MODIFIKASI KUNCI SIMETRIS CAESAR CIPHER DAN OTP MENGGUNAKAN ALGORITMA GENETIKA PADA STEGANOGRAFI

MODIFICATION OF SYMMETRICAL CAESAR CIPHER KEYS AND OTP USING GENETIC ALGORITHMS IN STEGANOGRAPHY

Dony Ariyus[1], Julia Kurniasih[2], Dwinda Etika Profesi[3]
[1,2,3]Magister Teknik Informatika, Universitas AMIKOM, Yogyakarta
e-mail: [1]dony.a@amikom.ac.id, [2]julia.k@students.amikom.ac.id,
[3]dwinda.20@students.amikom.a.c.id

Abstrak

Masalah keamanan data merupakan hal yang penting, karena data harus dijaga keamanan dan keutuhannya mulai dari proses pengiriman sampai diterima oleh pihak yang seharusnya. Kriptografi dan steganografi merupakan alternatif cara menjaga keamanan data. Informasi dapat diacak dan disembunyikan melalui media lain seperti media suara atau gambar, sehingga pesan yang ingin disampaikan terjaga kerahasiaannya. Penyandian/pengacakan informasi dapat dilakukan dengan menggunakan algoritma Caesar Cipher dan One Time Pad yang merupakan algoritma kriptografi kunci simetris. Kunci sebagai bagian penting dari algoritma kriptografi perlu dikembangkan/dimodifikasi untuk mendapatkan kekuatan keamanan informasi/teks yang akan disampaikan. Pada penelitian ini dilakukan modifikasi kunci algoritma kriptografi Caesar Cipher dan One Time Pad dengan menggunakan algoritma genetika yang merupakan salah satu jenis algoritma optimasi. Cipherteks (teks teracak) hasil algoritma kriptografi disisipkan pada media gambar untuk menghasilkan gambar sandi. Pengujian kekuatan cipherteks dilakukan dengan melihat frekuensi pengulangan karakternya. Dari hasil pengujian diketahui bahwa modifikasi kunci simetris dengan menggunakan algoritma genetika memberikan kekuatan keamanan yang cukup baik terhadap cipherteks, dilihat dari persentase pengulangan karakternya yang rendah.

Kata kunci—kriptografi, steganografi, Caesar Cipher, OTP, Algoritma Genetika

Abstract

Data security is important, because the data must be safeguarded and intact from the delivery process to being accepted by the party that should be. Cryptography and steganography are alternative ways to maintain data security. Information can be encrypted and also hidden through other media such as audio or image, so that the message to be conveyed is kept confidential. Encryption of information can be done using the Caesar Cipher and One Time Pad algorithms, which are symmetric key cryptography algorithms. The key as an important part of the cryptography algorithm needs to be developed/modified to get the security power of the information / text to be delivered. In this research, modifications of the key of Caesar Cipher and One Time Pad were carried out using a genetic algorithm which is one type of optimization algorithm. Ciphertext as a results of cryptography algorithms inserted in to the image to produce a stego-image. Testing the strength of ciphertext is done by looking at the repetition frequency of characters. From the results it is known that the symmetrical key modification using genetic algorithms provides a fairly good security power to the ciphertext, judging by the low percentage of character repetition.

Keywords—cryptography, steganography, Caesar Cipher, OTP, Genetic Algorithm

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi saat ini diikuti dengan meningkatnya transaksi data terutama di internet, karena proses pengiriman, penerimaan dan penyimpanan data dapat dilakukan dengan cepat dan mudah. Kondisi ini menyebabkan masalah keamanan data menjadi hal penting, karena data harus dijaga keamanan dan keutuhannya dimulai dari proses pengiriman sampai diterima oleh pihak yang seharusnya. Perkembangan ilmu pengetahuan menghasilkan bidang ilmu Kriptografi dan Steganografi yang dikenal sebagai ilmu penyandian dan penyembunyian informasi, yang dimaksudkan agar pesan yang disampaikan dapat terjaga kerahasiaan dan keamanannya [1]. Pesan yang ditulis menggunakan steganografi umumnya disisipkan pada sebuah media, diantaranya media suara atau media gambar.

Ada banyak algoritma kriptografi, diantaranya adalah Caesar Cipher dan One Time Pad. Caesar Cipher merupakan salah satu algoritma tertua dan merupakan salah satu jenis cipher substitusi, yang membentuk cipher dengan cara melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama. Kelemahan Caesar Cipher adalah pesan asli dapat diketahui dengan memanfaatkan metode brute force dan melihat prosentase frekuensi huruf yang paling sering muncul dalam kalimat [2]. Algoritma One Time Pad merupakan salah satu algoritma kriptografi simetris. One Time Pad berisi barisan karakter-karakter kunci yang dibangkitkan secara acak. One Time Pad (OTP) dalam dunia kriptografi dikenal sebagai metode penyandian yang sangat kuat sehingga tidak mudah dipecahkan [3].

Algoritma Genetika (AG) merupakan salah satu algoritma optimasi yang berdasarkan pada mekanisme seleksi alam dan genetika alami. Tujuannya adalah untuk mendapatkan populasi individu (kromosom) yang dapat beradaptasi dengan beberapa jenis lingkungan dan berperilaku secara alami. Kromosom dalam AG sering direpresentasikan dalam pengkodean biner. Secara umum AG dimulai dengan membuat populasi individu secara acak. Populasi baru akan dihasilkan dengan menerapkan operator reproduksi (crossover dan mutasi) pada populasi sebelumnya [4].

Berdasarkan kondisi diatas, pada penelitian ini dilakukan implementasi Algoritma Genetika pada kunci algoritma Caesar Cipher dan One Time Pad untuk menghasilkan sebuah algoritma kriptografi dengan sistematika yang sederhana namun tidak mudah dipecahkan yang diterapkan pada aplikasi steganografi..

Terdapat beberapa hasil penelitian terkait mengenai algoritma Caesar Cipher, One Time Pad dan penerapan Algoritma Genetika pada kriptografi dan steganografi. Jhingran dkk [4] mengusulkan pendekatan/metode baru untuk e-security dengan menggunakan konsep algoritma genetika dan deret pseudorandom untuk menghasilkan kunci enkripsi dan dekripsi data. Hasil penelitian menunjukkan bahwa algoritma yang diusulkan memberikan tingkat throughput yang lebih baik. Gunawan [5] melakukan kombinasi algoritma Caesar Cipher dan algoritma RSA untuk pengamanan file dokumen dan pesan teks. Kombinasi ini dilakukan untuk mengatasi kelemahan dari algoritma Caesar Cipher. Hasil penelitiannya menyatakan kombinasi Caesar Cipher dan algoritma RSA dapat meningkatkan sistem keamanan data dengan menggabungkan perhitungan struktur alphabetis dan pemfaktoran bilangan prima. Khoiruddin dan Khairina [6] melakukan analisis terhadap implementasi algoritma One Time Pad dan algoritma cipher transposisi untuk pengamanan teks. Hasil penelitiannya menyatakan bahwa pada pesan yang panjang implementasi algoritma cipher transposisi lebih baik dibandingkan dengan One Time Pad, dikarenakan algoritma cipher transposisi dapat melakukan pendekripsian dengan utuh, sementara One Time Pad mengalami hasil pendekripsian yang pecah. Nazeer dkk [7] mengusulkan algoritma yang disebut dengan Genetic Crypto. Pengembangan Genetic Crypto menggunakan Algoritma Genetika untuk meningkatkan kekuatan kunci yang pada akhirnya menjadikan keseluruhan algoritma lebih baik. Genetic Crypto terbagi menjadi tiga proses yaitu pembangkitan kunci, data difusi dan enkripsi data. Hasil penelitian menunjukkan Genetic Crypto memiliki hasil yang lebih baik dalam hal kekuatan kunci tetapi masih lemah dalam hal komputasi (kurang efisien). Srikanth dkk [8] mengimplementasikan operasi algoritma genetika untuk proses enkripsi dan dekripsi kriptografi. Hasil penelitiannya menyatakan operasi Algoritma Genetika dapat digunakan untuk memberikan keamanan pada data dalam suatu file. Gangeshawar dan Attri [9] mengusulkan teknik kombinasi algoritma genetika yang diimplementasikan pada gambar untuk pengoptimalan dalam Steganografi. Namun teknik yang diusulkannya juga meningkatkan waktu kompleksitas dari algoritma baru. Gaidhani dkk [10] mengembangkan steganografi gambar dengan

menggunakan algoritma genetika untuk menyembunyikan pesan. Pada penelitian ini faktor yang diperhatikan adalah perubahan gambar yang dapat terjadi akibat penyisipan pesan, bisa dalam bentuk peningkatan/penurunan ukuran gambar, penurunan intensitas piksel gambar, atau perubahan lain yang mudah terlihat oleh mata manusia. Indikatornya menggunakan parameter PSNR yang menghitung sinyal puncak untuk rasio noise antara dua gambar, jika PSNR rasio tinggi maka kualitas gambar baik. Dasguptaa dkk [11] mengusulkan skema steganografi video baru untuk penyembunyian informasi yang efisien dan efektif. Skema berbasis 3-3-2 LSB ditingkatkan menggunakan Algoritma Genetika untuk mendapatkan imperceptibilitas optimal dari data tersembunyi. Tes anti-steganalisis digunakan untuk memeriksa kesesuaian frame terhadap frame asli. Hasil eksperimen menunjukkan peningkatan substansial dalam nilai Peak Signal Noise Ratio (PSNR) dan Image Fidelity (IF) setelah dilakukan optimasi.

Berbeda dengan penelitian sebelumnya, pada penelitian ini algoritma genetika diimplementasikan pada kunci simetris yang akan digunakan pada kombinasi algoritma Caesar Cipher dan One Time Pad, untuk tujuan memberikan kekuatan pada hasil enkripsi teks (cipherteks) sehingga tidak mudah dibaca oleh pihak yang tidak berhak.

2. METODE PENELITIAN

Penelitian ini menggunakan algoritma kriptografi Caesar Cipher, One Time Pad (OTP) dan Algoritma Genetika dalam pengembangan modifikasi kunci simetris yang akan diimplementasikan pada aplikasi steganografi gambar. Perubahan plainteks menjadi cipherteks dan sebaliknya dilakukan dengan metode konversi hexadecimal menggunakan tabel ASCII.

2.1 Algoritma Caesar Cipher

Algoritma Caesar Cipher merupakan algoritma kunci simteris (kriptografi klasik) kelompok cipher substitusi dengan konsep dasarnya adalah setiap unit plainteks diganti dengan satu unit cipherteks. Satu unit dapat berupa satu huruf, pasangan huruf atau kelompok lebih dari dua huruf. Caesar Cipher disebut juga sandi geser sebab huruf-huruf dalam plainteks digantikan oleh huruf lainnya dalam posisi tertentu dalam susunan alfabet.

2. 2 One Time Pad (OTP)

Algoritma One Time Pad (OTP) adalah stream cipher yang melakukan enkripsi dan dekripsi satu karakter setiap kali. Algoritma ini merupakan perbaikan dari Vernam Cipher untuk menghasilkan keamanan yang lebih baik. Cipher ini termasuk ke dalam kelompok algoritma kriptografi simetri. One Time Pad berisi barisan karakter-karakter kunci yang dibangkitkan secara acak. Satu pad hanya digunakan sekali (one time) saja untuk mengenkripsi pesan, setelah itu pad yang telah digunakan dihancurkan supaya tidak dipakai kembali untuk mengenkripsi pesan yang lain, dan untuk mengenkripsi pesan lain dilakukan proses pengacakan lagi. Pada One Time Pad, jumlah kunci sama panjangnya dengan jumlah plainteks [3].

2.3 Algoritma Genetika (AG)

Algoritma Genetika (AG) merupakan salah satu algoritma optimasi yang berdasarkan pada mekanisme seleksi alam dan genetika alami. Tujuannya adalah untuk mendapatkan populasi individu (kromosom) yang dapat beradaptasi dengan beberapa jenis lingkungan dan berperilaku secara alami. Kromosom dalam AG sering direpresentasikan dalam pengkodean biner. Secara umum AG dimulai dengan membuat populasi individu secara acak. Populasi baru akan dihasilkan dengan menerapkan operator reproduksi pada populasi sebelumnya. Algoritma genetika menggunakan dua operator reproduksi, yaitu crossover dan mutasi. Untuk menggunakan operator crossover, kromosom induk dipasangkan bersama. Ada beberapa jenis operator crossover yaitu one-point crossover, two-point crossover dan multi-point crossover, dan pada penelitian ini digunakan jenis operator one-point crossover. Hasil dari proses crossover akan mengalami proses mutasi. Standar operator mutasi untuk string biner adalah cara inversi bit ‘0’ bermutasi menjadi ‘1’ dan sebaliknya [4].

3. HASIL DAN PEMBAHASAN

Pada penelitian ini operasi crossover pada algoritma genetika menggunakan jenis one-point crossover dengan konsep kerja sebagai berikut :

a. Menentukan crossover point (gen tertentu)
b. Kromosom baru pertama berisi gen pertama sampai gen crossover point dari kromosom induk kedua digabung dengan gen dari crossover point sampai gen terakhir dari kromosom induk pertama.
c. Kromosom baru kedua berisi gen pertama sampai gen crossover point dari kromosom induk pertama digabung dengan gen dari crossover point sampai gen terakhir dari kromosom induk kedua.

Skema proses enkripsi teks disajikan pada Gambar 1. Ilustrasi proses enkripsi teks menggunakan plainteks dan konversinya dalam bentuk hexadesimal disajikan pada Tabel 1 dan kunci yang digunakan disajikan pada Tabel 2.

Tabel 1. Plainteks dan Konversi Hexadesimalnya

S	**A**	**Y**	**A**		**M**	**A**	**U**		**B**	**E**	**L**	**A**	**J**	**A**	**R**
53	41	59	41	20	4D	41	55	20	42	45	4C	41	4A	41	52

Tabel 2. Kunci Enkripsi

K	**R**	**I**	**P**	**T**	**O**	**G**	**R**	**A**	**F**	**I**
4B	52	49	50	54	4F	47	52	41	46	49

Kunci pada Tabel 2 dimodifikasi dengan menggunakan algoritma genetika melalui operasi crossover dan mutasi. Untuk melakukan modifikasi, kunci dalam bentuk hexadesimal dikonversikan ke dalam bentuk biner dan hasilnya disajikan pada Tabel 3.

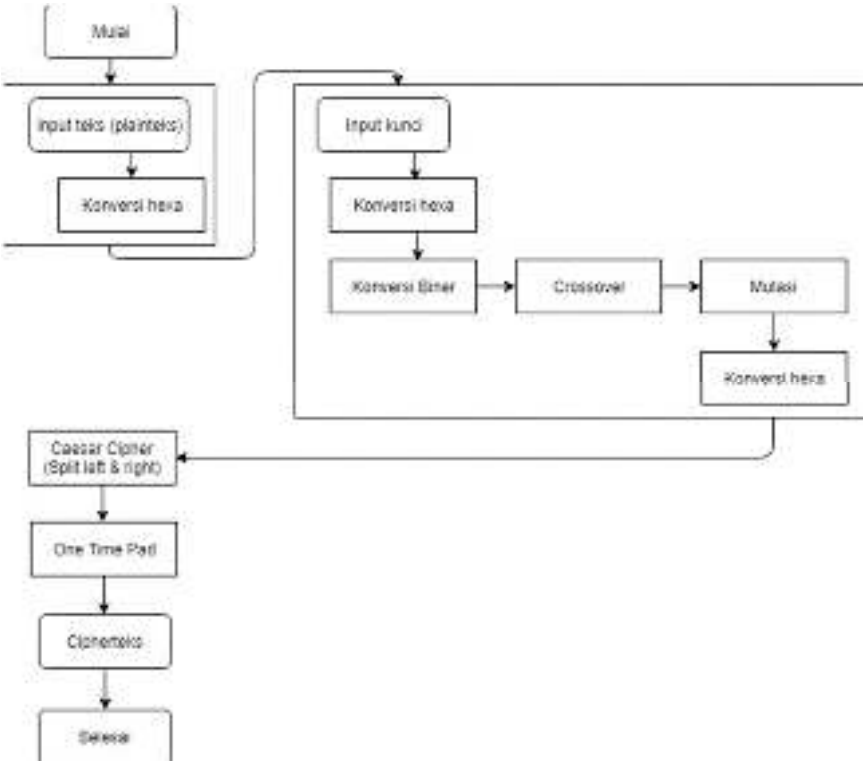
Tabel 3. Konversi Kunci ke Bentuk Biner

0100	0101	0100	0101	0101	0100	0100	0101	0100	0100	0100	0000
1011	0010	1001	0000	0100	1111	0111	0010	0001	0110	1001	0000

Kunci biner mengalami operasi crossover dengan metode one point crossover dan diperoleh hasil seperti terlihat pada Tabel 4. Hasil operasi crossover akan mengalami mutasi dan dikonversikan kembali ke dalam bentuk hexadesimal seperti terlihat pada Tabel 5.

Tabel 4. Operasi Crossover

0101	0100	0101	0100	0100	0101	0101	0100	0100	0100	0000
1011	0010	1001	0000	0100	1111	0111	0010	0001	0110	1001

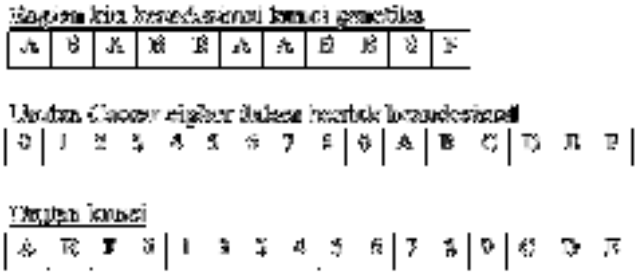


Gambar 1. Skema proses enkripsi

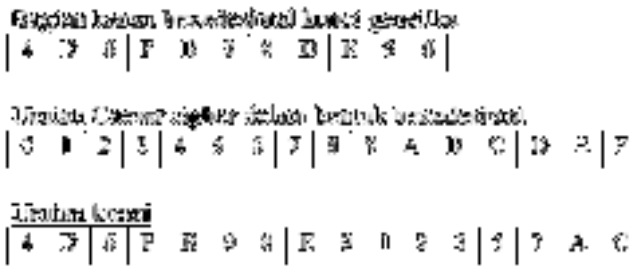
Tabel 5. Operasi Mutasi

1010 0100	1011 1101	1010 0110	1011 1111	1011 1011	1010 0000	1010 1000	1011 1101	1011 1110	1011 1001	1111 0110
A4	BD	A6	BF	BB	A0	A8	BD	BE	B9	F6

Kunci hasil modifikasi dengan menggunakan algoritma genetika yang dinamakan sebagai kunci genetika, selanjutnya akan digunakan untuk proses enkripsi teks dengan menggunakan algoritma Caesar Cipher dan One Time Pad. Untuk proses pada Caesar Cipher, kunci genetika dibagi menjadi dua bagian, yaitu kunci sisi kiri dan sisi kanan. Urutan kunci Caesar Cipher sisi kiri dan kanan diperlihatkan pada Gambar 2 dan Gambar 3 secara berurutan.



Gambar 2. Urutan kunci Caesar Cipher sisi kiri



Gambar 3. Urutan kunci Caesar Cipher sisi kanan

Proses enkripsi plainteks pada Tabel 1 dengan kunci Caesar Cipher sisi kiri dan kanan pada Gambar 2 dan Gambar 3 menghasilkan teks enkripsi seperti terlihat pada Tabel 6.

Tabel 6. Plainteks Caesar Cipher

2F	1D	21	1D	F4	17	1D	20	F4	16	10	15	1D	12	1D	26

Plainteks hasil Caesar Cipher selanjutnya akan mengalami proses enkripsi dengan menggunakan algoritma One Time Pad. Dengan menggunakan kunci genetika pada Tabel 5 dan urutan acak hexadesimal seperti terlihat pada Tabel 7, maka plainteks hasil dari Caesar Cipher akan dienkripsi untuk menghasilkan cipherteks seperti terlihat pada Tabel 8.

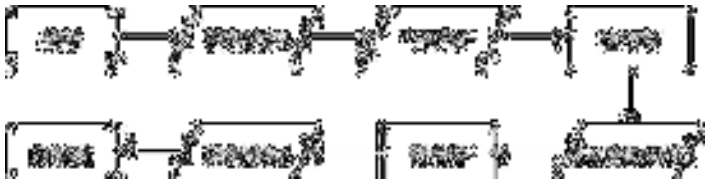
Tabel 7. Skema Urutan Acak Hexadesimal Untuk Algoritma One Time Pad

Normal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Acak	A	4	B	D	6	F	0	8	E	9	1	2	3	5	7	C
Desimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Tabel 8. Cipherteks Hasil Algoritma One Time Pad (dalam hexadesimal)

20	30	27	3E	8D	16	11	59	89	35	C1	3B	16	37	18	59

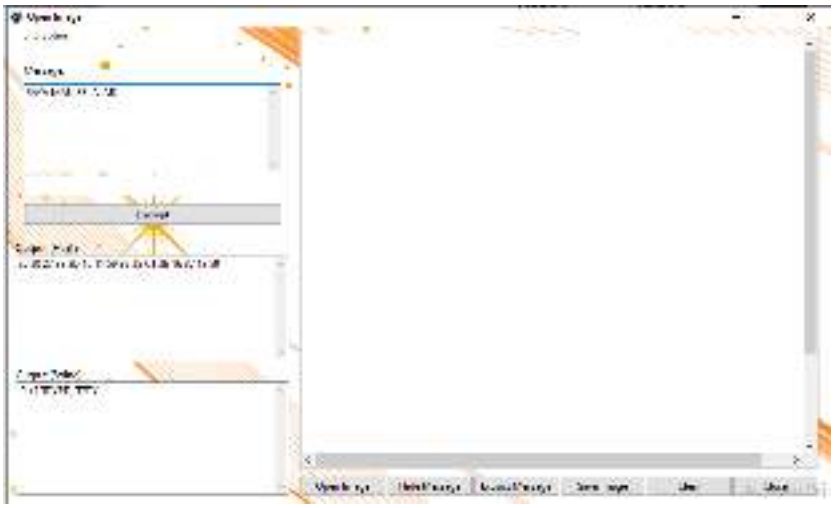
Dalam implementasinya pada steganografi yang diperlihatkan pada Gambar 4, cipherteks ini diubah ke dalam bentuk karakter-karakter yang membentuk string dengan menggunakan Tabel ASCII. String ini merupakan pesan rahasia yang akan disisipkan pada media gambar untuk proses encode yang akan menghasilkan sebuah file gambar sandi. Untuk mengambil cipherteks dari gambar sandi dilakukan proses decode. Dan untuk mengetahui pesan asli (plainteks) dari pesan yang disandikan/diacak (cipherteks) maka dilakukan proses dekripsi seperti terlihat pada Gambar 5.



Gambar 4. Alur proses encode dan decode pada steganografi gambar

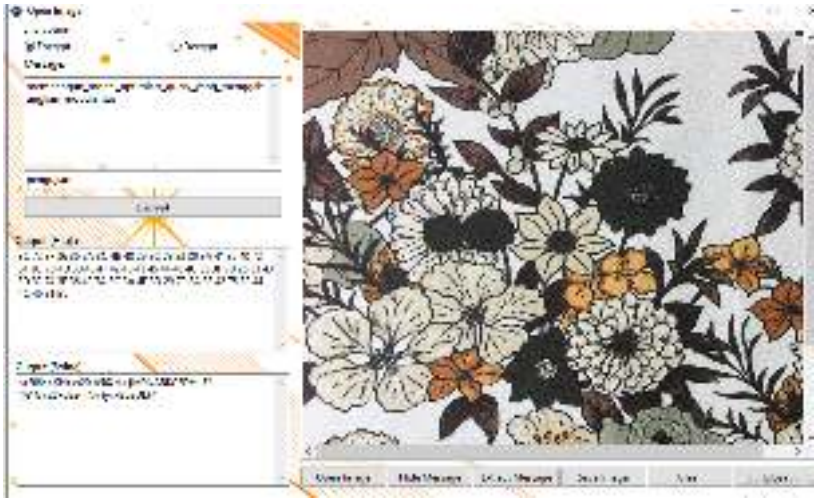
Gambar 5. Skema proses dekripsi

Pengujian pada penelitian ini dilakukan dengan menggunakan aplikasi kriptografi dan steganografi yang dapat dilihat pada Gambar 6.



Gambar 6. Aplikasi pengujian

Proses penyisipan cipherteks ke dalam media gambar diperlihatkan pada Gambar 7. Tampilan gambar awal dan gambar sandi (gambar yang disisipi pesan/cipherteks) diperlihatkan pada Gambar 8.



Gambar 7. Proses penyisipan teks pada gambar

Gambar awal

Gambar sandi

Gambar 8. Tampilan gambar awal dan gambar sandi

Pengujian modifikasi kunci simetris dengan menggunakan algoritma genetika ini dilakukan dengan melihat frekuensi pengulangan karakter yang muncul pada cipherteks yang dihasilkan. Semakin sering sebuah karakter muncul pada cipherteks maka kemungkinan pesan yang disembunyikan akan mudah dibaca/diketahui oleh pihak yang tidak berhak. Hasil pengujian pada penelitian ini dapat dilihat pada Tabel 9 dengan teks kunci yang digunakan adalah ‘pengujian’. Pemisah antar kata dalam plainteks pada penelitian ini menggunakan simbol underscore (_).

Tabel 9. Hasil Pengujian Modifikasi Kunci Simetris

Plainteks	**Cipherteks (hexadesimal)**	**Ciperteks (karakter)**	**Frekuensi Pengulangan Karakter pada Cipherteks**
membangun_model_optimizer_query_yang_menggabungkan_modularitas	3C 72 3F 36 36 7A 3C 4B 48 29 3C 78 32 30 3A 41 35 40 72 34 3C 7B 4D 30 4E 41 42 4B 43 45 44 48 4C 35 3F 7B 25 31 43 3D 32 74 3E 36 42 7A 3C 3A	<r?66z<KH)<x20:A5@r4<{M0NABKCEDHL5?{%1C=2t>6Bz<:N=)y:>Bu2DLF1	- Karakter yang paling banyak muncul adalah ‘<’ sebanyak 5 kali. - Jumlah total karakter adalah 61 karakter.

	4E 3D 29 79 3A 3E 42 75 32 44 4C 46 31 B5 9F 9B		- Persentase kemunculan karakter '<' = 5/61 = 0,08%.
UNTUK_MENGETAHUI_EFEKTIFITAS_QUERY_HASIL_PENGEMBANGAN	2E 6F 22 20 1D 41 1A 1B 58 12 1E 40 1E 14 22 6D 25 1B 54 1E 1B 40 1C 12 1B 43 12 22 3A 21 2E 62 20 27 28 6C 12 22 5C 1F 29 41 13 19 14 64 1A 14 5E 1D 12 66 18 9D 9C	.o" AX-@-"m%T-@C":!.b '(l"\-)Ad^f	- Karakter yang paling banyak muncul adalah '' sebanyak 20 kali. - Jumlah total karakter adalah 51 karakter. - Persentase kemunculan karakter '' = 20/51 = 0,39%.
Menentukan_jumlah_DATA_dan_sumber_DATA_yang_digunakan	1C 72 38 30 3F B3 47 3A 4E 3D 29 7C 43 3D 3A 70 3D 26 52 11 26 66 2A 3E 36 7A 25 42 73 3C 35 72 40 2F 10 60 24 13 3A 44 31 7F 37 2F 30 7D 3C 4B 48 31 3B 76 38 9D 9C	r80??G:N=)|C=:p=&R&f*>6z% Bs<5r@/`$:D1 7/0}<KH1;v8	- Karakter yang paling banyak muncul adalah '' sebanyak 5 kali. - Jumlah total karakter adalah 53 karakter. - Persentase kemunculan karakter '' = 5/53 = 0,09%.
rumus_untuk_menghitung_luas_segitiga=1/2(alas*tinggi)	45 B2 3F 40 45 41 47 35 72 4E 3B 48 3F 30 3F 7B 3D 3F 72 4E 3D 74 2A 38 42 70 40 26 76 3E 32 7B 42 37 34 70 0A 03 8A 05 F3 76 31 35 45 A9 44 3F 48 32 32 7B FC 9D 9C	E??@EAG5rN; H?0?{=?rN=t*8 Bp@&v>2{B74 p ??v15E?D?H22 {	- Karakter yang paling banyak muncul adalah '?' sebanyak 9 kali. - Jumlah total karakter adalah 53 karakter. - Persentase kemunculan karakter '?' = 9/53 = 0,17%.
Kulit_Jeruk_Bisa_Digunakan_Untuk_Membuat_Permen_Dan_Teh_Jeruk._Bahkan_Di_Jamaika,_Kulit_Jeruk_Digunakan_Untuk_Menghilangkan_Minyak_Dan_Lemak	1B B2 31 37 40 41 1F 3B 70 4E 3B 48 10 37 45 70 25 17 4C 32 4E 7F 3E 3C 36 7A 25 2B 48 46 4E 7D 2A 1D 32 78 33 4B 4E 46 29 41 33 46 39 74 31 26 52 31 3D 48 22 30 37 41 1F 3B 70 4E 3B AF 2A 16 36 7C 38 33 48 29 16 7B 2A 1B 36 78 32 3F 49 31 FF 48 19 40 3A 7D 44 26 5D 3E 45 B2 39 2F 10 7D 3C 4B 48 31 3B 76 38 2F 22 7A 44 4B 49 29 1C 72 38 33 37 7D 36 33 48 32 3B 76 38 2F 19 7D 31 4F 4E 3B 29 60 3E 39 28 65 37 31 4E 3B 9C 8C	?17@A-;pN;H7Ep%L2 N ><6z%+HF N}*2x3KNF)A 3F9t1&R1=H"0 7A-;pN;?*6|83H){* 6x2?I1?H@:}D &]>E?9/}<KH1 ;v8/"zDKI)r837 }63H2;v8/}1ON ;)`>9(e71N;	- Karakter yang paling banyak muncul adalah '' sebanyak 12 kali. - Jumlah total karakter adalah 140 karakter. - Persentase kemunculan karakter '' = 12/140 = 0,09%.

4. KESIMPULAN

Dari hasil pengujian diketahui rata-rata pengulangan karakter pada cipherteks hasil algoritma kriptografi Caesar Cipher dan OTP dengan modifikasi kunci simetris menggunakan algoritma genetika adalah sebesar 0,16%. Angka ini menunjukkan kondisi yang masih dapat diterima dari segi kekuatan enkripsi teks yang diimplementasikan pada steganografi. Sehingga dapat disimpulkan

bahwa modifikasi kunci simetris dengan menggunakan algoritma genetika dapat memberikan kekuatan enkripsi teks (cipherteks) pada kriptografi dan steganografi.

5. SARAN

Untuk lebih meningkatkan kekuatan enkripsi teks pada aplikasi kriptografi dan steganografi, perlu dilakukan penelitian dengan kombinasi dua atau lebih kunci dengan mengimplementasikan algoritma genetika pada kombinasi kuncinya.

DAFTAR PUSTAKA

[1] Dony Ariyus, 2008, *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*, Andi Offset, Yogyakarta.

[2] Rachmawati, D., dan Candra, A., 2015, Implementasi Kombinasi Caesar Cipher dan Affine Cipher Untuk Keamanan Data Teks, *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, Vol. 1, No. 2.

[3] Agustanti, S. P., 2010, Pengamanan Kunci Enkripsi One-Time Pad (OTP) Menggunakan Enkripsi RSA, *Jurnal Media Teknik*, vol. 7, no. 1, pp. 95-100.

[4] Jhingran, R., Thada, V., and Dhaka, S., 2015, A Study on Cryptography using Genetic Algorithm, *International Journal of Computer Applications* (0975 – 8887), vol. 118, no.20.

[5] Gunawan, I., 2018, Kombinasi Algoritma Caesar Cipher dan Algoritma RSA Untuk Pengamanan File Dokumen dan Pesan Teks, *InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan)* e-ISSN : 2540-7600, vol. 2, no. 2.

[6] Khoiruddin, M., dan Khairina, N., 2017, Analisis Algoritma One Time Pad Dengan Algoritma Cipher Transposisi Sebagai Pengamanan Pesan Teks, *Jurnal & Penelitian Teknik Informatika*, vol. 1, no. 2.

[7] Nazeer, M. I., Mallah, G. A., Shaikh, N. A., Bhatra, R., Memon, R. A., and Mangrio, M. I., 2018, Implication of Genetic Algorithm in Cryptography to Enhance Security, *(IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 9, no. 6.

[8] Srikanth, P., Mehta, A., Yadav, N., Singh, S., and Singhal, S., 2017, Encryption and Decryption Using Genetic Algorithm Operations and Pseudorandom Number, *IJCSN - International Journal of Computer Science and Network*, vol. 6, issue 3.

[9] Gangeshawar, and Attri, J., 2015, Optimizing Image Steganography using Genetic Algorithm, *International Journal of Engineering Trends and Technology (IJETT)*, vol. 24, number 1.

[10] Gaidhani, C. R., Deshpande, V. M., and Bora, V. N., 2014, Image Steganography for Message Hiding Using Genetic Algorithm, *International Journal of Computer Science and Engineering (JCSE)*, vol. 2, issue 3.

[11] Dasguptaa, K., Mondalb, J. K., and Dutta, P., 2013, Optimized Video Steganography using Genetic Algorithm (GA), *International Conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA), Procedia Technology* 10 (2013) 131 – 137.