STEGANOGRAFI DAN MODIFIKASI CIPHER SUBSTITUSI MENGGUNAKAN KODE ASCII DAN DERET FIBONACCI

STEGANOGRAPHY AND SUBSTITUTION CIPHER MODIFICATION USING CODE ASCII AND FIBONACCI SERIES

Musthofa Galih Pradana*[1], Bondan Wahyu Pamekas[2]
[1]Universitas Alma Ata, Yogyakarta.
[,2]Universitas AMIKOM, Yogyakarta.
e-mail: ***[1]mgalihpradana@almaata.ac.id** , [2]bondan.1044@students.amikom.ac.id

Abstrak

Ilmu Kriptografi banyak dimanfaatkan untuk mengamankan data dan informasi baik agar tidak mudah disalahgunakan oleh pihak yang tidak berkepentingan terhadap data tersebut. Salah satu jenis algoritma kriptografi adalah Caesar Cipher dan Vigenere Cipher. Kedua algoritma tersebut merupakan algoritma kriptografi klasik yang perlu dilakukan proses modifikasi agar menjadi lebih optimal dalam proses pengamanan data. Modifikasi yang pertama adalah dengan memodifikasi kunci Vigenere menggunakan Fibonacci. Pada umumnya Vigenere Cipher akan mengulang kata kunci yang sama untuk melengkapi jumlah karakter yang kurang sehingga jumlah karakternya sama dengan jumlah karakter pada plainteks. Modifikasi kedua adalah dengan mengubah atau mengkonversi huruf plainteks ke dalam huruf ASCII agar kode lebih susah dipecahkan. Setelah proses konversi ASCII dilakukan, maka berikutnya hasil akan di konversi kembali dalam huruf Hexa. Selain kedua modifikasi yang dilakukan, ditambahkan juga teknik steganografi dengan menyembunyikan kode dibalik media berupa gambar. Gambar yang menjadi sample akan dilakukan rename dan disimpan pada tempat yang berbeda.

Kata kunci—Caesar Cipher, Vigenere Cipher, Modifikasi, Steganografi, Kriptografi.

Abstract

Cryptography is widely used to secure data and information so that it is not easily misused by parties who are not interested in the data. One type of cryptographic algorithm is Caesar Cipher and Vigenere Cipher. Both of these algorithms are classic cryptographic algorithms that need to be modified so that they become more optimal in the data security process. The first modification is to modify the Vigenere key using Fibonacci. In general, Vigenere Cipher will repeat the same keyword to complete the number of characters that are lacking so that the number of characters is the same as the number of characters in the plaintext. The second modification is to change or convert plaintext letters into ASCII letters so that the code is more difficult to solve. After the ASCII conversion process is done, the next results will be converted back in Hexa letters. In addition to the two modifications made, the steganography technique is also added by hiding the code behind the media in the form of images. Images that are sampled will be renamed and stored in different places.

Keywords—*: Caesar Cipher, Vigenere Cipher, Modification, Steganography, Cryptography.*

1. PENDAHULUAN

Kriptografi digunakan untuk menjaga dan melindungi keamanan data. Jenis algoritma dalam Kriptografi sangat banyak, dari yang sederhana sampai yang rumit. Tingkat kerumitan algoritma menjadikan tingkat keamanan menjadi lebih baik. Namun algoritma yang sederhana bukan berarti

tidak dapat menjadi alternatif yang baik untuk diterapkan mengamankan data. Salah satu jenis algoritma klasik adalah Algoritma Caesar Cipher dan Vigenere Cipher. Kedua algoritma ini termasuk dalam algoritma klasik yang mudah dipecahkan.

Algoritma klasik seperti Caesar dan Vigenere dapat ditingkatkan lagi kemampuan dalam melindungi data dengan modifikasi dan penambahan teknik lain di dalamnya. Dalam penelitian ini dilakukan modifikasi dan kombinasi antara Algoritma Caesar Cipher dan Vigenere Cipher serta dilakukan penambahan fitur steganografi dengan tujuan meningkatkan tingkat kehandalan algoritma.

Modifikasi yang dilakukan berfokus pada algoritma Vigenere Cipher dimana ada 2 jenis modifikasi yang dilakukan. Yang pertama adalah dengan membuat kunci otomatis Vigenere Cipher. Pada normalnya jika kata kunci pada Vigenere Cipher lebih kecil dari plainteks maka kata pada kunci akan diulang dengan kata atau huruf yang sama untuk melengkapi kunci agar sesuai dengan jumlah karakter plainteks. Pada modifikasi yang dilakukan, pengulangan kunci di generate secara otomatis oleh sistem menggunakan rumus deret fibonnacci.

Modifikasi yang kedua dilakukan dengan mengubah plainteks sebelum diolah di Vigenere Cipher, dilakukan konversi ke dalam huruf ASCII. Setelah dirubah ke dalam huruf ASCII, maka hasil berupa cipherteks masih akan dikonversi menjadi huruf hexa. Dengan modifikasi ini diharapkan akan mempersulit proses pemecahan algoritma.

Selain itu penambahan fitur Steganografi menggunakan media gambar dapat menjadikan keamanan dari pesan lebih baik, dikarenakan tidak hanya media teks saja, namun sudah bisa disembunyikan di dalam sebuah gambar multimedia.

Beberapa penelitian tentang kriptografi pernah yang dapat dijadikan referensi diantaranya oleh Dr. M. Ilayaraja, Dr. K.Shankar, Dr. G. Devika dengan judul A Modified Symmetric Key Cryptography Method forSecure Data Transmission. Pada penelitian ini Caesar Cipher dimodifikasi menggunakan ASCII code untuk meningkatkan keamanan data [1].

Selanjutnya penelitan Ansar Rizal, Didi Susilo Budi Utomo, Rihartanto Rihartanto, Marselina Endah Hiswati, Haviluddin Haviluddin yang melakukan penelitian dengan memodifikasi vigenere cipher dengan multi cycle encryption. Hasil dari penelitian ini adalah berhasil mengimplementasikan modifikasi dengan 128 ASCII code dan multi cycle key encryption [2].

Penelitian yang dilakukan Sewindu Putro dkk yang melakukan modifikasi Caesar cipher dan Playfair menggunakan kode pos. Proses enkripsi yang dilakukan adalah dengan melakukan enkripsi dengan 2 algoritma dahulu, baru dilakukan conversi kedalam plat nomor dan kode pos [3].

Kriptografi dengan Algortima Caesar Cipher pernah ditulis oleh Retnani Latifah dkk, dengan melakukan modifikasi menggunakan kode ASCII dan kombinasi dengan algoritma Rail Fence. Akan lebih baik lagi, jika pada penelitian ini dapat ditambahkan fitur steganografi yang dapat menjadi nilai lebih [4].

Peneltian rujukan yang berikutnya adalah dari Angga Aditya Permana, yang melakukan penerapan algoritma Vigenere Cipher dengan aplikasi berbasis Android. Penerapan Vigenere Cipher pada android belum disertai modifikasi yang bisa memperbaiki performa keamanan algoritma [5].

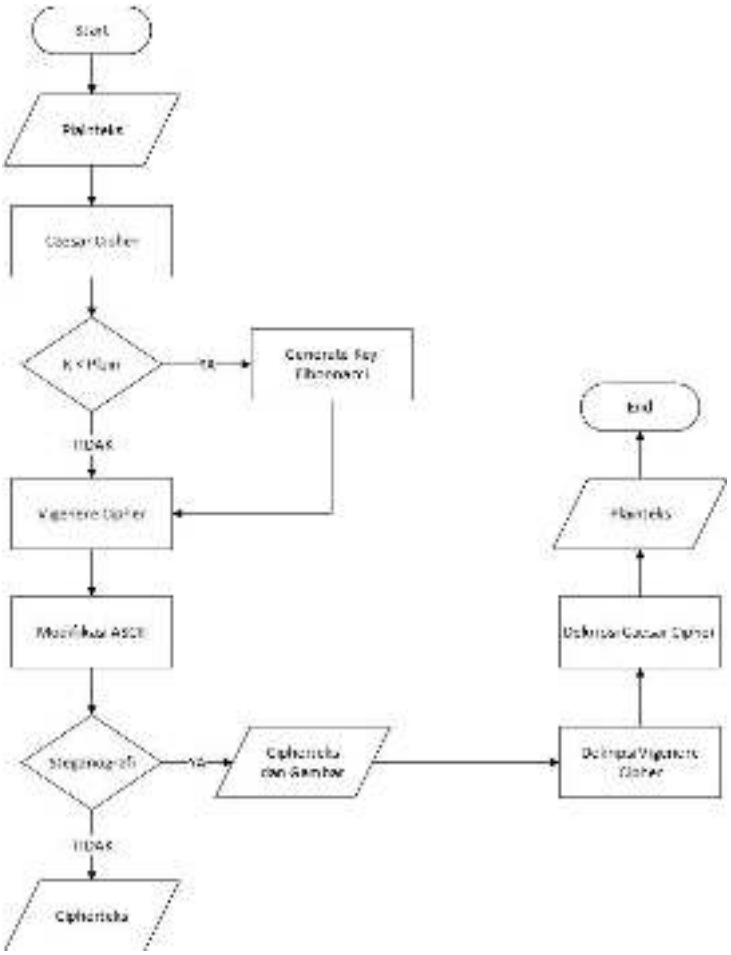
Optimalisasi cipher substitusi juga pernah dituliskan oleh dony ariyus dan ardiansyah dengan nmenggunakan LSB Method. Modifikasi kriptografi dilakukan di metode viginere cipher dengan menggunakan letters key dan hill cipher, selain itu juga dilakukan modifikasi di Hill Cipher, Caesar Cipher dan One Time Pad (OTP) [6].

Modifikasi vigenere cipher yang dituliskan Khairun Nahar, Partha Chakraborty memodifikasi Vigenere Cipher menggunakan tabel 95x95. Modifikasi ini memperbanyak karakter yang digunakan. Dan semua jenis tulisan (lower dan upper case alphabets) harus dilakukan konversi ke uppercase alphabet sebelum dilakukan enkripsi. Ini meminimilaisir case sensitive yang terjadi di algoritma vigenere sebelum dilakukan modifikasi [7].

Rujukan yang terakhir adalah dari A Subandi, M S Lydia, R W Sembiring, M Zarlis dan S Efendi yang melakukan modifikasi vigenere cipher dengan mengadopsi RC6 key expansion dan juga melakukan proses enkripsi vigenere sebanyak 2 kali untuk meningkatkan tingkat keamanan data [8]
.

2. METODE PENELITIAN

Alur dari sistem pertama adalah dengan memasukan teks kemudian, input kunci Caesar dan Vigenere. Ada 2 pilihan untuk langsung memproses dalam algoritma kriptografi atau menambahkan proses steganografi, ketika steganografi dipilih maka kode plainteks akan disembunyikan dibalik gambar. Adapun detail dari alur penelitian ditunjukan pada
Gambar *1*.



Gambar 1. Alur Penelitian

2.1 Caesar Cipher

Caesar Cipher adalah salah satu jenis algoritma Cipher Substitusi. Cara yang digunakan pada metode ini adalah dengan menggeser alphabet sebanyak 3 huruf ke sebelah kanan. Caesar Cipher merupakan teknik kriptografi yang paling lemah. Caesar Cipher mudah dipecahkan dengan exhaustive key search karena jumlah kuncinya sangat sedikit (hanya 26 kunci) [6].
Model matematis dari proses enkripsi caesar cipher dapat dihitung dengan menggunakan persamaan :

$$C = E(P, K) = (P + K)\ mod\ 26 \qquad (1)$$

Sedangkan proses dekripsi metode caesar cipher dapat menggunakan persamaan :

$$P = D\ (C, K) = (C - K)\ mod\ 26 \qquad (2)$$

2. 2 Vigenere Cipher

Vigenere Cipher termasuk ke dalam cipher abjad-majemuk (polyalpabetic substitution cipher). Dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigènere pada abad 16 (tahun 1586), algoritma baru dikenal luas 200 tahun kemudian [9].
Proses enkripsi dapat dihitung dengan persamaan berikut (Stalling, 2011) :

$$Ei = (Pi + Ki)\ mod\ 26 \quad (3)$$

dimana Ei , Pi dan Ki merupakan karakter hasil enkripsi, karakter pesan dan karakter kunci. Sedangkan proses dekripsi dapat menggunakan persamaan berikut :

$$D = (C-K)\ mod\ 26 \quad (4)$$

dengan Di adalah karakter hasil dekripsi, C adalah karakter cipher text atau sandi, Ki adalah karakter kunci.

2.3. Steganografi

Steganografi merupakan ilmu yang mempelajari tentang teknik menyembunyikan teks pada media lain yang telah ada sehingga teks tersebut dapat menyatu dengan media [10].

3. HASIL DAN PEMBAHASAN

3.1. Caesar Cipher

Dalam Caesar Cipher huruf akan disubstitusi ke dalam angka pada Tabel 1.

Tabel 1. Konversi Huruf

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

Contoh Kasus :
Plaintext : WISUDA
Key : 10
Perhitungan Caesar Cipher :
Huruf = WISUDA
Nomor Karakter Huruf W = 22
C = (22 + 10) mod 26
C = (32) mod 26
C = 6 --> Huruf G
Nomor Karakter Huruf I = 8
C = (8 + 10) mod 26
C = (18) mod 26
C = 18 --> Huruf S
Nomor Karakter Huruf S = 18
C = (18 + 10) mod 26
C = (28) mod 26
C = 2 --> Huruf C
Nomor Karakter Huruf U = 20

C = (20 + 10) mod 26
C = (30) mod 26
C = 4 --> Huruf E
Nomor Karakter Huruf D = 3
C = (3 + 10) mod 26
C = (13) mod 26
C = 13 --> Huruf N
Nomor Karakter Huruf A = 0
C = (0 + 10) mod 26
C = (10) mod 26
C = 10 --> Huruf K
Cipherteks Caesar = GSCENK

3.2. Vigenere Cipher

Hasil Cipherteks Caesar Cipher akan di proses pada algoritma Vigenere Cipher. Modifikasi yang dilakukan pada Vigenere Cipher ada 2 yakni :

a. Generate Kunci Otomatis, ketika jumlah kunci < jumlah plainteks menggunakan bilangan fibonnacci.
b. Perubahan ke dalam kode ASCII saat proses enkripsi.

Didapatkan ciphertext dari Caesar Cipher sebagai berikut :
Plainteks = GSCENK
Digunakan kunci inputan dari Vigenere Cipher :
Key = OKE
Kunci pada Vigenere berjumlah 3, sedangkan plaintext berjumlah 6, maka masih dibutuhkan 3 kunci lagi, kemudian dilakukan modifikasi dengan menggunakan bilangan fibonnacci dengan rumus :
Un = (Un – k + Un – k + m) mod 26
di mana :
Un = karakter kunci ke-n
k = panjang kunci masukan
m = 1 + (∑ (karakter_tiap_kunci) mod (k-1))
Proses Generate Key Fibbonaci =
k = 3 (jumlah key awal)
m = 1 + ((14+10+4) mod 2) = 1 + (28) mod 2 = 1 + 0 = 1
Lalu dicari kekurangan kunci pada kunci ke 4,5,6 :
Rumus dasar :
Un = (Un – k + Un – k + m) mod 26
U4=(U4-3+U4-3+1) mod 26=U1+U2 mod 26 = O+K mod 26 =14+10 mod 26=24=Y
U5=(U5-3+U5-3+1) mod 26 = U2+U3 mod 26 = K + E mod 26=10+4 mod 26=14=O
U6=(U6-3+U6-3+1) mod 26= U3+U4 mod 26= E+Y mod 26=4+24 mod 26=2 = C
Maka dihasilkan kunci tambahan yakni : Y,O,C
KEY GENERATE = OKEYOC
Berikutnya dimasukan ke dalam ASCII :
GSCENK = 71,83,67,69,78,75
OKEYOC = 79,75,69,89,79,67
Angka kunci dan plaintext dimasukan ke dalam tabel plain dan kunci, hasil merupakan hasil penjumlahan dari plain+kunci. Cipher didapatkan dengan me modulo 127 (sesuai jumlah karakter ASCII) angka dari hasil. Hasil ditunjukan pada Tabel 2.

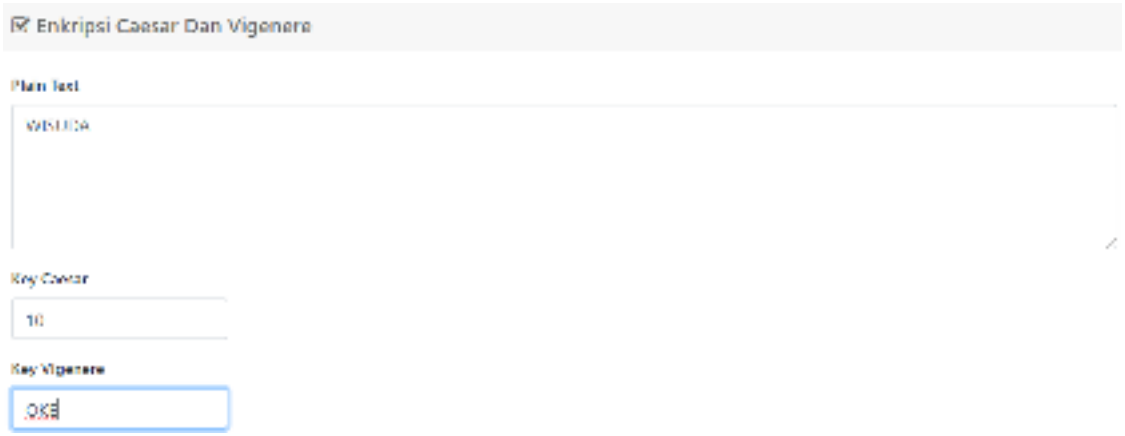
Tabel 2. Konversi ASCII Enkripsi

Plainteks	**71**	**83**	**67**	**69**	**78**	**75**
Kunci	79	75	69	89	79	67
Hasil	150	158	136	158	157	142
Cipher(desimal)	23	31	9	31	30	15

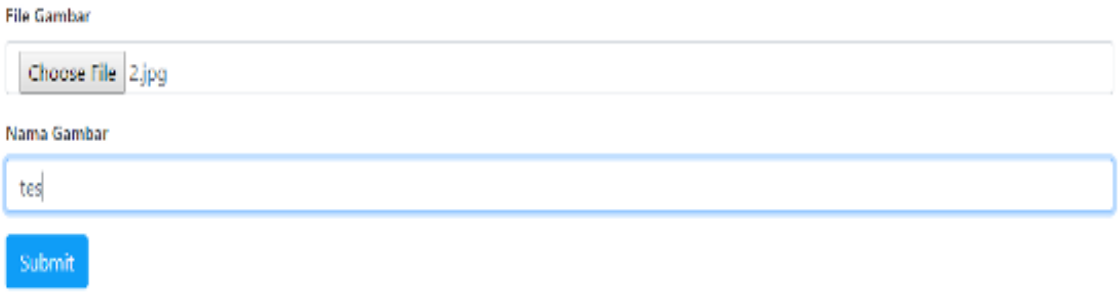
Ciphertext Akhir = 23,31,9,31,30,15. Kemudian di rubah ke dalam bentuk Hexa.
Hexa = 17, 1F,9,1F,1E,F.

3.3. Steganografi

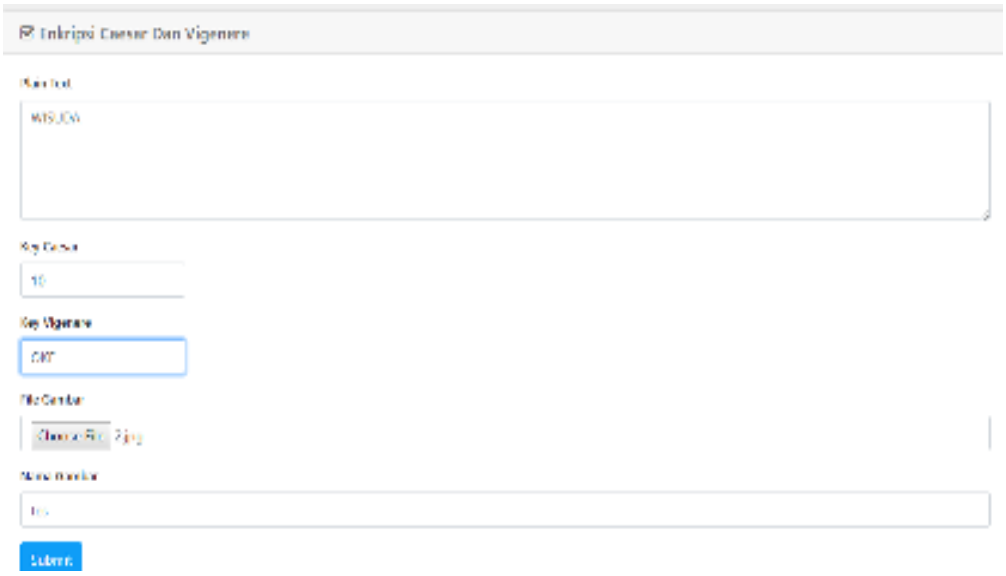
Proses steganografi yang dilakukan adalah dengan menyembunyikan kode cipherteks ke dalam gambar, dimana gambar tersebut akan disimpan dan dapat di dekripsikan untuk mengetahui isi pesan dengan memasukan kode Caesar dan kode hasil generate Vigenere Cipher. Adapun implementasi dari proses kriptografi steganografi ditunjukan pada Gambar 2, Gambar 3, Gambar 4.



Gambar 2. Proses Enkripsi.

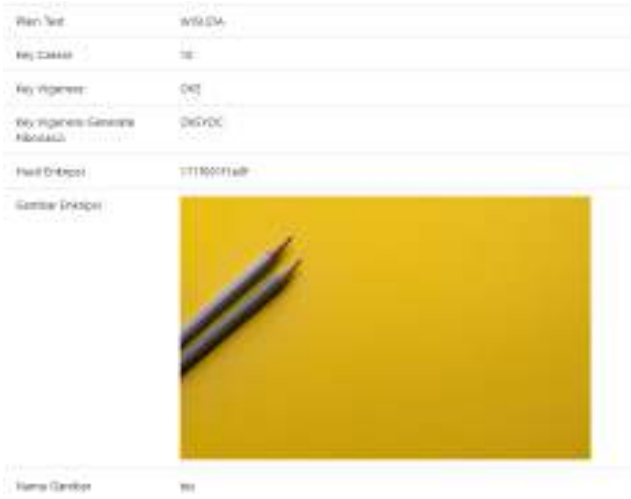


Gambar 3. Proses Input Gambar



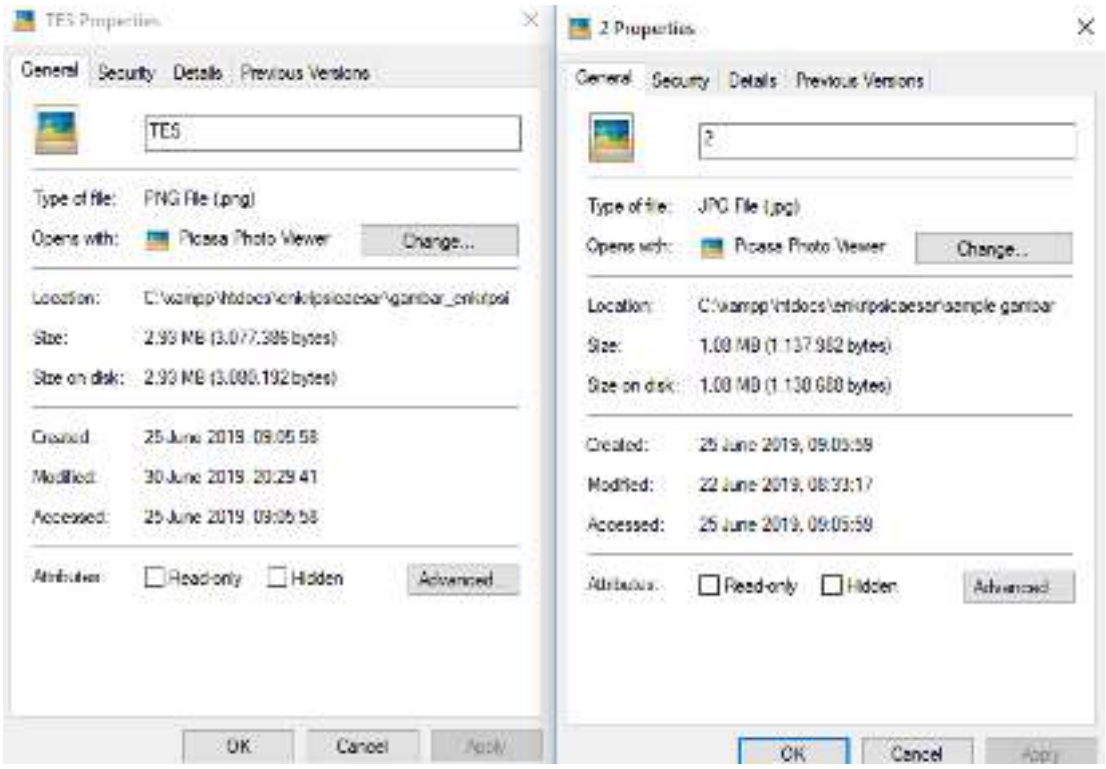
Gambar 4. Proses Input Keseluruhan

Sementara hasil steganografi ditunjukan pada Gambar 5.



Gambar 5. Hasil Kriptografi dan Steganografi

Ukuran gambar yang dihasilkan berbeda-beda sesuai dengan banyaknya teks yang disembunyikan. Adapun perbandingan dari hasil steganografi ditunjukan pada Gambar 6.



Gambar 6. Komparasi Ukuran Gambar

3.4. Dekripsi

3.4.1. Dekripsi Vigenere Cipher

Bilangan Cipher Hexa dirubah menjadi decimal

Hexa = 17, 1F,9,1F,1E,F

Cipher = 23,31,9,31,30,15

Angka kunci dan plaintext dimasukan ke dalam tabel cipher dan kunci, hasil merupakan hasil pengurangan dari cipher-kunci. Cipher didapatkan dengan me modulo 127 (sesuai jumlah karakter ASCII) angka dari hasil. Hasil ditunjukan pada Tabel 3.

Tabel 3. Proses Dekripsi Kode ASCII

Cipherteks	**23**	**31**	**9**	**31**	**30**	**15**
Kunci	79	75	69	89	79	67
Hasil	-56	-44	-60	-58	-49	-52
Plain(desimal)	71	83	67	69	78	75

Hasil = 71,83,67,69,78,75 dirubah kembali ke bentuk huruf = GSCENK. Lalu di proses ke dekripsi Algoritma Caesar Cipher.

3.4.2. Dekripsi Caesar Cipher

Huruf : GSCENK
Nomor Karakter Huruf G : 6
P = (6 - 10) mod 26
P = (-4) mod 26
P = 26 - 4

P = 22 --> W
Nomor Karakter Huruf S : 18
P = (18 - 10) mod 26
P = (8) mod 26
P = 8 --> I
Nomor Karakter Huruf C : 2
P = (2 - 10) mod 26
P = (-8) mod 26
P = 26 - 8
P = 18 --> S
Nomor Karakter Huruf E : 4
P = (4 - 10) mod 26
P = (-6) mod 26
P = 26 - 6
P = 20 --> U
Nomor Karakter Huruf N : 13
P = (13 - 10) mod 26
P = 3 mod 26
P = 3 --> D
Nomor Karakter Huruf K : 10
P = (10 - 10) mod 26
P = 0 mod 26
P = 0 --> A
Plaintext = WISUDA

4. KESIMPULAN

Adapun kesimpulan dari penelitian ini adalah :

a. Penerapan modifikasi pada algoritma Vigenere Cipher berhasil diterapkan pada proses enkripsi dan proses dekripsi. Metode Vigenere Cipher diharapkan menjadi lebih susah untuk dipecahkan setelah dilakukan modifikasi.
b. Penambahan proses steganografi dengan media gambar dapat menjadi nilai lebih, bahwa pesan dapat disembunyikan dibalik gambar sehingga proses pertukaran data dapat menjadi lebih aman.Kesimpulan harus mengindikasi secara jelas hasil-hasil yang diperoleh, kelebihan dan kekurangannya, serta kemungkinan pengembangan selanjutnya.

5. SARAN

Adapun saran dari penelitian ini adalah :

a. Dapat dilakukan modifikasi pada algoritma Caesar Cipher agar keamanan data menjadi lebih baik lagi, karena metode Vigenere sudah dilakukan modifikasi
b. Dapat ditambahkan jenis steganografi yang lain, bisa dapat berupa file multimedia lainnya.Saran-saran untuk untuk penelitian lebih lanjut untuk menutup kekurangan penelitian. Tidak memuat saran-saran diluar untuk penelitian lanjut.

DAFTAR PUSTAKA

[1] M. Ilayaraja, K. Shankar, and G. Devika, “A modified symmetric key cryptography method for secure data transmission,” *Int. J. Pure Appl. Math.*, vol. 116, no. 10, pp. 301–308, 2017.

[2] A. Rizal, D. S. B. Utomo, R. Rihartanto, M. E. Hiswati, and H. Haviluddin, "Modified key using multi-cycle key in vigenere cipher," *Int. J. Recent Technol. Eng.*, vol. 8, no. 2 Special Issue 11, pp. 2600–2606, 2019, doi: 10.35940/ijrte.B1313.0982S1119.

[3] D. A. Sewindu Putro, Sumbogo Wisnu Pamungkas, "Modification Of Two Playfair Algorithm And Caesar Chiper Al- gorithm Using City Post Code," *J. Mantik*, vol. 3, no. January, pp. 31–38, 2019.

[4] R. Latifah, S. N. Ambo, and S. I. Kurnia, "Modifikasi Algoritma Caesar Chiper dan Rail Fence untuk Peningkatan Keamanan Teks Alfanumerik dan Karakter Khusus," *Semin. Nas. Sains dan Teknol.*, no. 1-2 November, pp. 1–7, 2017.

[5] A. A. Permana, "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android," *J. Al-AZHAR Indones. SERI SAINS DAN Teknol.*, vol. 4, no. 3, p. 110, 2018, doi: 10.36722/sst.v4i3.280.

[6] D. Ariyus and Ardiansyah, "Optimization Substitution Cipher and Hidden Plaintext in Image Data Using LSB Method," *J. Phys. Conf. Ser.*, vol. 1201, no. 1, 2019, doi: 10.1088/1742-6596/1201/1/012033.

[7] K. Nahar and P. Chakraborty, "A Modified Version of Vigenere Cipher using 95×95 Table," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 5, pp. 1144–1148, 2020, doi: 10.35940/ijeat.e9941.069520.

[8] A. Subandi, M. S. Lydia, R. W. Sembiring, M. Zarlis, and S. Efendi, "Vigenere cipher algorithm modification by adopting RC6 key expansion and double encryption process," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 420, no. 1, pp. 3–9, 2018, doi: 10.1088/1757-899X/420/1/012119.

[9] Munir Rinaldi, *KRIPTOGRAFI*. Informatika, 2006.

[10] Kurniawan Yusuf, *KRIPTOGRAFI KEAMANAN INTERNET DAN JARINGAN TELEKOMUNIKASI*. Informatika, 2004.