PENGGUNAAN ALGORITMA *DATA ENCRYPTION STANDARD* UNTUK CITRA DIGITAL

Lukman Hakim
Jurusan Teknik Informatika Sekolah Tinggi Ilmu Manajemen dan Komputer MURA Lubuklinggau

ABSTRAK

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan yang cepat dalam kehidupan manusia. Untuk menjaga keamanan dan kerahasiaan pesan, data, atau informasi dalam jaringan komputer akan membutuhkan beberapa enkripsi untuk membuat pesan, data atau informasi yang tidak dapat dibaca atau dipahami oleh siapapun. Salah satu ilmu pengetahuan untuk menjaga keamanan dan kerahasiaan data atau informasi yang kriptografi. Algoritma ini dikembangkan untuk memungkinkan organisasi tertentu yang ditunjuk untuk mengakses informasi. Julius caesar dikenal sebagai orang yang pertama kali mengembangkan algoritma kriptografi untuk mengirim pesan ke pasukan. Algoritma terdiri dari algoritma enkripsi dan dekripsi algoritma. Citra digital telah banyak digunakan dalam berbagai proses sehingga perlindungan gambar digital dari pihak yang tidak memiliki hak akses yang sangat penting. Ada banyak model dan metode enkripsi, salah satunya dienkripsi dengan DES (data standar enkripsi).

Keywords: Cryptography, DES, Digital imagery, Encryption, decryption

ABSTRACT

The development of information and communication technology has brought rapid change in human life. To maintain the security and confidentiality of messages, data, or information in a computer network would require some encryption to create messages, data or information that can not be read or understood by anyone. One of the science to maintain the security and confidentiality of data or information that is cryptography. Algorithm was developed to allow certain designated organizations to access the information. Julius caesar is known as the person who first developed the cryptographic algorithm to send a message to the troops. Algorithm consists of encryption algorithms and decryption algorithms. Digital imagery has been widely used in various processes so that the protection of digital images of the party who does not have access rights are very important. There are many models and encryption methods, one of which is encrypted with DES (data encryption standard).

Kata Kunci : *Cryptography, DES, Digital imagery,Encryption, Decryption*

1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi komunikasi dan informasi yang pesat telah membawa perubahan bagi kehidupan manusia. Salah satu contoh nyata dari perkembangan teknologi komunikasi dan informasi adalah perkembangan internet yang memungkinkan pertukaran data dengan mudah melalui internet tersebut. Seiring dengan perkembangan tersebut, berbagai kejahatan teknologi komunikasi dan informasi juga turut berkembang. Berbagai ancaman dari keamanan komunikasi lewat jaringan telah menjadi perhatian bagi para pengguna internet, seperti interupsi, penyadapan, modifikasi, maupun fabrikasi. Tentunya ancaman ini akan berakibat pada data-data yang dikomunikasikan (Sukrisno, 2007).

Keamanan dan kerahasiaan data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan jaringan komputer saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Sistem-sistem vital, seperti sistem pertahanan, sistem perbankan, sistem bandar udara dan sistem-sistem yang lain setingkat itu, membutuhkan tingkat kemanan yang sedemikian tinggi. Hal ini disebabkan karena kemajuan bidang jaringan komputer dengan konsep open systemnya sehingga siapapun, dimanapun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut. Untuk menjaga keamanan dan kerahasiaan pesan, data, atau informasi dalam suatu jaringan komputer maka diperlukan beberapa enkripsi guna membuat pesan, data atau informasi agar tidak dapat di baca atau dimengerti oleh sembarang orang. Kecuali untuk penerima yang berhak (Kristanto, 2003).

Salah satu ilmu untuk menjaga keamanan dan kerahasiaan data atau informasi adalah kriptografi. Algoritma kriptografi pertama kali dikembangkan untuk mengijinkan organisasi tertentu yang ditunjuk untuk mengakses suatu informasi. Oleh sebab itu penelitian ini akan membangun sebuah Aplikasi Enkripsi dan Dekripsi Dengan Algoritma DES *(Data encryption standard)* Untuk Citra Digital.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan diatas maka rumusan masalah yang akan dibahas adalah bagaimana membuat aplikasi enkripsi dan dekripsi dengan algoritma *Data encryption standard* (DES) untuk citra digital ?

1.3. Tujuan dan Manfaat

tujuan dari penulisan ini adalah untuk :
memungkinkan kita untuk mengakses informasi penting dengan tingkat keamanan yang tidak dapat dibaca atau dipahami oleh siapapun.

– **Manfaat**

Sedangkan manfaat yang dapat diperoleh adalah: dapat melindungi data – data yang dianggap penting dan dapat juga di pakai oleh suatu instansi atau perusahaan.

1.4. Metode Pembahasan

Metode yang digunakan dalam penulisan ini adalah metode studi literartur dengan analisa yang dikemukakan berserta deskriptif berdasarkan data yang didapat dari hasil penelitian yang telah dilakukan .

Mengetahui Detektor Gas yang dapat mendetaksi kebocoran Gas LPG dengan sensor TGS2610

2. TINJAUAN PUSTAKA

2.1 Kriptografi

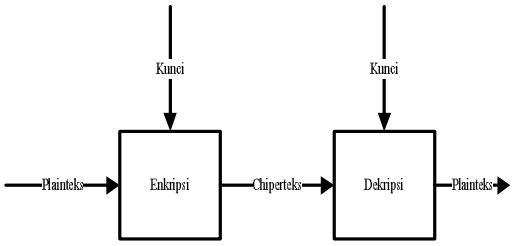
Kriptografi *(cryptography)* atau yang sering dikenal dengan sebutan ilmu penyandian data, adalah suatu bidang ilmu dan seni *(art and science)* yang bertujuan untuk menjaga kerahasiaan suatu pesan yang berupa data-data dari akses oleh orang-orang atau pihak-pihak lain yang tidak berhak sehingga tidak menimbulkan kerugian. *Cryptography* berasal dari bahasa yunani *cryptos (secret)* dan *graphein (writing).* Jadi kriptografi berarti *secret writing* (tulisan rahasia). bidang ilmu kriptografi ini semula hanya populer di bidang militer dan bidang intelijen untuk menyandikan pesan-pesan panglima perang kepada pasukan yang berada di garis depan akan tetapi seiring dengan semakin berkembangnya teknologi terutamanya teknologi informasi dan semakin padatnya lalu lintas informasi yang terjadi tentu saja semakin menuntut adanya suatu komunikasi data yang aman, bidang ilmu ini menjadi semakin penting. Sekarang bidang ilmu ini menjadi salah satu isu suatu topik riset yang tidak habis-habisnya diteliti dengan melibatkan banyak peneliti (Tarbudi, 2010). Didalam kriptografi kita akan sering menemukan berbagai istilah atau terminologi, yaitu pesan. Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain dari pesan adalah plainteks. Agar pesan tidak dapat dimengerti maka pesan perlu disandikan kebentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut cipherteks (munir, 2006).

Ilmu kriptografi sebenarnya sudah mulai dipelajari manusia sejak tahun 400 SM, yaitu pada zaman yunani kuno. Dari catatan bahwa penyandian transposisi merupakan sistem kriptografi pertama yang digunakan atau dimanfaatkan. Bidang ilmu ini terus berkembang seiring dengan kemajuan peradaban manusia dan memegang peranan penting dalam strategi peperangan yang terjadi dalam sejarah manusia, mulai dari sistem kriptografi *caesar chiper* yang terkenal pada zaman romawi kuno, *playfair cipher* yang digunakan inggris dan *ADFVGX Cipher* yang digunakan jerman pada perang dunia I hingga algoritma-algoritma kriptografi rotor yang populer pada perang dunia II seperti *sigaba* M-134 (Amerika serikat), *typex* (inggris), *purple* (jepang), dan mesin kriptografi legendaris *enigma* (jerman) (Tarbudi, 2010).

Dalam teknologi informasi telah dan sedang dikembangkan cara-cara untuk menangkal berbagai bentuk serangan semacam penyadapan dan pengubahan data yang dikirimkan. Salah satu cara yang ditempuh mengatasi masalah ini ialah dengan menggunakan kriptografi yang menggunakan transformasi data sehingga data yang dihasilkan tidak dapat dimengerti oleh pihak yang tidak berhak mengakses. Transformasi ini memberikan solusi pada dua macam masalah keamanan data, yaitu masalah privasi dan keotentikan. Privasi mengandung arti bahwa data yang diinginkan hanya dapat dimengerti informasinya oleh penerima yang sah atau berhak. Sedangkan keotentikan mencegah pihak ketiga untuk mengirimkan data yang salah atau mengubah data yang dikirimkan.

Didalam kriptografi kita akan sering menemukan berbagai istilah atau terminologi, yaitu pesan. Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain dari pesan adalah plainteks. Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan perlu disandikan kebentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut cipherteks. Cipherteks harus dapat ditransformasikan kembali menjadi plainteks semula agar pesan yang diterima bisa dibaca. Proses menyandikan plainteks menjadi chiperteks disebut enkripsi *(encryption).* Sedangkan proses mengembalikan cipherteks menjadi plainteks semula dinamakan dekripsi *(decryption).*

Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara kedua himpunan tersebut. misalkan *P* menyatakan plainteks dan *C* menyatakan chiperteks, maka fungsi enkripsi *E* memetakan *P* ke *C* (Munir, 2006).



Gambar 2.1 Enkripsi Dan Dekripsi

3. METODELOGI

Pada penelitian Drs. Akik hidayat. Proses enkripsi dan dekripsi suatu data dengan algoritma 3DES dilakukan dengan cara mengimplementasikan algoritma DES sebanyak tiga kali, sesuai dengan pemilihan kuncinya dan urutan proses yang dipilih. Untuk algoritma 3DES, pada proses enkripsi kecepatan rata-ratanya adalah 0.03024 kb/detik dan pada proses dekripsi kecepatan rata-ratanya adalah 0.05908 kb/detik. sedangkan untuk algoritma DES, pada proses enkripsi kecepatan rata-ratanya adalah 0.08828 kb/detik dan pada proses dekripsi kecepatan rata-ratanya adalah 0.16667 kb/detik (Hidayat, 2008).

Pada penelitian Rizqi firmansyah, danWahyu suadi. pesan yang semakin panjang akibat enkripsi DES tidak menjadi faktor utama dalam menghasilkan distorsi gambar. Oleh karena itu penggunaan algoritma kriptografi DES tidak mempengaruhi kinerja algoritma steganografi REDD itu sendiri. Penambahan kriptografi DES dalam proses REDD malah semakin memperkuat keamanan steganografi tersebut (Firmansyah, 2011).

3.1 Citra

Citra *(image)* istilah lain untuk gambar, sebagai salah satu komponen multimedia yang memegang peranan sangat penting sebagai bentuk informasi *visual*. Citra mempunyai karakteristik yang tidak dimiliki oleh data teks. Citra kaya dengan informasi. Ada sebuah peribahasa yang berbunyi "sebuah gambar bermakna lebih dari seribu kata" *(a pciture is more than a thousand words)*. Maksudnya tentu sebuah gambar dapat memberikan informasi yang lebih banyak dari pada informasi yang disajikan dalam bentuk kata-kata. Secara harafiah citra *(image)* adalah gambar pada bidang dwimatra (dua dimensi). Ditinjau dari sudut pandang matematis citra merupakan fungsi menerus *(continue)* dari intensitas cahaya pada bidang dwimatra. Sumber cahaya menerangi objek. Objek memantulkan kembali sebagian dari berkas cahaya tersebut. Pantulan cahaya ini ditangkap oleh alat-alat optik, misalnya mata pada manusia, kamera, pemindai *(scanner)*. Sehingga bayangan objek yang disebut citra tersebut terekam. Citra sebagai keluaran dari suatu sistem perekaman data dapat bersifat (Munir, 2004).

Gambar 2.2 Webcam dan Orang

Format citra yang baku di lingkungan sistem operasi Microsoft Windows adalah file bitmap (BMP). Pada saat ini format BMP kurang begitu populer dan mulai jarang digunakan dibanding format JPG atau GIF, karena file BMP pada umumnya tidak dimampatkan, sehingga ukuran relatif lebih besar dari pada file JPG atau GIF.

Terjemahan bebas bitmap adalah pemetaan bit. Artinya nilai intensitas piksel di dalam citra dipetakan ke sejumlah bit tertentu. Peta bit umumnya adalah 8, yang berarti setiap piksel panjangnya 8 bit. Delapan bit ini mempresentasikan nilai intensitas piksel. Dengan demikian ada sebanyak 2^8 =256 derajat keabuan, mulai dari 0 (00000000) sampai 255 (11111111).

Terdapat tiga macam citra dalam format BMP, yaitu citra biner, citra berwarna dan citra hitam-puth (*grayscale*). Citra biner hanya memiliki dua nilai keabuan 0 dan 1. Oleh kerena itu 1 bit telah cukup untuk mempresentasikan nilai piksel. Citra berwarna adalah citra yang lebih umum. Warna yang terlihat di dalam citra bitmap merupakan kombinasi dari tiga komponen warna, yaitu R (Red), G (Green) dan B (Blue). Kombinasi dari tiga warna RGB tersebut menghasilkan warna yang khas untuk piksel yang bersangkutan. Pada citra 256 warna, setiap piksel memiliki panjang 8 bit, akan tetapi komponen RGB nya disimpan dalam tabel RGB yang disebut *palet*. Berikut ini akan memperlihatkan panjang informasi palet untuk tiap versi bitmap, masing-masing untuk citra 16 warna, 256 warna dan 16,7 juta warna. Berkas citra 24 bit tidak mempunyai palet RGB, karena langsung di uraikan ke dalam data *bitmap*

3.2 Analisis Dan Pembahasan

Citra (foto) merupakan suatu dokumentasi yang biasa disimpan dalam kurun waktu tertentu.

Hampir semua aktivitas manusia dengan berbagai kehidupannya bisa di foto untuk dokumentasi. Dalam sebuah karya citra terdapat hak cipta fotografi. Hak cipta baik untuk dilindungi karena dalam dunia internet tingkat keamanan sebuah citra sudah melemah. Untuk menjaga keamanan citra khususnya citra digital dapat menggunakan kriptografi.

Tahapan dalam Algoritma DES dimulai dengan membentuk kunci. Kunci yang dimaksud adalah kunci internal yang dibangkitkan oleh kunci eksternal yang diberikan oleh pengguna. Sebagai contoh, ditentukan "yunika78" sebagai kunci eksternal. Tiap karakter dari kunci ini diterjemahkan ke dalam bilangan biner.

Tabel 3.1 *Kunci eksternal*

Kunci	Heksadesimal	Biner
y	79h	01111001
u	75h	01110101
n	6Eh	01101110
i	69h	01101001
k	6Bh	01101011
a	61h	01100001
7	37h	00110111
8	38h	00111000

Sehingga bit kunci eksternal disusun sebagai berikut :

yunika78 = 01111001 01110101 01101110 01101001 01101011 01101011 00110111 00111000

Setiap bit dari kunci eksternal kemudian diacak menggunakan matriks permutasi kompresi PC-1. Matriks ini meletakkan tiap bit dari susunan kunci eksternal ke dalam susunan bit yang telah ditentukan

Tabel 3.2 *PC-1*

57	49	41	33	25	27	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Sehingga didapat bit hasil permutasi kompresi PC-1 dari bit kunci eksternal sebagai berikut:

PC-1 = 0000000 1001111 1111111 1111100 0111010 0000111 1010111 1010011

Hasil permutasi kompresi PC-1 dari kunci eksternal kemudian dikelompokkan menjadi 2 bagian, kiri dan kanan, yang masing-masing panjangnya 28 bit dan dimasukkan ke dalam variabel C_0 dan D_0.

C_0= 0000000 1001111 1111111 1111100

D_0= 0111010 0000111 1010111 1010011

Kemudian kedua bagian digeser ke kiri (*left shift*) sepanjang satu atau dua bit sesuai dengan ketentuan.

Tabel 3.3 Jumlah pergeseran bit pada tiap putaran

Putaran, i	Jumlah
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Setelah pergeseran bit, komponen variabel C_i dan D_i digabung kembali dan mengalami permutasi kompresi dengan menggunakan matriks PC-2

Tabel 3.4 *PC-2*

14	17	11	24	1	5	3	28	60	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Proses enkripsi pada algoritma DES, dilakukan pada tiap blok *plaintext* yang berisi 64 bit. Sebagai contoh kita ambil plaintext "enkripsi", kemudian dirubah ke dalam bentuk biner.

enkripsi : 01100101 01101110 01101011 01110010 01101001 01110000 01110011 01101001

Bilangan biner dari plaintext tadi, kemudian di acak dengan menggunakan permutasi awal atau *initial permutation* (IP).

Sehingga didapat hasil permutasi awal dari plaintext "enkripsi" .

enkripsi : 01100101 01101110 01101011 01110010 01101001 01110000 01110011 01101001

IP : 11111111 01101000 00000011 11010101 00000000 11111111 10010110 01001110

Hasil permutasi dari IP, kemudian dikelompokkan menjadi dua bagian. Sebelah kiri dimasukkan ke dalam variabel L_0 sebanyak 32 bit dan 32 bit sebelah kanan dimasukkan ke dalam variabel R_0.

L_0 : 11111111 01101000 00000011 11010101
R_0 : 00000000 11111111 10010110 01001110

Selanjutnya dilakukan putaran dengan menggunakan fungsi *feistel* sebanyak 16 kali, dengan tahapan sebagai berikut:

a) Nilai variabel R_{i-1} dimasukkan ke dalam variabel L_i
$L_i = R_{i-1}$
b) Kemudian nilai variabel R_{i-1} yang panjangnya 32 bit diekspansi menjadi 48 bit dengan menggunakan matriks permutasi *E*.
c) Kemudian hasil ekspansi $E(R_{i-1})$ dilakukan operasi *xor* dengan K_i, menghasilkan vektor *A* dengan panjang 48 bit.
$E(R_{i-1}) \oplus K_i = A$
d) Vektor *A* dikelompokkan menjadi 8 kelompok, masing-masing 6 bit, dan menjadi masukan bagi proses substitusi. Proses substitusi dilakukan dengan menggunakan delapan buah *S-box*, S_1 sampai S_8. Setiap kotak-S menerima masukan 6 bit dan menghasilkan keluaran 4 bit.
e) Keluaran proses substitusi adalah vektor *B* yang panjangnya 32 bit.
f) Kemudian Vektor *B* diacak dengan menggunakan matriks permutasi *P*, menghasilkan *P(B)*.
g) Selanjutnya, bit-bit *P*(*B*) di-*xor*-kan dengan L_{i-1} untuk mendapatkan R_i.
$R_i = L_{i-1} \oplus P(B)$

Sehingga didapat

L_{16} = 11011111010011000100000000111100
R_{16} = 10010111100110101110100011010101

Kemudian digabungkan blok variabel R_{16} dan L_{16} menjadi:

10010111100110101110100011010101110111110100110001000000000111100

Terakhir, dipermutasikan lagi dengan *inverse initial permutation* (IP-1)

Ciphertext :
11000001110100001110001110110110110100110001101010110111010101

Dan akan ditampilkan menjadi: ÁÐã¶ÓÕ

Secara keseluruhan setiap tahapan pada proses dekripsi sama dengan tahapan pada proses enkripsi, menggunakan kunci yang sama, menggunakan matriks permutasi yang sama dan menggunakan *s-box* yang sama. Perbedaanya hanya pada urutan penggunaan kunci internal. Pada proses dekripsi kunci K_{16} yang terlebih dahulu digunakan berurut secara menurun hingga kunci K_1.

Ciphertext yang telah didapat dari proses penyandian kata "enkripsi", kemudian dipermutasikan dengan tabel permutasi awal (IP).

Ciphertext :
11000001110100001110001110110110110100110001101010110111010101

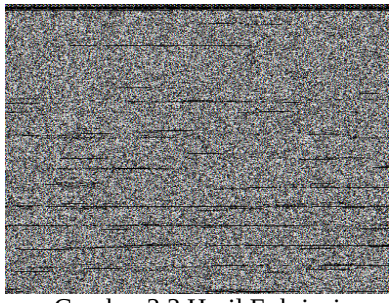
Menjadi:

IP : 10010111 10011010 11101000 11010101 11011111 01001100 01000000 00111100

Kemudian dibagi menjadi dua bagian dengan masing-maing 32 bit bagian sebelah kiri dengan nama L_0 dan 32 bit bagian sebelah kanan dengan nama R_0.

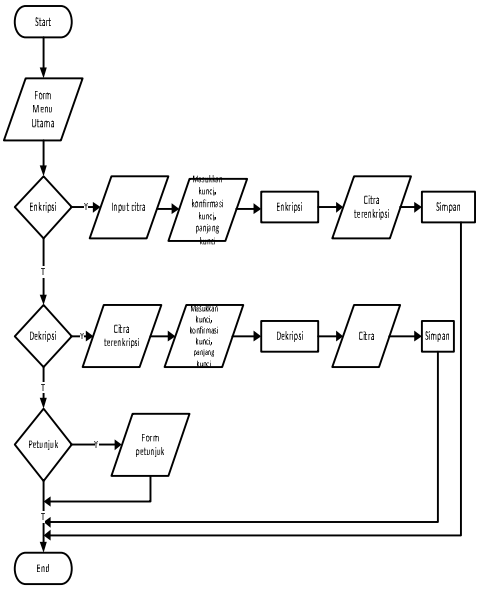
L_0 : 10010111100110101110100011010101
R_0 : 11011111010011000100000000111100

Selanjutnya dilakukan putaran dengan fungsi *feistel* sebanyak 16 kali seperti pada proses enkripsi, namun urutan kunci dimulai dari K_{16}.

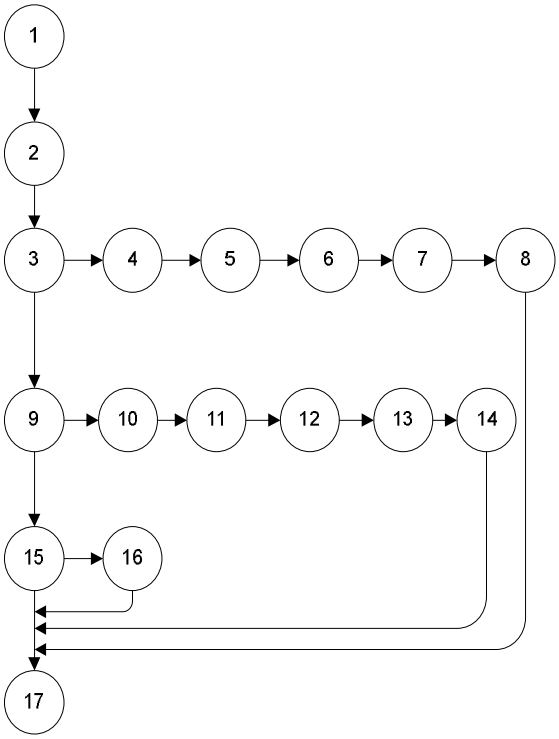


Gambar 3.3 Hasil Enkripsi

Flowchart adalah bagan yang memperlihatkan urutan prosedur dan proses dari beberapa file didalam media tertentu. Melalui *flowchart* dapat terlihat jenis media penyimpanan yang dipakai dalam pengolahan data. Selain itu juga menggambarkan file yang dipakai sebagai *input* maupun *output* (Sommerville, 2003).

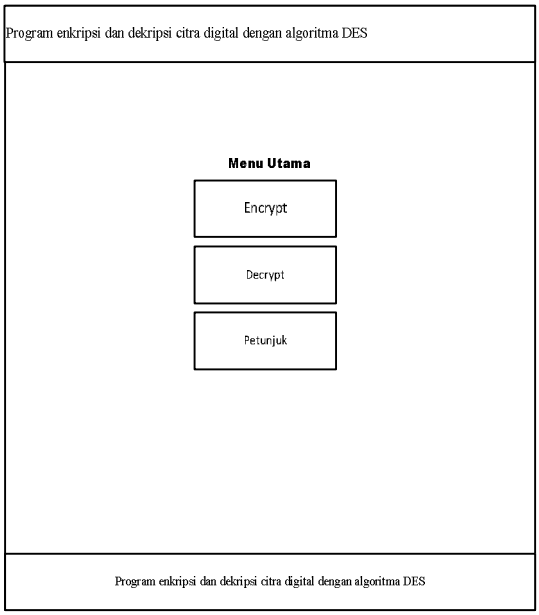


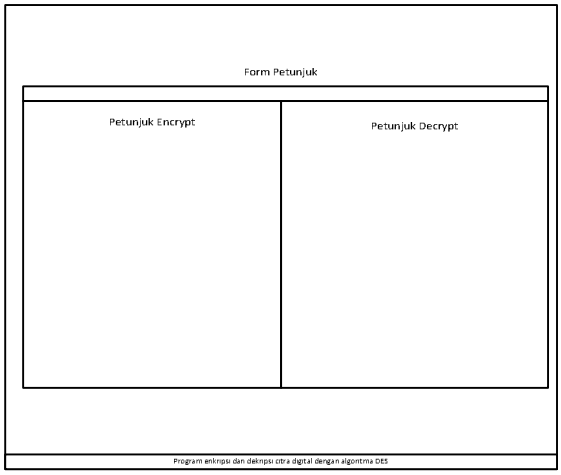
Gambar 3.4 *Flowchart Enkripsi Dan Dekripsi*

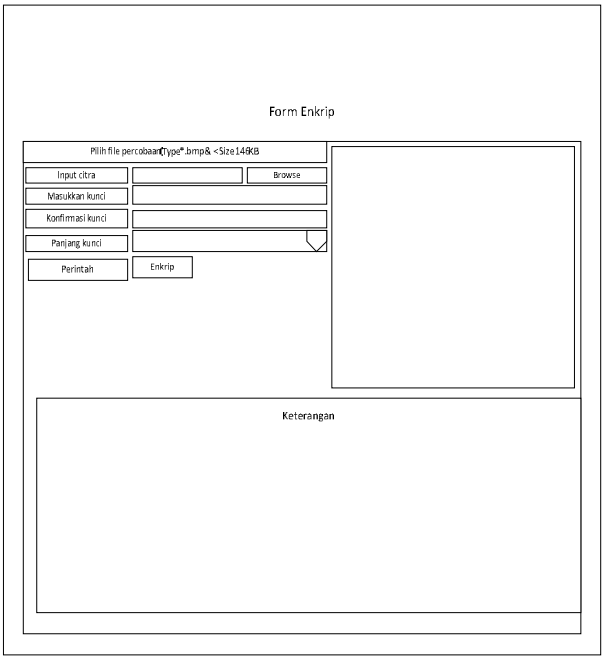


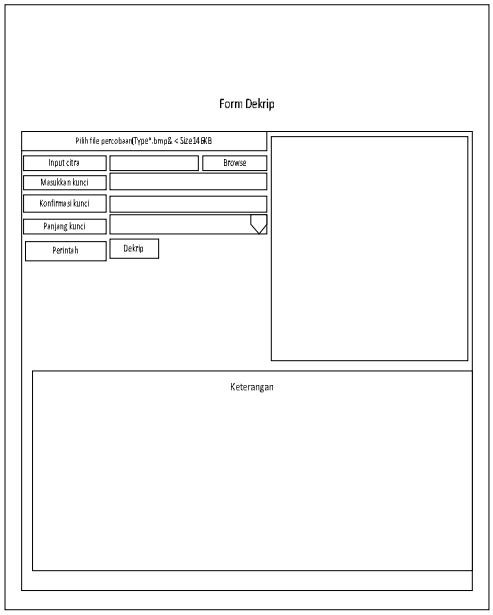
Gambar 3.6 *Flowgraph Aplikasi Enkripsi Dekripsi*

Rancangan Tampilan Antarmuka





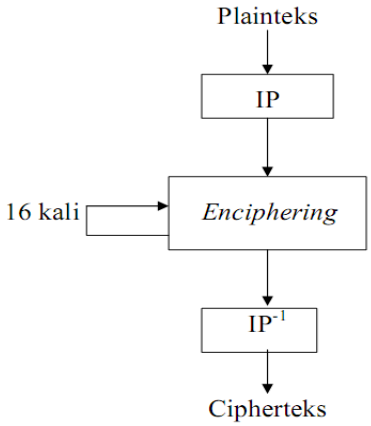




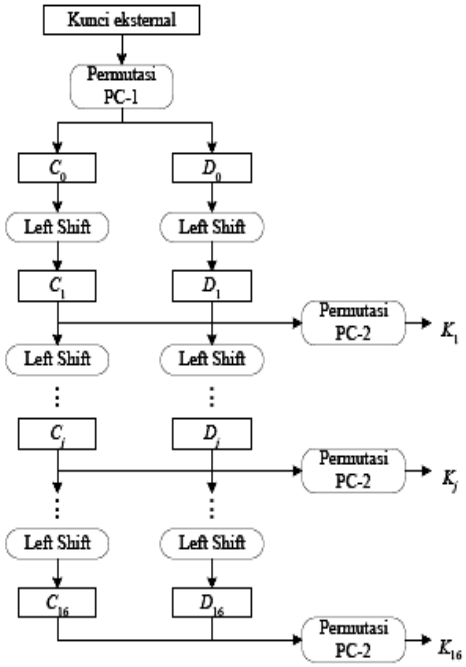
3.3 Algoritma DES Dan Program

DES (*Data encryption standard*) adalah algoritma cipher blok yang populer karena dijadikan standard algoritma enkripsi kunci simetri. Algoritma DES dikembangkan di *IBM* dibawah kepemimpinan W.L. Tuchman pada tahun 1972. Algoritma ini didasarkan pada algoritma lucifer yang dibuat oleh Horst feistel. Algoritma ini telah disetujui oleh *national bureau of standard* (*NBS*) setelah penilaian kekuatannya oleh national security agency (*NSA*) amerika serikat. DES termasuk kedalam sistem kriptografi simetri dan tergolong jenis cipher blok. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (*internal key)*. Kunci internal dibangkitkan dari kunci eksternal *(eksternal key)* yang panjangnya 64 bit (Munir, 2004). Skema global dari algoritma

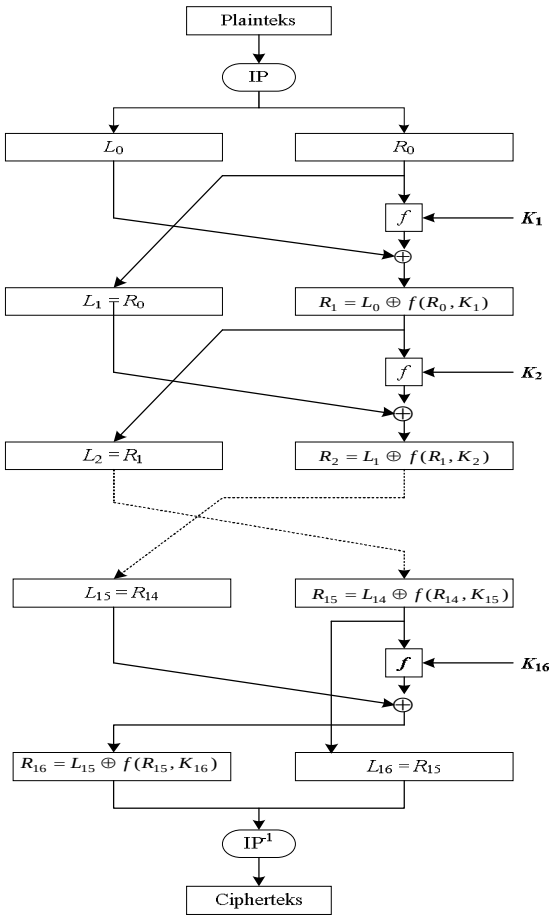
DES *(Data encryption standard)* pertama-tama adalah melakukan permutasi terhadap blok plainteks dengan matriks permutasi awal *(initial permutation atau IP).* Hasil permutasi awal kemudian di *enciphering* sebanyak 16 kali (16 putaran) dimana Setiap putaran menggunakan kunci internal yang berbeda. Hasil *enciphering* kemudian dipermutasi dengan matriks permutasi balikan *(invers initial permutation atau* IP^{-1}*)* menjadi cipherteks. Dapat dilihat pada gambar dibawah ini.



Gambar 3. 5 Skema Global Algoritma DES



Gambar 3.6. Pembangkitan Kunci Internal



Gambar 3.7 Proses Enkripsi

4. KESIMPULAN DAN SARAN

4.1. Kesimpulan

1. Pada saat proses enkripsi dan dekripsi citra dengan format bitmap tidak memerlukan waktu yang sangat lama hal ini terjadi karena ukuran file citra yang digunakan dengan batas ukuran <146KB.
2. Proses enkripsi dan dekripsi dengan menggunakan algoritma *Data encryption standard* dengan ukuran file citra 144KB, 12KB, dan 16KB membutuhkan spesifikasi perangkat keras yang besar dengan prosesor 2.00GHz dan memori 4.00GB agar waktu proses enkripsi dan dekripsi tidak memakan waktu lama. Hasil yang didapat bahwa proses enkripsi dengan algoritma *Data encryption standard* dapat mengubah citra bitmap yang asli menjadi citra bitmap terenkripsi dan proses dekripsi akan mengembalikan citra terenkripsi menjadi citra bitmap yang asli dengan waktu yang singkat.
3. Kunci yang digunakan pada proses enkripsi dan pada proses dekripsi harus sama dan tidak boleh berbeda.
4. Pada saat proses enkripsi dan dekripsi dengan menggunakan algoritma *Data encryption standard* informasi citra digital dapat dikatakan aman.

4.2. SARAN

Disini penulis menyarankan pengembangan lebih lanjut, dari rekan rekan sekalian agar dapat berman faat bagi perkembangan teknologi dan keamana data dimasa mendatang .

DASFTAR PUSTAKA

Ahmad, 2005. Proses pencitraan

[1].Firmansyah, Rizqi., dan Wahyudi suadi. 2011. Implementasi kriptografi dan steganografi pada media gambar dengan menggunakan metode DES dan Region Embe data density.

[2].Hidayat, Akik .2008. Enkripsi dan dekripsi dengan algoritma 3DES.

[3].Krikor, Lala, Sami Baba, Thawar Arif, Zyad Shaaban.2009. Image encryption using DCT and stream cipher

[4].Kristanto, Andri. Keamanan Data pada Jaringan Komputer, Gava Media, Yogyakarta, 2003.

[5].Munir, Rinaldi.2006. Kriptografi

[6].Munir, Rinaldi.(2004). Bahan kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[7].Pressman, Roger s.PHD .1997. Software engineering (Rekayasa Perangkat Lunak (buku 1)) the McGraw-hill Companies,inc.

[8].Pressman, Roger. S. 2005. Software Engineering A Practitioners's Approach Sixth Edition. Singapore: McGraw-Hill International Edition.

[9].Sukrisno dan Ema Utami. 2007. *Implementasi Steganografi Teknik EOF Dengan Gabungan Enkripsi Rijndael, Shift Chiper dan Fungsi Hash MD5.*

[10].Sommerville, Ian. 2003. *Software Engineering (Rekayasa Perangkat Lunak).* Erlangga : Jakarta.

[11].Tarbudi, membangun aplikasi keamanan transmisi data multimedia menggunakan kriptografi algoritma data encryption standard.