HASIL CEK_42 Pengamanan

by 42 Pengamanan Jurnal Dosen

Submission date: 28-May-2022 09:52AM (UTC+0700)
Submission ID: 1845719421
File name: 42 Pengamanan.pdf (1.09M)
Word count: 4035
Character count: 24153

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 157-169
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Pangamanan Pesan Menggunakan Kriptografi *Caesar Cipher* dan Steganografi EOF pada Citra

Hermansa[1], Rusydi Umar[2], Anton Yudhana[3]
Universitas Ahmad Dahlan,
Jl. Prof. Dr. Soepomo, S.H., Janturan, Umbul Harjo, Yogyakarta 55164, Indonesia
himmaherman@gmail.com

Abstract

Security in the protection of sending messages is a matter that must be considered, because the more the development of the age, the more sophisticated the technology. So that security in sending messages and data communication should be of more concern. Therefore we need a method or algorithm that can protect the message to be sent to the recipient of the message. The algorithm that can be used in encrypting is Caesar Cipher, as a cryptographic coding technique for messages so that messages that look difficult to read and solve. As for the method of inserting messages on encrypted image media using the End of File (EOF) steganography method, which is the method used directly at the end of the file. In the work of securing techniques of messages on this system, using various sizes of images or images that will be inserted a coded secret message or encryption whose capacity is not much different from the photos or images to be used. The conclusion of this study is that the application of the Caesar Cipher Algorithm can be used as a message security technique even though the algorithm is so simple but the level of security is assisted by the End of File (EOF) method to insert the encryption results from the Caesar Cipher algorithm so that the security level it has is sufficient to protect message information to be safe from eavesdroppers or hackers of the message that is not responsible or as a protection of data held.

Keywords: *Caesar Chiper, end of file, Message Security*

Abstrak

Keamanan dalam perlindungan pengiriman pesan merupakan hal yang harus diperhatikan, dikarenakan semakin berkembangnya zaman maka semakin canggih pula teknologi. Sehingga keamanan dalam pengiriman pesan maupun komunikasi data harus menjadi perhatian yang lebih. Oleh sebab itu dibutuhkan suatu metode atau algoritma yang dapat melindungi pesan yang akan dikirimkan kepada penerima pesan. Adapun Algoritma yang dapat digunakan dalam pengenkripsian yaitu Caesar Cipher*, sebagai teknik kriptografi pengkodean pesan agar pesan yang terlihat sulit dibaca dan dipecahkan. Sedangkan untuk metode penyisipan pesan pada media gambar yang telah dienkripsi menggunakan steganografi metode End Of File (EOF), yaitu metode yang digunakan langsung pada akhir file. Dalam pengerjaan teknik pengamanan pesan pada system ini, menggunakan berbagai ukuran citra atau gambar yang akan disisipkan pesan rahasia yang telah dikodekan atau enkripsi yang kapasitasnya tidak jauh beda dengan foto atau gambar yang akan digunakan. Kesimpulan dari penelitian ini adalah bahwa penerapan Algoritma Caesar Cipher bisa dijadikan teknik pengamanan pesan dengan baik walaupun algoritmanya yang begitu sederhana namun tingkat keamanannya dibantu dengan metode End Of File (EOF) untuk menyisipkan hasil enkripsi dari algoritma Caesar Cipher sehingga tingkat keamanan yang dimiliki cukup untuk melindungi pesan informasi agar aman dari para penyadap atau peretas pesan yang tidak bertanggung jawab maupun sebagai perlindungan data-data yang dimiliki.*

Kata kunci: *Caesar chiper, end of file, Pengamanan Pesan*

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 157-169
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

1. PENDAHULUAN

Keamanan dalam perlindungan pengiriman pesan merupakan hal yang harus diperhatikan, dikarenakan semakin berkembangnya zaman maka semakin canggih pula teknologi. Kerentanan dalam system layanan online berpotensi diserang peretas, serangan pada layanan online dapat terjadi kapan saja dan butuh solusi untuk memperbaikinya[1]. Layanan-layanan mesin pencari selalu berkembang yang berdampak pada privasi pengguna termasuk opsi fitur untuk menjelajahi Internet secara pribadi[2]. Sehingga keamanan dalam pengiriman pesan maupun komunikasi data harus menjadi perhatian yang lebih. Aktifitas manusia saat ini sebagian besar berhubungan dengan data, informasi, dan komunikasi, serta dalam kegiatannya secara langsung maupun tidak langsung akan berhubungan dengan perangkat teknologi *computer*[3]. Teknologi yang semakin canggih menjadi bagian yang tidak bisa lepas dari kehidupan masyarakat, tidak hanya melakukan kegiatan- kegiatan positif namun kegiatan-kegiatan negatif[4]. Sehingga celah-celah dalam pembobolan pengiriman pesan dizaman sekarang mudah terlihat dengan menggunakan berbagai macam penunjang baik *tools* aplikasi maupun melalui peretasan jaringan komunikasi data. Penjahat dunia maya terus mengubah strategi mereka untuk menargetkan media sosial yang berkembang pesat dan pengguna pesan yang ketat[5].

Manfaat teknologi memberikan banyak kemudahan kepada manusia dalam hal komunikasi. Walaupun memberikan dampak positif, kemajuan teknologi informasi dan telekomunikasi juga memberikan dampak negative juga yaitu banyaknya kejahatan yang berkaitan dengan aplikasi internet[6]. Dampak dari banyaknya kejahatan menggunakan teknologi informasi khususnya menggunakan Internet, dapat kita lihat dari beberapa kejahatan sering dilakukan dalam bentuk serangan yang terjadi dalam lembaga atau lembaga tertentu[7]. Oleh sebab itu dibutuhkan suatu metode atau algoritma yang dapat melindungi pesan yang akan dikirimkan kepada penerima pesan. Sehingga pesan yang hendak dikirimkan dapat dilindungi privasinya. Adapun Algoritma yang dapat digunakan dalam pengenkripsian yaitu *Caesar Cipher*, sebagai teknik kriptografi pengkodean pesan agar pesan yang terlihat, sulit dibaca dan dipecahkan. Sedangkan untuk metode penyisipan pesan pada media gambar yang telah dienkripsi menggunakan steganografi metode *End Of File* (EOF), yaitu metode yang digunakan langsung pada akhir *file*. Kriptografi sudah ada sejak dahulu sebelum masa digital berkembang, yang digunakan untuk keamanan privasi agar lebih aman, contohnya militer, utusan-utusan negara dan mata-mata, yang digunkan untuk menjaga kerahasiaan komunikasi yang dilakukan agar tidak tersebar atau tidak diketahui oleh pihak lain. Namun dizaman digital sekarang kriptografi tidak hanya sekedar keamanan komunikasi akan tetapi juga bisa digunakan untuk pengamanan data integritas, keaslian dan pemalsuan atau manipulasi [8]. Kriptografi *Caesar Cipher* merupakan salah satu teknik enkripsi yang terkenal dan sederhana dalam penanganan pengamanan pesan didunia. *Sandi Caesar* merupakan sandi subtitusi dimana

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 157-169
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

plaintext yang mau dikodekan ditukar dengan huruf lain yang mempunyai perbedaan tempat tertentu dalam *alphabet*[9].

Steganografi adalah cabang ilmu dari kriptografi yang memungkinkan pengguna untuk mengamankan pesan atau informasi rahasia dengan cara menyembunyikan pesan itu kedalam media tertentu[10]. Metode *End Of File* (EOF) merupakan metode yang dapat digunakan dalam menyisipkan file pada akhir berkas, sehingga wadah penyimpanan atau *image* tidak teralu nampak perubahan secara kasat mata dikarenakan metode ini memasukkan atau penyisipan akhir file yang digunakan, akan tetapi kelemahannya dari segi kapasitas ukuran *image* yang terlihat, sehingga dapat menimbulkan kecurigaan[11]. Citra sebagai representasi suatu system perekaman data dapat bersifat optik berupa foto, bersifat analog berupa sinyal-sinyal video seperti gambar pada monitor televisi, atau bersifat digital yang dapat langsung disimpan pada suatu pita *magnetic* [12]. Penelitian terdahulu banyak sekali yang membahas mengenai Kriptografi dalam pengamanan enkripsi pesan begitupun dengan steganografi dalam penyisipan pesan pada media penampung baik teks, citra (gambar), audio maupun video.

Diantara penelitian terdahulu yaitu, "Implementasi Kriptografi dan Steganografi dengan Metode Algoritma DES dan Metode *End of File*", pada penelitian ini maka didapatkan beberapa kesimpulan sebagai berikut: 1. Dari hasil percobaan yang telah dilakukan membuktikan bahwa aplikasi dapat mengacak dan menyembunyikan file dengan aman dan tidak menimbulkan kecurigaan pada pihak lain. Pada file hasil kriptografi dan steganografi tidak menimbulkan efek yang dapat merusak ataupun mengganggu kinerja file sebelumnya. 2. Hasil akhir yang diperoleh dari penggabungan 2 buah file yang berbeda ekstensi menghasilkan ukuran yang lebih besar yaitu merupakan gabungan dari ukuran kedua buah file tersebut yang dikarenakan file yang disembunyikan juga mempunyai kapasitas ukuran file sendiri [13].

"Penggunaan Algoritma Kriptografi Steganografi *Least Significant Bit* untuk Pengamanan pesan Teks dan Data Video", pada penelitian ini penggunaan Algoritma Kriptografi Steganografi *Least Significant Bit* dapat digunakan untuk memberikan pengamanan terhadap file video yang disisipkan oleh pesan teks, sehingga dengan menggunakan algoritma kriptografi steganografi LSB, bisa dijadikan sebagai suatu cara untuk memberikan pengaman terhadap *file video* yang akan dikirim kepada sipenerima [14].

"Pengamanan Data dengan Kombinasi Teknik Kriptografi Rabin dan Teknik Steganografi *Chaotic* LSB", pada penelitian ini Dari implementasi dan pengujian yang telah dibahas sebelumnya, penulis dapat menyimpulkan beberapa hal mengenai penelitian ini, diantaranya: 1. Penggunaan algoritma kriptografi Rabin sangat baik untuk data numeric yang relative kecil tetapi tidak cukup efektif untuk data dengan ukuran yang besar. 2. Teknik steganografi Chaotic LSB dapat dikombinasikan dengan algoritma kriptografi dan hal ini menjamin data yang tersimpan pada media stego (citra) lebih aman dan mengurangi kecurigaan terhadap kerahasiaan data. 3. Media stego

(gambar) yang dihasilkan dengan menggunakan teknik Chaotic LSB tidak mengalami perubahan warna yang kontras jika dibandingkan dengan citra yang dihasilkan oleh teknik steganografi LSB biasa. 4. Media stego (gambar) yang efektif berukuran 10 sampai 100 kali ukuran pesan yang ingin disisipin[15] .

"Implementasi Pengamanan Data dan Informasi dengan Metode Steganografi LSB dan Algoritma Kriptografi AES", pada penelitian ini didapatkan beberapa hasil kesimpulan dari pengujian yang dilakukan yaitu: 1) Pengujian terhadap beberapa *sample* membuktikan bahwa metode *Modified* LSB memenuhi aspek *imperceptibility*, dimana keberadaan pesan rahasia pada citra digital sulit untuk dipersepsi oleh inderawi. Hal ini karena perubahan yang terjadi tidak begitu berarti dan tidak menghasilkan perbedaan yang mencolok terhadap *stego object*. Pengujian terhadap aspek recovery menunjukkan bahwa cipherteks dapat diekstraksi dengan tepat menggunakan metode Modified LSB 2) Pengimplementasian teknik kriptografi AES dan steganografi dengan metode LSB pada data citra RGB berhasil dan berjalan dengan baik. Semakin besar ukuran pesan semakin lama proses enkripsi dan *embed*[16].

2. METODOLOGI PENELITIAN

Pada metodologi penelitian ini, peneliti melakukan tahapan-tahapan didalam mendapatkan hasil penelitian yang baik, mulai dari pengumpulan data, jurnal terkait, analisis masalah, alir penelitian, dan pengujian algoritma atau metode.

2.1. Pengumpulan Data

Tahap awal yang dilakukan adalah pengumpulan data mengenai kebutuhan yang dilakukan terhadap permasalahan yang akan diangkat atau dianalisa. Pengumpulan data disini berupa jurnal terkait sebagai pembanding atau referensi tambahan yang dapat melengkapi penelitian dan buku sebagai penjelasan komperehensif terhadap penelitian yang dilakukan.

2.2. Jurnal Terkait

Referensi terkait merupakan hal penting dalam pendalaman masalah yang akan dilakukan sebagai rujukan atau perbandingan berupa Jurnal terkait yang berhubungan dengan Steganografi dan Kriptografi khususnya metode EOF dan Algoritma *Caesar Cipher*. Jurnal terkait digunakan untuk pengembangan atau pembanding yang diambil berdasarkan intisari bacaan yang dilakukan dalam penelitian ini.

2.3. Analisis Masalah

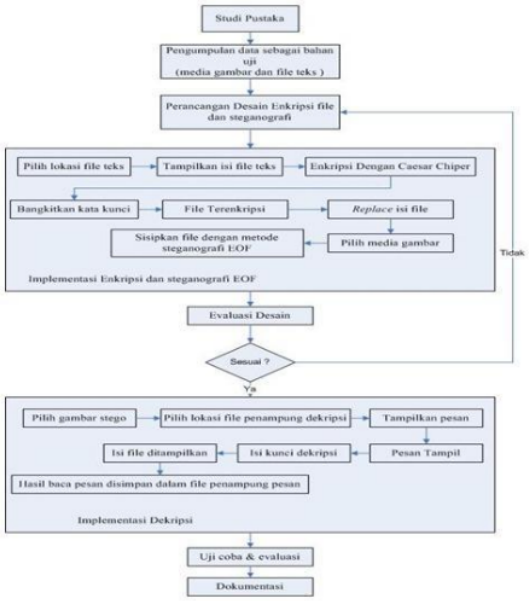
Setelah membaca dan memahami jurnal terkait maka setelah itu akan dilakukan analisa masalah mengenai bidang Kriptografi dan Steganografi. Analisa dilakukan dengan cara memahami kelemahan-kelemahan yang terdapat dalam Jurnal penelitian sebelumnya dan mengambil pemahaman

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 157-169
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

yang terdapat dalam pemikiran peneliti sebelumnya sebagai rujukan dan perbandingan dalam masalah yang akan diangkat sebagai data pegangan dalam pengembangan penelitian yang akan dilakukan.

2.4. Alir Penelitian

Alir penelitian adalah tahapan-tahapan yang dikerjakan dalam penelitian mulai dari awal, proses dan akhir. Konsep yang dibangun alir penelitian adalah penyesuaian yang dilakukan dalam analisa sistem sesuai dengan algoritma yang dibangun mulai dari pemilihan *stego image* (wadah penampung), proses enkripsi menggunakan algoritma *Caesar Cipher* kemudian *encode ciphertext* menggunakan metode *End of File* (EOF), sebagaimana dalam Gambar 1.

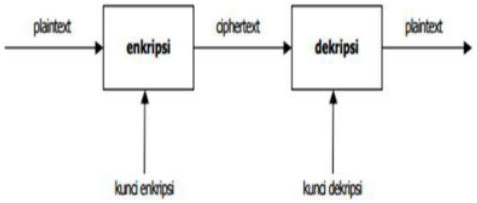


Gambar 1. Alir Penelitian

2.5. Enkripsi Caesar Cipher

Didalam *caesar cipher,* tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan alphabet. *Caesar cipher* tidak memiliki kunci, keamanan algoritma terletak pada kerahasiaan algoritmanya (hanya raja Julius Caesar para gubernurnya yang tahu). Dalam buku Practical Workbook: Information Theory, 4th edition, Department of Computer & Information System Engineering NED University of Engineering & Technology, Karachi, Pakistan [15], dijelaskan bahwa metode *Caesar cipher* yang digunakan menggunakan prinsip modulo 26. Secara matematis dapat dituliskan sebagai berikut:

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 157-169
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti



Gambar 2. Skema Enkripsi dan Dekripsi [17]

Pada teknik Caesar cipher ada dua deretan baris alphabet yang disusun, pada deratan baris pertama berisikan urutan alphabet A-Z dan pada deretan kedua berisikan alphabet sandi untuk mengenkripsi pergesaran dari plaintext.

Tabel 1. Substitusi

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
Ciphertext	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

Jadi, huruf a pada *plaintetx* disubstitusikan dengan D, huruf b disubstitusi dengan E, demikian seterusnya. Pergeseran huruf tersebut besifat siklik, jadi huruf x digeser menjadi A, huruf y menjadi B, dan huruf z menjadi C. Dalam prakteknya pegeseran siklik didalam *caesar cipher* ini dapat diimplementasikan dengan sebuah roda yang bernama *Caesar wheel.* Gambar 3 memperlihatkan *Caesar wheel. Caesar wheel* terdiri dari dua buah lempeng lingkaran besi. Lingkaran besi paling luar menyatakan huruf-huruf p*laintext* sedangkan lingkaran besi terdalam menyatakan huruf-huruf *ciphertext.* Lingkaran besi terdalam dapat diputar sejauh pergeseran yang diinginkan. Misalnya jika lingkaran besi terdalam digeser sejauh 3 huruf, maka susunan huruf-huruf didalam kedua lingkaran besi merepresentasi-kan tabel substitusi diatas.

Gambar 3. *Caesar Wheel* (Sumber: www.prizecodebreaker.com)

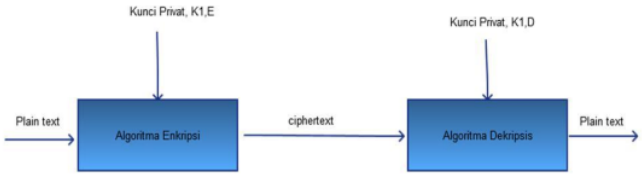
Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 157-169
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Untuk penerapan pengkodean pesan dengan cara mencari pesan huruf yang mau disandikan pada *alphabet* pertama kemudian tuliskan huruf sesuai dengan apa yang ada pada alphabet kedua.
Proses penghitungan biasa menggunakan rumus matematis operasi modulus dengan cara diketahui angka, A=0, B=1, Z=25. Enkripsi (E_n) dari "huruf" x dengan digeser n secara rumus diketahui dengan,

$$E_n(x) = (x + n) mod\ 26 \quad (1)$$

Adapun untuk proses pemunculan setelah dikodekan melalui Pendekripsian kode (D_n) yaitu:

$$D_n(x) = (x - n) mod\ 26 \quad (2)$$



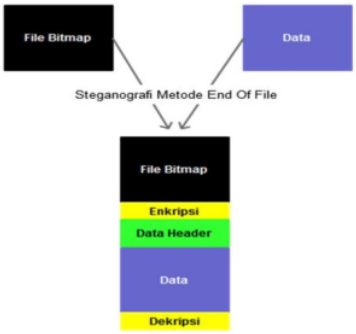
Gambar 4. Proses Enkripsi dan Dekripsi

Proses pengamanan pesan atau plaintext pada *Caesar Cipher* yaitu dengan cara pengenkripsian dengan menggunakan kunci (*Key*) sehingga menghasilkan *Ciphertext.* Adapun dalam proses Dekripsi dengan cara *ciphertext* dimasukkan kemudian menggunakan kunci (*key*) yang sama ketika proses enkripsi sehingga menghasilkan *plaintext* kembali.

2.6. Metode *End of File* (EoF)

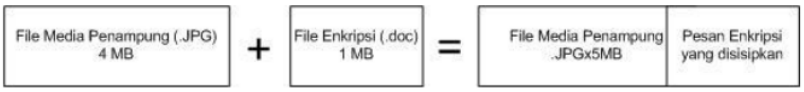
Dalam metode EOF memiliki tahapan-tahapan dalam penyisipan pesan agar pesan dapat disisipkan dengan baik dan tertata sesuai dengan sifat dari metode EOF. Adapun tahapan encode dari metode EOF yaitu, mengubah pesan menjadi nilai desimal, mencari letak nilai akhir dari piksel *citra,* memberikan sebuah tanda khusus sebagai pengenal pada pesan rahasia dan juga memberikan tanda desimal. Adapun pada tahapan proses *decode* atau pengungkapan pesan rahasia, maka proses yang dibutuhkan adalah mengetahui letak tanda pengenal dan mengambil nilai *decima*l dari pesan rahasia kemudian mengubah nilai desimal menjadi sebuah pesan. Tahapan *encode* pesan rahasia dapat dilihat pada Gambar 1.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 157-169
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti



Gambar 5. Konsep Metode *End of File* (EoF)[17]

Teknik EOF merupakan teknik yang memiliki model penyisipan pesan pada akhir file (Citra Image) dengan cara menambahkan pesan rahasia *ciphertext* dengan dikonversikan dari pesan asli *plaintext* kedalam bentuk angka atau karakter dengan bantuan table ASCII kemudian ditambahhkan pada akhir nilai pada media penampung.



Gambar 6. Alir *End of File*

Tahapan EoF dalam proses *encode message* dimulai dengan membaca ciri akhir dari *file citra*, kemudian masukkan atau sisipkan pesan yang telah dienkripsi kedalam media penampung dengan diberikan tanda awal dan akhir dari pesan enkripsi yang hendak disisipkan, terakhir adalah media penampung yang telah berisi enkripsi atau *ciphertext* dipisahkan menjadi sebuah *stego citra.* Adapun dalam tahapan *decode* pesan dimuai dengan membaca ciri tanda EoF media penampung, setelah itu pengambilan pesan enkripsi yang terletak pada EoF media penampung, kemudian yang terakhir adalah pisahkan tanda awal dan tanda akhir sehingga meninggalkan pesan enkripsi atau *ciphertext* yang siap didekripsi.

3. HASIL DAN PEMBAHASAN

Dalam pengerjaan teknik pengamanan pesan pada *system* ini, menggunakan berbagai ukuran citra atau gambar yang akan disisipkan pesan rahasia yang telah dikodekan atau enkripsi yang kapasitasnya tidak jauh beda dengan foto atau gambar yang akan digunakan. Pesan yang dienkripsi dan didekripsi menggunkan algoritma Caesar Cipher dan Metode penyisipan dan pengungkapan pada *stego image* menggunaka EOF.

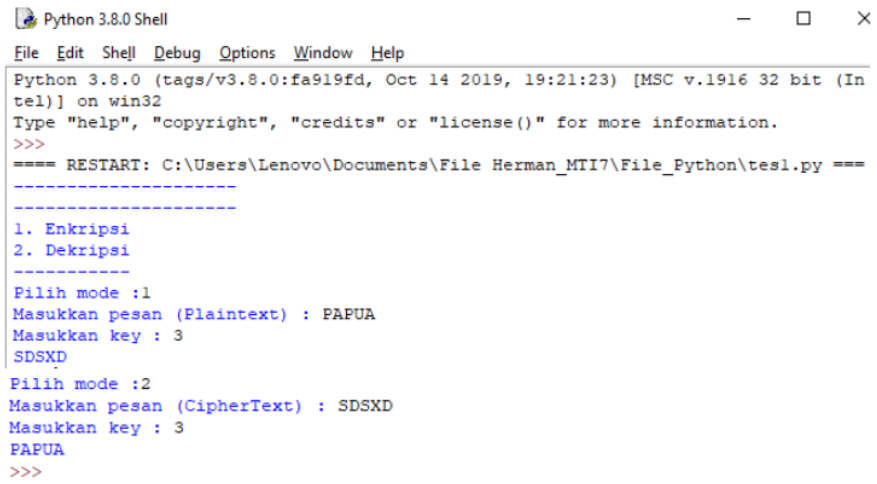
Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 157-169
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

3.1. Program Hasil Caesar Cipher

```
import string
abjad = string.printable

def enkrip (pesan):
    global abjad

    key = int (input ('Masukkan key : '))
    cipher=''
    for i in pesan :
        if i in abjad :
            k = abjad.find(i)
            k = ( k+key)%100
            cipher = cipher + abjad[k]
        else:
            cipher = cipher + i

    return cipher


def dekrip (cipher):
    global abjad

    key = int (input ('Masukkan key : '))
    pesan=''
    for i in cipher :


        if i in abjad :
            k = abjad.find(i)
            k = ( k-key)%100
            pesan = pesan + abjad[k]
        else:
            pesan = pesan + i

    return pesan

if __name__ == '__main__':
    print('---------------------')
    print('---------------------')
    pilihan = int (input ('1. Enkripsi\n2. Dekripsi\n-----------\nPilih mode :'))


    if pilihan == 1:
        pesan = input ('Masukkan pesan (Plaintext) : ')

    return pesan

if __name__ == '__main__':
    print('---------------------')
    print('---------------------')
    pilihan = int (input ('1. Enkripsi\n2. Dekripsi\n-----------\nPilih mode :'))


    if pilihan == 1:
        pesan = input ('Masukkan pesan (Plaintext) : ')
        print(enkrip(pesan))
    elif pilihan ==2:
        cipher= input ('Masukkan pesan (CipherText) : ')
        print (dekrip(cipher))
    else :
            print ('Masukkan pilihan 1 atau 2 !!')
```

Gambar 7. Program Enkripsi dan Dekripsi *Caesar Cipher*

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 157-169
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti



Gambar 8. Output Enkripsi dan Dekripsi *Caesar Cipher*

3.2. Enkripsi dan Dekripsi Pesan *Caesar Cipher*

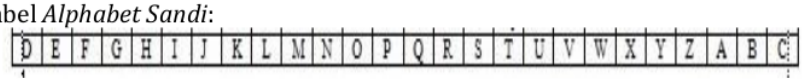
Pada pembahasan ini peneliti melakukan simulasi atau skenario dalam penerapan algoritma *Caesar Cipher s*sebagaimana dalam contoh berikut ini:

Plaintext: * PAPUA*
Tabel Alpabet A-Z:

Gambar 9. Alpabet A-Z

Proses awal yang dibutuhkan yaitu,pengurutan abjad A-Z yang berfungsi nantinya *plaintext* akan disubstitusikan dengan tabel *alphabet sandi* sehingga *plaintext* akan mengalami perubahan posisi yang tidak sama dari awalnya. Dalam pengurutan tidak harus menggunakan huruf *Capital* begitupun jika *plaintext dalam* bentuk angka maka pengurutannya bisa disesuaikan dengan angka.

Tabel *Alphabet Sandi*:



Gambar 10. Alpabet Sandi

Ciphertext: *SDSXD*

Tahap kedua yang dilakukan yaitu, menggunakan urutan *alpabhet* namun disini urutan dari *alphabet* telah mengalami pergeseran sebanyak tiga kali kesamping kiri sehingga dalam proses substitusi dengan *plaintext* akan mengalami perubahan dalam bentuk posisi yang sudah tidak sama,

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 157-169
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

perubahan bentuk posisi inilah yang disebut dengan *ciphertext.* Begitupun sebaliknya dalam tahapan dekripsi *ciphertext* yang telah mengalami perubahan posisi abjad maka dikembalikan dalam posisi semula baik jika telah mengalami tiga pergesaran maupun lebih sehingga *ciphertext* akan kembali pada posisi semula atau *plaintext.*

3.3. *Encode* dan *Decode Ciphertext* EOF

Dalam tahapan ini peneliti melanjutkan atau menggunakan pesan yang telah teracak dari proses enkripsi dari *Caesar Cipher.*

Ciphertext: SDSXD
Konversi Nilai ASCII: 42 83 68 83 88 68 42
Nilai wadah penampung atau *citra image* 8 x 8 yang mempunyai nilai dari setiap *pixel yaitu:*

Tabel 2. Nilai *Pixel Citra Image*

104	38	55	104	96	96	77	92
80	93	60	60	60	51	56	94
91	79	16	62	90	69	73	87
97	98	70	52	60	62	52	99
85	83	37	18	82	88	51	56
87	84	56	65	68	39	106	101
69	37	44	74	80	68	99	99
66	62	60	32	105	88	71	77

Nilai *pixel citra image* diatas akan disisipkan *ciphertext,42* 83 68 83 88 68 42. *Ciphertext* akan dimasukkan kedalam nilai *pixel citra image* pada akhir baris nila *pixel.* Pada nilai akhir *pixel ciphertext* akan diisi dengan penanda "y" yang diberi nilai 255. Sebagaimana pada Gambar 8.

Tabel 3. Nilai *Pixel Citra Image* yang telah disisipkan *Ciphertext*

104	38	55	104	96	96	77	92
80	93	60	60	60	51	56	94
91	79	16	62	90	69	73	87
97	98	70	52	60	62	52	99
85	83	37	18	82	88	51	56
87	84	56	65	68	39	106	101
69	37	44	74	80	68	99	99
66	62	60	32	105	88	71	77
42	83	68	83	88	68	42	255

Tahapan *Decode Ciphertext* atau pengambilan pesan tersembunyi pada media penampung *citra image yaitu:*

a. Masukkan media penampung yang disisipkan pesan rahasia/ *ciphertext.*

b. Mencari nilai akhir dari *pixel citra image* yang diletakkan pada akhir matriks pixel.
c. Mengambil pesan rahasia yang terletak pada baris akhir matriks citra sebelum akhir nilai penanda.
d. Konversikan kembali dari bilangan angka kepada symbol atau huruf dengan table ASCII.
e. Dekripsikan symbol dan huruf yang telah didapat kedalam tabel alphabet sandi dan tabel alphabet A-Z sehingga menghasilkan pesan asli atau plaintext.

4. SIMPULAN

Memberikan pernyataan bahwa apa yang diharapkan sebagaimana dinyatakan dalam "Pendahuluan" akhirnya dapat diperoleh hasil dalam "Hasil dan Pembahasan", sehingga terdapat kesesuaian. Selain itu dapat juga ditambahkan prospek pengembangan dari hasil penelitian dan aplikasi lebih jauh yang menjadi prospek kajian berikutnya.

Kesimpulan dari penelitian ini adalah bahwa penerapan Algoritma *Caesar Cipher* bisa dijadikan teknik pengamanan pesan dengan baik walaupun algoritmanya yang begitu sederhana dikarenakan algoritma yang digunakan adalah Kriptografi Klasik namun tingkat keamanannya dibantu dengan metode EOF untuk menyisipkan pesan rahasia dari algoritma *Caesar Cipher* sehingga tingkat keamanan yang dimiliki cukup untuk melindungi pesan informasi agar aman dari para penyadap atau peretas pesan yang tidak bertanggung jawab maupun sebagai perlindungan data-data yang dimiliki.

Untuk pengembangan selanjutnya bisa menggunakan algoritma yang kompleks atau Kriptografi moderen contohnya, DES, Triple DES, AES, RC4, A5, dan sebagainya. Begitupun untuk Metode Steganografi bisa menggunakan metode lainnya. Kemudian pada program yang ingin dibuat bisa menggunakan dalam bentuk visual yang lebih baik lagi dalam bentuk aplikasi.

DAFTAR PUSTAKA

[1] A. Yudhana, I. Riadi, and F. Ridho, "DDoS classification using neural network and naïve bayes methods for network forensics," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 11, pp. 177–183, 2018.
[2] R. Umar, A. Yudhana, and M. N. Faiz, "Experimental analysis of web browser sessions using live forensics method," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 2951–2958, 2018.
[3] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," vol. 3, no. 1, pp. 70–82, 2018.
[4] M. I. Syahib, I. Riadi, and R. Umar, "Analisis Forensik Digital Aplikasi Beetalk Untuk Penanganan," *Semin. Nas. Inform. 2018 (semnasIF 2018) UPN "Veteran" Yogyakarta, 24 Novemb. 2018*, vol. 2018, no. November, p. 134, 2018.
[5] N. Anwar and I. Riadi, "Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web," *J. Ilm. Tek. Elektro Komput.*

dan Inform., vol. 3, no. 1, p. 1, 2017.

[6] I. Zuhriyanto *et al.*, "Perancangan Digital Forensik Pada Aplikasi," vol. 2018, no. November, pp. 86–91, 2018.

[7] I. Riadi, A. Yudhana, and M. C. F. Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute of Justice (Nij)," *J. Tek. Inform. dan Sist. Inf.*, vol. 4, no. 2, pp. 219–227, 2018.

[8] M. H. Arif and A. Z. Fanani, "Kriptografi Hill Cipher Dan Least Significant Bit Untuk Keamanan Pesan Pada Citra," *CSRID (Computer Sci. Res. Its Dev. Journal)*, vol. 8, no. 1, p. 60, 2016.

[9] E. I. M. Aida Halimatusadiah, "IMPLEMENTASI KRIPTOGRAFI METODE CAESAR CHIPER PADA CHATING BERBASIS WEB," *CAESAR CIPHER CHATING*, vol. 1, 2016.

[10] P. Fitriani and T. S. Alasi, "Pengamanan Pesan Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit Pada Citra Digital," *J. Inf. Komput. Log.*, vol. 1, no. 2, pp. 35–38, 2019.

[11] B. V. Indriyono, "Implementasi Sistem Keamanan File dengan Metode Steganografi EOF dan Enkripsi Caesar Cipher," *Sisfo*, vol. 06, no. 01, pp. 1–16, 2016.

[12] M. K. Achmad Ardiansyah, "Penyembunyian Pesan Rahasia Pada Citra Digital Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB)," *J. Teknol. Inf.*, vol. XIII, no. November, pp. 96–101, 2018.

[13] A. Rohmanu, "Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma Des dan Metode End Of File Ajar Rohmanu," *J. Inform. SIMANTIK*, vol. 1, no. 2, pp. 1–11, 2017.

[14] I. Gunawan, "Penggunaan Algoritma Kriptografi Steganografi Least Significant Bit Untuk Pengamanan Pesan Teks dan Data Video," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 2, no. 1, p. 57, 2018.

[15] M. Zarlis and dan Tulus, "Pengamanan Data dengan Kombinasi Teknik Kriptografi Rabin dan Teknik Steganografi Chaotic LSB," 2015.

[16] S. Anwar, M. I. Komputer, and U. B. Luhur, "Implementasi Pengamanan Data Dan Informasi Dengan," pp. 37–42, 2017.

[17] D. Kusumaningsih, A. Pudoli, and I. Rahmadan, "Steganografi Metode End of File Untuk Keamanan Data," vol. 9, no. 1, pp. 47–55, 2017.

HASIL CEK_42 Pengamanan

ORIGINALITY REPORT

9%	9%	3%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	dedyhermaw.blogspot.com Internet Source	3%
2	github.com Internet Source	3%
3	docobook.com Internet Source	3%

Exclude quotes	On	Exclude matches	< 3%
Exclude bibliography	On		