrahman, E. Utami, and F. W. Wibowo, "Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakan One Time Pad Dengan Enkripsi Berlanjut," *J. Inform. dan Teknol. Inf.*, vol. 4, no. 1, p. (halaman 2), 2019.

[3] M. O. I. Ruing and E. I. H. Ujianto, "Penerapan Kombinasi Algoritma Kriptografi (Caesar, Vigenere, Zig-Zag) Dan Metode Steganografi Lsb Untuk Mengamankan Pesan Ke Dalam Citra Digital," pp. 1–8, 2020, [Online]. Available: http://eprints.uty.ac.id/4888/.

[4] M. A. Maricar and N. P. Sastra, "Efektivitas Pesan Teks Dengan Cipher Substitusi, Vigenere Cipher, dan Cipher Transposisi," *Maj. Ilm. Teknol. Elektro*, vol. 17, no. 1, p. 59, 2018, doi: 10.24843/mite.2018.v17i01.p08.

[5] M. Zalukhu, K. J. Hondro, and Y. S. Hondro, "Aplikasi Pengamanan File Video Menggunakan Teknik Kriptografi Algoritma Transposisi Zig-Zag," *J. Mahajana Inf.*, vol. 3, no. 2, pp. 33–40, 2018.

[6] M. R. Firdaus and S. Waluyo, "Sistem Keamanan Chat Berbasis Web Menggunakan Algoritma Zig Zag Studi Kasus : Noktournal Motoshop," *Skanika*, vol. 1, no. 1, pp. 166–172, 2018.

[7] Jamaludin, "Rancang Bangun Kombinasi Chaisar Cipher dan Vigenere Cipher Dalam Pengembangan Algoritma Kriptografi Klasik," *Semant. (Seminar Nas. Tek. Inform.*, vol. 1, no. 1, pp. 234–243, 2017, [Online]. Available: https://semantika.polgan.ac.id/index.php/Semantika/article/view/36.

[8] Imam Riadi, Abdul Fadlil, and Fahmi Auliya Tsani, "Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 1, pp. 33–45, 2022, doi: 10.14421/jiska.2022.7.1.33-45.

[9] A. D. Achmad, A. A. Dewi, M. R. Purwanto, P. T. Nguyen, and I. Sujono, "Implementation of vigenere cipher as cryptographic algorithm in securing text data transmission," *J. Crit. Rev.*, vol. 7, no. 1, pp. 76–79, 2020, doi: 10.22159/jcr.07.01.15.

[10] D. Astuti and C. Sundari, "Implementasi Algoritma Vigenere Cipher Untuk Enkripsi Dan Dekripsi Pada Peresepan Data Obat Di Puskesmas Mertoyudan 1 Kabupaten Magelang," *J. Tek. Inf. dan Komput.*, vol. 5, no. 2, p. 341, 2022, doi: 10.37600/tekinkom.v5i2.534.

[11] V. K. Mittal and M. Mukhija, "Cryptosystem Based on Modified Vigenere Cipher using Encryption Technique," *Int. J. Trend Sci. Res. Dev.*, vol. 3, no. 5, pp. 1936–1939, 2019, doi: https://doi.org/10.31142/ijtsrd27878.

[12] A. Hariati, K. Hardiyanti, and W. E. Putri, "Kombinasi Algoritma Playfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks," *Sinkron*, vol. 2, no. 2, pp. 13–17, 2018, [Online]. Available: https://jurnal.polgan.ac.id/index.php/sinkron/index.

[13] R. S. Lubis, Tulus, and E. B. Nababan, "Pengamanan File Teks Menggunakan Algoritma RSA – LUC dan Algoritma Zig- Zag dalam Hybrid Crypto Sistem," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 6, no. 2, pp. 185–189, 2022.

[14] M. A. Budiman, Amalia, and N. I. Chayanie, "An Implementation of RC4+ Algorithm and Zig-zag Algorithm in a Super Encryption Scheme for Text Security," *J. Phys. Conf. Ser.*, vol. 978, no. 1, pp. 1–6, 2018, doi: 10.1088/1742-6596/978/1/012086.

[15] T. Zebua, "Analisa Perbandingan Least Significant Bit dan End of File Untuk Steganografi Citra Digital Menggunakan Matlab," no. July, 2018.

[16] O. Dakhi, M. Masril, R. Novalinda, J. Jufrinaldi, and A. Ambiyar, "Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Cipher," *INVOTEK J. Inov. Vokasional dan Teknol.*, vol. 20, no. 1, pp. 27–36, 2020, doi: 10.24036/invotek.v20i1.647.

[17] A. Amrulloh and E. I. H. Ujianto, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher," *J. CoreIT*, vol. 5, no. 2, pp. 71–77, 2019.

[18] A. Suheri, "Keamanan File Dengan Teknik Zig-zag dan Huffman," *Media J. Inform.*, vol. 9, no. 2, pp. 78–83, 2017, [Online]. Available: https://jurnal.unsur.ac.id/mjinformatika/article/view/450.

[19] M. D. Irawan, "Implementasi Kriptografi Vigenere Cipher Dengan Php," *J. Teknol. Inf.*, vol. 1, no. 1, pp. 11–21, 2017, doi: 10.36294/jurti.v1i1.21.

[20] A. E. Adeniyi, S. Misra, E. Daniel, and A. Bokolo, "Computational Complexity of Modified Blowfish Cryptographic Algorithm on Video Data," *Algorithms*, vol. 15, no. 373, pp. 1–14, 2022.

[21] Z. Huwaidi and K. Prayoga, "Penerapan Enkripsi Dan Dekripsi Pesan Menggunakan Algoritma Qwerty, Caesar Chiper, Dan Zig-Zag Chiper," *Fak. Ilmu Komputer, Univ. AMIKOM, Jur. Tek. Komput.*, pp. 1–4, 2018.