TEKNIK KRIPTOGRAFI UNTUK MENJAGA KEAMANAN INFORMASI DENGAN MEMANFAATKAN CITRA DIGITAL SEBAGAI KUNCI

[1]Muhamad Arfiq Khoiron (1110651034),
[2]Ari Eko Wardoyo, S.T., M.Kom, [3]Bakhtiyar Hadi Prakoso, S.Kom
Program Studi Teknik Informatika
Fakultas Teknik
Universitas Muhammadiyah Jember
Email : mu.apieq@gmail.com

Abstrak

Keamanan sebuah informasi kini menjadi hal yang sangat mutlak untuk menjaga agar informasi tersampaikan pada pihak yang tepat. Kriptografi merupakan ilmu untuk menyamarkan suatu pesan demi menjaga kerahasiaannya. Suatu pesan (*plaintext*) harus melalui proses enkripsi terlebih dulu menjadi bentuk yang tidak berarti (*ciphertext*) sebelum dikirimkan ke penerima yang berhak. Hanya pihak yang berhak lah yang dapat melakukan proses dekripsi, yaitu mengubah kembali *ciphertext* menjadi *plaintext* memakai suatu kunci rahasia.

Desain sebuah algoritma untuk kriptografi telah banyak dibuat oleh kriptografer, dari algoritma yang bersifat klasik maupun modern. Pada umumnya algoritma yang dibuat terkuncikan oleh sebuah teks rahasia. Pada kesempatan ini penulis akan mengembangkan algoritma *caesar cipher* yang mana kunci untuk proses enkripsi dan dekripsi adalah sebuah gambar yang sama dengan memanfaatkan citra digital. Dalam sebuah citra berwarna, setiap piksel memiliki nilai intensitas warna *red, green, blue* yang dapat diubah dalam sebuah data teks. Nilai intensitas warna inilah yang akan menentukan banyaknya pergeseran huruf untuk proses enkripsi dan deskripsi yang berbeda pada tiap karakter.

Hasil yang didapatkan adalah sebuah pengembangan dari algoritma *caesar cipher* yang menggunakan citra digital sebagai kunci untuk proses enkripsi dan deskripsi. Dengan demikian informasi dalam bentuk *chiphertext* akan lebih sulit dipecahkan oleh penerima yang tidak berhak.

Kata kunci : *Kriptografi, Citra Digital, Caesar Cipher*

1. Latar Belakang

Informasi kini menjadi sebuah kunci utama dalam segala hal. Pada masa lampau, penguasa dunia adalah dia yang memiliki pasukan yang banyak. Adanya teknologi membuat pasukan yang banyak tak lagi menguasai dunia. Pada era sekarang ini penguasa dunia adalah dia yang menguasai informasi. Barang siapa yang dapat menguasai semua informasi, maka ia dapat menguasai dunia.

Dikarenakan pentingnya informasi, berbagai cara digunakan untuk mengamankan informasi yang dimiliki agar tidak jatuh pada pihak yang tidak memiliki hak untuk mengetahui informasi tersebut. Informasi dalam bentuk teks dapat disandikan menjadi informasi lain yang tidak jelas dengan teknik kriptografi. Kriptografi merupakan ilmu yang mempelajari teknik matematis yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta autentifikasi data (Wahana Komputer, 2010).

Salah satu algoritma kriptografi klasik adalah *Caesar cipher*, yang mana algoritma ini bekerja dengan menggeser tiga abjad ke kanan untuk setiap karakter pada deret huruf alfabet. Algoritma ini digunakan pada zaman romawi untuk menyandikan pesan yang akan disampaikan kepada sekutunya.

Semakin canggih teknologi informasi, semakin rentan keamanan sebuah informasi, oleh karenanya diperlukan penemuan atau perbaikan algoritma yang ada. Pada algoritma *caesar cipher*, pergeseran huruf dilakukan dengan jumlah pergeseran yang sama pada setiap karakter. Pada tugas akhir ini penulis akan mengembangkan algoritma caesar cipher dengan pergeseran yang berbeda-beda pada setiap karakter yang diinputkan dengan memanfaatkan nilai intensitas warna pada citra digital.

Setiap orang yang pernah menggunakan sandi rahasia berupa teks pada teknik kriptografi, kemungkinan besar mereka pernah mengalami lupa dengan sandi yang dibuat, sehingga ciphertext tidak dapat diterjemahkan. Dari kasus ini penulis akan membuat sebuah sandi berupa gambar digital sebagai sandi dalam proses enkripsi dan dekripsi. Dengan demikian, pengguna akan lebih mudah mengingat sandi yang digunakan dalam bentuk gambar.

Setiap piksel pada citra RBG 24-bit memiliki nilai intensitas *red, green, blue* yang masing-masing berkisar dari 0 s/d 255, nilai inilah yang akan dijadikan nilai pergeseran pada masing-masing karakter dalam teks yang akan dienkripsi. Citra digital yang telah diinputkan akan diubah resolusinya menjadi 100 x 100 piksel untuk mendapatkan pola pergeseran yang lebih beragam. Nilai intensitas warna akan dibaca dan akan dideretkan untuk setiap piksel pada citra digital dalam bentuk data teks.

Untuk memberikan keamanan yang lebih kuat, pengguna dapat menentukan index awal pada data teks intensitas warna yang telah dibuat. Dengan demikian, untuk dapat mendekripsikan kembali *ciphertext*, pengguna harus memiliki citra digital yang dipakai untuk enkripsi dan index yang ditentukan saat proses enkripsi.

Berdasarkan paparan di atas maka algoritma *caesar cipher* dapat dikembangkan dengan pergeseran yang berbeda pada setiap karakternya. Sehingga tugas akhir ini berjudul **Teknik Kriptografi untuk Menjaga Keamanan Informasi dengan Memanfaatkan Citra Digital sebagai Kunci.**

2. Tinjauan Pustaka

a. Kriptografi

Cikal bakal dari enkripsi dan dekripsi adalah berasal dari ilmu kriptografi. Kriptografi adalah ilmu yang mempelajari teknik matematis yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta *autentifikasi* data. Kriptografi tidak berarti hanya memberikan keamanan informasi saja, namun lebih ke arah teknik-tekniknya

b. Enkripsi dan Dekripsi

Proses utama dalam suatu algoritma kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses mengamankan suatu informasi dngan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Keuntungan dari enkripsi adalah kode asli kita tidak dapat dibaca oleh orang lain. Enkripsi mengubah sebuah *plaintext* ke dalam bentuk *ciphertext.*

Dekripsi adalah proses mengembalikan suatu informasi dengan cara tertentu dan sesuai dengan algoritma enkripsi yang dipakai. Dekripsi merupakan proses kebalikan dari proses enkripsi, mengubah *ciphertext* kembali ke dalam bentuk *plaintext*.

c. Algoritma Kriptografi Klasik

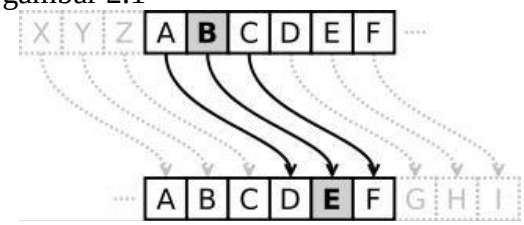
Kriptografi mempunyai sejarah yang panjang, mulai dari kriptografi Caesar yang berkembang pada zaman sebelum Masehi sampai kriptografi modern yang digunakan dalam komunikasi antar komputer di abad 20. Ada dua teknik yang paling dasar, yaitu: teknik subtitusi dan teknik transposisi.

d. Metode Kriptografi Caesar Cipher atau Sift Chiper

Metode kriptografi *shift chiper* mula-mula digunakan oleh kaisar Romawi, Julius Caesar untuk menyandikan pesan yang dikirim kepada para gubernurnya, sehingga metode ini disebut *caesar chiper*. Dalam kriptografi, *shift chiper*

dikenal dengan beberapa nama seperti: *code caesar* atau c*aesar shift*.

Shift chiper merupakan teknik enkripsi yang paling sederhana dan banyak digunakan. *Chiper* ini berjenis c*hiper* substitusi, dimana setiap huruf pada *plaintext* digantikan dengan huruf lain yang tetap pada posisi alfabet. Misalnya diketahui bahwa pergeseran = 3, maka huruf A akan digantikan oleh huruf D, huruf B menjadi huruf E, dan seterusnya. Sebagai ilustrasinya dapat dilihat pada gambar 2.1



Gambar 2.1 Ilustrasi metode kriptografi Shift Chiper atau Caesar Cipher

e. Citra Digital

Citra atau gambar dapat didefinisikan sebagai sebuah fungsi dua dimensi, f(x,y), dimana x dan y adalah koordinat bidang datar, dan harga fungsi f di setiap pasangan koordinat (x,y) disebut intensitas atau level keabuan (*grey level*) dari gambar di titik itu.

Jika x,y dan f semuanya berhingga (*finite*), dan nilainya diskrit, maka gambarnya disebut citra digital (gambar digital).

RGB Image terkadang diaggap sebagai *truecolor image. RGB image* disimpan dalam MATLAB sebagai array nx3 yang mendefinisikan komponen warna *red, green* dan *blue* dari masing-masing piksel. Warna dari tiap piksel ditentukan dengan kombinasi intensitas *red, green* dan *blue* yang disimpan di tiap saluran warna di lokasi piksel tertentu. Format file grafik menyimpan *RGB image* sebaga 24-bit image, di mana komponen *red, green* dan *blue* masing-masing 8-bit. Suatu piksel yang mempunyai komonen warna (0,0,0) berwarna hitam, sedangkan piksel dengan komponen warna (255,255,255) berwarna putih. Tiga komponen warna untuk masing-masing piksel disimpan sebagai array tiga dimensi.

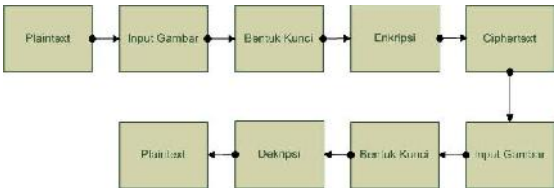
Dasar dari pengolahan citra adalah pengolahan warna RGB pada posisi tertentu. Dalam pengolahan citra warna dipresentasikan dengan nilai hexadesimal dari 0x00000000 sampai 0x00ffffff. Warna hitam adalah 0x00000000 dan warna putih adalah 0x00ffffff.

3. Perancangan Sistem

Pada tahap ini akan dijelaskan bagaimana kerja aplikasi yang akan dibangun, sehingga sebelum aplikasi dibangun, peneliti sudah bisa mendapatkan dugaan hasil yang akan diperoleh setelah terbangunnya aplikasi ini.

Tujuan dari perancangan sistem adalah untuk memenuhi kebutuhan pengguna mengenai gambaran yang jelas tentang perancangan sistem yang akan dibuat serta diimplementasikan. Untuk mulai membangun suatu aplikasi kriptografi, maka penulis terlebih dahulu merencanakan alur kerja berdasarkan kebutuhan penggna yang akan menggunakan aplikasi ini.

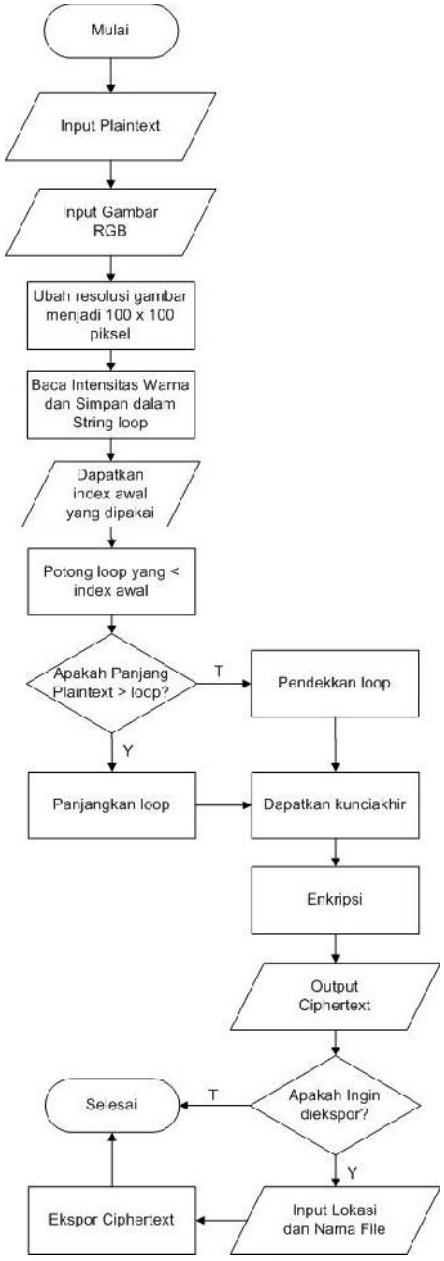
Diagram Blok



Gambar 3.1 Diagram Blok Aplikasi Kriptografi

Diagram Alur Algoritma

Berikut ini adalah diagram alur kerja aplikasi kriptografi, yang terdiri dari diagram alur proses enkripsi dan diagram alur proses dekripsi.



Gambar 3.2 Diagram Alur Proses Enkripsi

Pada diagram alur proses enkripsi, dapat diamati bahwa:

1. Proses awal adalah memasukkan plainteks yang akan dienkripsi, yang mana plainteks ini dapat diketik langsung pada teks area yang telah disediakan maupun mengimpor file teks yang telah disimpan.
2. Tahap kedua dari proses enkripsi adalah memasukkan gambar RGB 24-bit yang akan diambil nilai intensitas warna pada setiap pikselnya. Semakin banyak variasi warna pada gambar, maka kualitas cipherteks akan lebih bagus, sebaliknya jika gambar yang diinputkan berwarna hampir sama atau sama pada setiap pikselnya, maka keamanan cipherteks akan semakin berkurang. Misalkan gambar bendera Indonesia, yang mana warna piksel pada setengah jumlah baris dan semua kolom adalah sama, yaitu merah dan putih, maka pergeseran pada setiap karakter akan sama dan hal ini akan membuat ciphertext akan mudah untuk dikenali oleh pihak yang tidak berhak.
3. Setelah citra digital dimasukkan, maka citra akan diubah resolusinya menjadi 100 x 100 piksel untuk membuat variasi pergeseran yang lebih unik.
4. Tahap selanjutnya adalah membaca nilai intensitas warna RGB yang akan dikonversi dan disusun dalam sebuah String loop. Data inilah yang nantinya akan dipakai untuk pergeseran karakter Pi+Ki.
5. Memasukkan index awal pada kunci akhir yang menandai awal pergeseran pada karakter pertama.
6. Plaintext yang diinputkan tentunya memiliki panjang yang sama atau tidak sama dengan panjang String loop yang telah dibuat. Maka tahap selanjutnya adalah atur kunci dari String loop menjadi String kunciakhir yang mana:
   - Jika panjang loop < panjang plaintext, maka kunciakhir akan diperpanjang sepanjang plaintext.
   - Selainnya panjang kunciakhir akan diperpendek sepanjang plaintext.
7. Setelah terbentuk kunciakhir, maka dilanjutkan dengan proses enkripsi, yang dapat dirumuskan sebagai berikut:

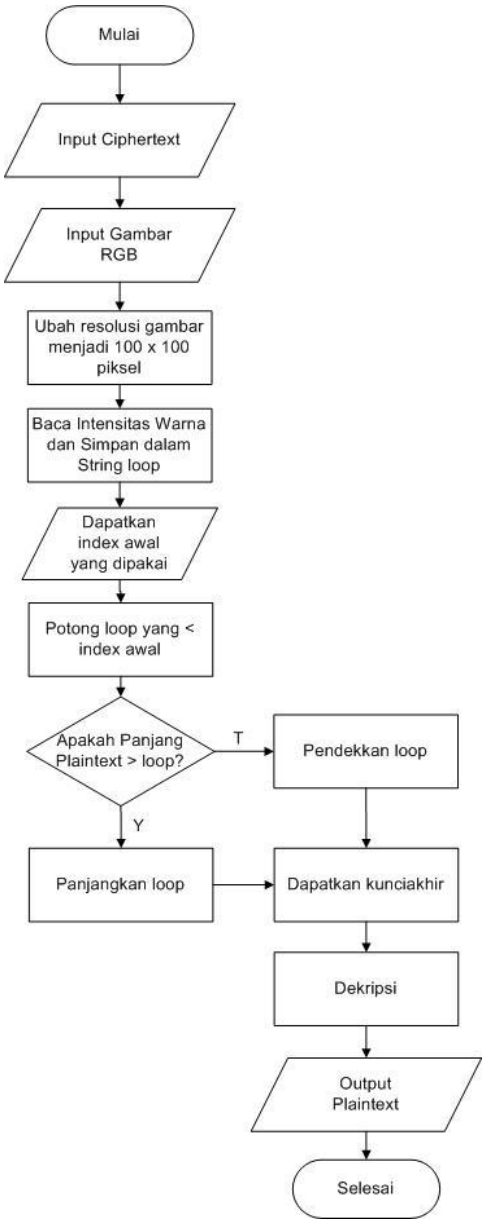
$$Ci=Pi+Ki$$

Yang mana:
Ci = ciphertext karakter ke i
Pi = plaintext karakter ke i
Ki = kunciakhir karakter ke i

Pada rumusan ini tidak menggunakan modulus, hal ini dikarenakan pada bahasa pemrograman java data char hingga urutan ke-381 masih dikenali. Angka 381 didapatkan dari karakter teakhir pada keyboard standar yaitu ~ =

karakter ke-126 ditambahkan dengan nilai maksimal pergeseran, yaitu intensitas warna tertinggi yang bernilai 255 pada setiap warna.

8. Setelah dilakukan proses enkripsi, maka akan ditampilkan sebuah cipherteks pada teks area yang disediakan. Cipherteks yang telah didapat dapat disimpan dalam file teks, jika tidak proses enkripsi berhenti sampai disini.



Gambar 3.3 Diagram Alur Proses Dekripsi

Pada diagram alur proses dekripsi, dapat diamati bahwa:

1. Proses awal adalah memasukkan cipherteks yang mana cipherteks ini dapat diketik pada teks area yang telah disediakan atau mengimpor file teks yang telah disimpan.
2. Tahap kedua dari proses dekripsi adalah memasukkan gambar RGB 24-bit yang sama dengan gambar yang digunakan saat proses enkripsi.
3. Setelah citra digital dimasukkan, maka citra akan diubah resolusinya menjadi 100 x 100 piksel untuk membuat variasi pergeseran yang lebih unik.
4. Tahap selanjutnya adalah membaca nilai intensitas warna RGB yang akan dikonversi dan disusun dalam sebuah String loop. Data inilah yang nantinya akan dipakai untuk pergeseran karakter Pi-Ki.
5. Plaintext yang diinputkan tentunya memiliki panjang yang sama atau tidak sama dengan panjang String loop yang telah dibuat. Maka tahap selanjutnya adalah atur kunci dari String loop menjadi String kunciakhir yang mana:
   - Jika panjang loop < panjang plaintext, maka kunciakhir akan diperpanjang sepanjang plaintext.
   - Selainnya panjang kunciakhir akan diperpendek sepanjang plaintext.
6. Memasukkan index awal pada kunci akhir yang menandai awal pergeseran pada karakter pertama.
7. Setelah terbentuk kunciakhir, maka dilanjutkan dengan proses dekripsi, yang dapat dirumuskan sebagai berikut:

$$Pi=Ci-Ki$$

Yang mana:
Pi = plaintext karakter ke i
Ci = ciphertext karakter ke i
Ki = kunciakhir karakter ke i

Pada rumusan ini tidak menggunakan modulus, hal ini dikarenakan pada bahasa pemrograman java data char hingga urutan ke-381 masih dikenali. Angka 381 didapatkan dari karakter teakhir pada keyboard standar yaitu ~ = karakter ke-126 ditambahkan dengan nilai maksimal pergeseran, yaitu intensitas warna tertinggi yang bernilai 255 pada setiap warna. Atau dapat

disimpulkan bahwa ada batasan karakter inputan plaintext yaitu maksimal 126 dan jumlah pergeseran maksimal 255.

4. Implementasi dan Pengujian

Implementasi Antar Muka

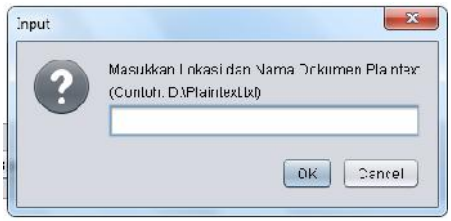
a. Antar Muka Enkripsi dan Dekripsi

Gambar 4.1 Antar Muka Enkripsi dan Dekripsi

Pada Antar Muka di atas terdapat:

- Tombol Buka Plainteks (*txt file*), dipakai untuk memasukkan plainteks dari file yang telah disimpan.
- Area plainteks, digunakan untuk menampilkan isi file yang dimasukkan atau mengetikkan langsung plainteks yang akan dienkripsi.
- Tombol Buka Ciphertext (*txt file*), dipakai untuk memasukkan cipherteks dari file yang telah disimpan.
- Area cipherteks, digunakan untuk menampilkan isi file yang dimasukkan atau mengetikkan langsung cipherteks yang akan didekripsi.
- Tombol Enkripsikan, digunakan untuk melakukan proses enkripsi.
- Tombol Dekripsikan, digunakan untuk melakukan proses dekripsi.
- Tombol Ekspor Ciphertext, digunakan untuk melakukan proses ekspor cipherteks berupa file teks.
- Tombol Bersihkan, digunakan untuk mereset variabel pada aplikasi.

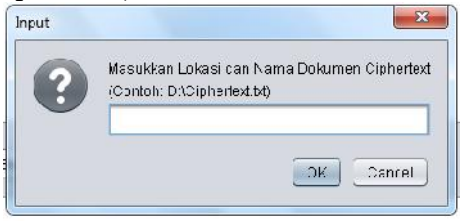
b. Antar Muka Impor File Teks (Plainteks)



Gambar 4.2 Antar Muka Impor File Teks (Plainteks)

Antar muka ini digunakan untuk memasukkan lokasi dan nama dokumen plainteks.

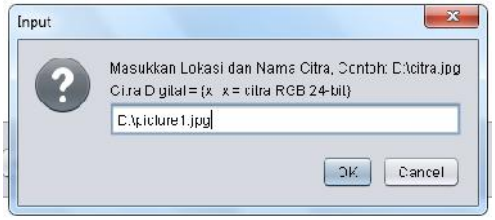
c. Antar Muka Impor File Teks (Cipherteks)



Gambar 4.3 Antar Muka Impor File Teks (Cipherteks)

Antar muka ini digunakan untuk memasukkan lokasi dan nama dokumen cipherteks.

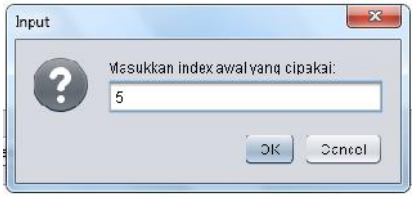
d. Antar Muka Input Lokasi dan Nama Citra Berwarna



Gambar 4.4 Antar Muka Input Lokasi dan Nama Citra Berwarna

Antar muka ini digunakan untuk memasukkan lokasi dan nama gambar yang akan digunakan.

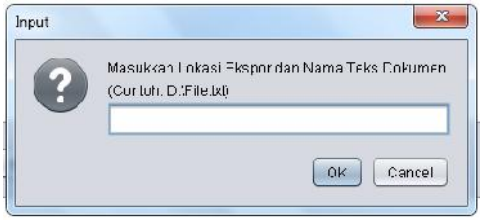
e. Antar Muka Input Indek yang dipakai



Gambar 4.5 Antar Muka Input Indek yang dipakai

Antar muka ini digunakan untuk mendapatkan indek awal pada String loop yang akan dipakai untuk proses enkripsi atau dekripsi.

f. Antar Muka Ekspor Cipherteks dalam File Teks



Gambar 4.6 Antar Muka Ekspor Cipherteks dalam File Teks

Antar muka ini digunakan untuk mengekspor cipherteks dalam file teks.

Hasil Pengujian

Pengujian enkripsi dan dekripsi seluruh karakter input keyboard

Tabel 4.1 Pengujian enkripsi dan dekripsi seluruh karakter input keyboard

Pengujian enkripsi dan dekripsi dengan jumlah karakter < 30000

Tabel 4.1 Pengujian enkripsi dengan jumlah karakter < 30000

Uji Coba Ke-1	
Plaintext	"Teknik Kriptografi untuk Mengamankan Informasi dengan Menggunakan Citra Digital sebagai Kunci"
Nama Gambar	3.BMP 
Index	1992
Ciphertext	E Q Ek ª ±¶lËÄÈ·¬_§¾ÅÁ·ÀËÓÍ×Ü ªÅ ¼ÑÊÄ×ßÔ|»¸Áµ«¾l áæÜ×äÙ¸ Á³ç ¹Þéåh'Ioonzis&{lfineq'O}u gq)
Uji Coba ke-2	
Plaintext	"Teknik Kriptografi untuk Mengamankan Informasi dengan Menggunakan Citra Digital sebagai Kunci"
Nama Gambar	1.JPG 
Index	15
Ciphertext	₸Ï Íô Ôø5ÛĤ ĘĿ¼ĝŌ½ĉİmēį Áď₶pÅĀ£Õï ßČ çđYÚĕ¯ đĒ° ÷ĢÄ©ąºøĈ¼ï·¤ãā¿ÞāÁÐïªÄ q ¼z fIÉÞ ăĆĐ·ĞÕÉÛ©Ëæf¦ ã¥×îs
Uji Coba ke-3	
Plaintext	"Teknik Kriptografi untuk Mengamankan Informasi dengan Menggunakan Citra Digital sebagai Kunci"
Nama Gambar	2.PNG 
Index	10
Ciphertext	y - ĮÅvŕÔ|ĝÌ Ũć§Ůø şé ďë{šëyď ÇxŘÛqŘØ Ţè ęØ śĀ-ă sÛ: dÇgÉ)Ç ú¬ Ā zö¨+áª Đ¡<Ö¢ û¶ Ąq ø° û¬ · ¢þª ¸

Tabel 4.1 Pengujian dekripsi dengan jumlah karakter < 30000

Uji Coba Ke-1	
Ciphertext	E Q Ek ª ±¶lËÄÈ·¬_§¾ÅÁ·ÀËÓÍ×Ü ªÅ ¼ÑÊÄ×ßÔ|»¸Áµ«¾l áæÜ×äÙ¸ Á³ç ¹Þéåh'Ioonzis&{lfineq'O}u gq)
Nama Gambar	3.BMP 
Index	1992
Plaintext	"Teknik Kriptografi untuk Mengamankan Informasi dengan Menggunakan Citra Digital sebagai Kunci"
Uji Coba ke-2	
Ciphertext	₸Ï Íô Ôø5ÛĤ ĘĿ¼ĝŌ½ĉİmēį Áď₶pÅĀ£Õï ßČ çđYÚĕ¯ đĒ° ÷ĢÄ©ąºøĈ¼ï·¤ãā¿ÞāÁÐïªÄ q ¼z fIÉÞ ăĆĐ·ĞÕÉÛ©Ëæf¦ ã¥×îs
Nama Gambar	1.JPG

	
Index	15
Plaintext	"Teknik Kriptografi untuk Mengamankan Informasi dengan Menggunakan Citra Digital sebagai Kunci"
Uji Coba ke-3	
Ciphertext	y - ĮÅvŕÔ|ĝÌ Ũć§Ůø şé ďë{šëyď ÇxŘÛqŘØ Ţè ęØ śĀ-ă sÛ: dÇgÉ)Ç ú¬ Ā zö¨+áª Ð¡<Ö¢ û¶ Ąq ø° û¬ · ¢þª
Nama Gambar	2.PNG 
Index	10
Plaintext	"Teknik Kriptografi untuk Mengamankan Informasi dengan Menggunakan Citra Digital sebagai Kunci"

5. Kesimpulan dan Saran

Kesimpulan

Aplikasi kriptografi ini merupakan kriptografi yang mengadopsi dari metode Caesar Cipher, namun kriptografi ini memiliki pergeseran yang berbeda pada setiap karakter yang tergantung pada nilai intensitas warna pada citra digital yang dimasukkan.

Dari hasil Implementasi dan Pengujian dapat disimpulkan sebagai berikut:

1. Algoritma Caesar Cipher dapat diimplementasikan pada file teks untuk seluruh karakter.
2. Citra digital dapat digunakan sebagai kunci dalam proses enkripsi dan dekripsi pada aplikasi kriptografi yang dibangun.
3. Aplikasi kriptografi ini dapat mengamankan file teks dari pihak yang tidak memiliki hak untuk mengetahuinya.
4. Pengguna dapat lebih mengingat kunci dalam bentuk gambar daripada berupa teks dalam proses enkripsi dan dekripsi

Saran

Aplikasi kriptografi ini merupakan aplikasi dekstop yang berdiri sendiri tanpa adanya interaksi dengan aplikasi lain. Oleh karenanya diharapkan akan terbangun kembali aplikasi lain yang dapat berinteraksi dengan aplikasi ini serta dapat menggunakan multimedia lain sebagai kunci

6. Daftar Pustaka

Agus Kurnia, Chandra. (2014). *Implementasi Kriptografi Teks Berbasis Modified Caesar Cipher Menggunakan Visual Basic.* Jember: Universitas Muhammadiyah Jember.

Ariyus, Dony. (2008). *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi.* Yogyakarta: C.V Andi Offset.

Astuti Hermawati, Fajar. (2013). *Pengolahan Citra Digital. Yogyakarta*: C.V Andi Offset.

Agus Kurnia, Chandra. (2014). *Implementasi Kriptografi Teks Berbasis Modified Caesar Cipher Menggunakan Visual Basic.* Jember: Universitas Muhammadiyah Jember.

Fairuzabadi, Muhammad. (2010). *Implementasi Kriptografi Klasik menggunakan Borland Delphi.* Yogyakarta: Universitas PGRI Yogyakarta.

Nugroho, Adi. (2008). *Algoritma dan Struktur Data dalam Bahasa Java*. Yogyakarta: C.V Andi Offset.

Rahardian, Rizal, dkk. (2012). *Integrasi Algoritma DES pada Public Key Cryptography untuk Aplikasi Transaksi Online.* Surabaya: Politeknik Elektronika Negeri Surabaya.