Jurnal Sarjana Teknik Informatika
Volume 2 Nomor 2, Juni 2014
e-ISSN: 2338-5197

IMPLEMENTASI ALGORITMA KRIPTOGRAFI KUNCI PUBLIK ELGAMAL UNTUK PROSES ENKRIPSI DAN DEKRIPSI GUNA PENGAMANAN FILE DATA

[1] Faqihuddin Al-Anshori, [2]Eko Aribowo (0006027001)

[1,2] Program Studi Teknik Informatika
Universitas Ahmad Dahlan
Prof. Dr. Soepomo, S.H., Janturan, Umbulharjo, Yogyakarta 55164
[2]Email: ekoab@tif.uad.ac.id

ABSTRAK

Di masa sekarang ini hampir semua komunikasi data serba digital mulai dari pengiriman file-file baik dokumen-dokumen berbasis teks, gambar, suara, maupun video. Berbagai macam cara menyembunyikan file telah banyak kita temui salah satunya yang paling populer adalah dengan cara menghidden. Perkembangan penyembunyian file itu sendiri semakin hari semakin pesat. Dengan kata lain file yang disembunyikan tersebut sudah barang tentu banyak orang sudah mengetahui cara untuk membukanya hal ini membuat setiap orang yang akan menyembunyikan data/file merasa bahwa ini sudah tidak aman lagi.

Subyek dalam penelitian ini adalah bagaimana mengamankan sebuah file data. Metode yang digunakan adalah Kriptografi ElGamal metode ini merupakan bagian dari kriptografi asimetris Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi dan hasilnya digabungkan. Keamanan algoritma ElGamal terletak pada kesulitan penghitungan logaritma diskret pada bilangan modulo prima yang besar sehingga upaya untuk menyelesaikan masalah logaritma ini menjadi sangat sukar. Sistem yang dihasilkan diuji dengan dua metode, yaitu Black Box Test dan Alpha Test.

Hasil dari penelitian ini akan diimplemtasikan dalam sebuah program aplikasi menggunakan bahasa pemrograman Visual Basic yang dapatmemberikan kemudahan bagi setiap orang yang akan mengamankan file-file penting. Salah satu algoritma yang digunakan untuk enkripsi dan dekripsi pada tugas akhir ini adalah algoritma ElGamal. Hasil pengujian sistem menunjukkan bahwa pengamanan file menggunakan Kriptografi dengan metode ElGamal ini layak dan dapat dipergunakan untuk mengamankan file data yang akan kita amankan.

Kata kunci: Kriptogafi, ElGamal, Asimetris, Enkripsi, Dekripsi.

 e-ISSN: 2338-5197

1. PENDAHULUAN

Di masa sekarang ini hampir semua komunikasi data serba digital mulai dari pengiriman file-file baik dokumen-dokumen berbasis teks, gambar, suara ,maupun video. Berbagai macam cara menyembunyikan file telah banyak kita temui salah satunya yang paling populer adalah dengan cara menghidden.

Perkembangan penyembunyian file itu sendiri semakin hari semakin pesat. Dengan kata lain file yang disembunyikan tersebut sudah barang tentu banyak orang sudah mengetahui cara untuk membukanya hal ini membuat setiap orang yang akan menyembunyikan data/file merasa bahwa ini sudah tidak aman lagi. Sehingga apabila berbicara mengenai sebuah pengamanan pasti tidak akan jauh dari apa yang disebut kriptografi.

Penyembunyian data/file tidaklah terjamin dan selalu ada resiko terbuka untuk umum, dalam artian semua isinya dapat dibaca oleh orang yang tidak berhak. Hal ini disebabkan karena fitur penyembunyian itu tadi tidak untuk diamankan akan tetapi lebih kepda penyembunyiannya. Tidak tertutup kemungkinan ada orang yang mencoba untuk membuka dokumen tersebut. Untuk meningkatkan keamanan salah satunya adalah dengan cara mengenkripsikan data tersebut. Belum banyaknya fitur pengenkripsian data sehingga menjadi peluang untuk dilakukan penelitian dalam tugas akhir ini. Salah satu metode yang diambil di tugas akhir ini adalah metode Elgamal. Kriptografi ElGamal merupakan bagian dari kriptografi asimetris. Pertamakali dipublikasikan oleh Taher ElGamal pada tahun1985. Kriptografi ElGamal pada mulanya digunakan untuk digital signature,namun kemudian dimodifikasi sehingga juga biasa digunakan untuk enkripsi dan deskripsi. Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi dan hasilnya digabungkan. Keamanan algoritma ElGamal terletak pada kesulitan penghitungan logaritma diskret pada bilangan modulo prima yang besar sehingga upaya untuk menyelesaikan masalah logaritma ini menjadi sangat sukar. Algoritma ini mempunyai kerugian pada cipherteksnya yang mempunyai panjang dua kali lipat dari plainteksnya. Akan tetapi, algoritma ini mempunyai kelebihan pada enkripsi. Untuk plainteks yang sama, algoritma ini memberikan cipherteks yang berbeda (dengan kepastian yang dekat) setiap kali plainteks di enkripsi.

Berdasarkan latar belakang masalah tersebut diatas, maka dibuat : “Imoplementasi Algoritma Kriptografi Kunci Publik El-Gamal Untuk Keamanan Perpindahan File Data”.

2. KAJIAN PUSTAKA

Ada beberapa penelitian yang telah dilakukan pada algoritma ElGamal. Kajian terdahulu diambil dari penelitian Mukhammad Ifanto ”Metode Enkripsi Dan Dekripsi Dengan Menggunakan Algoritma Elgamal, Institut Teknolgi Bandung”. Pada penelitian ini diperoleh bahwa algoritma ElGamal keamanannya terletak pada logaritma diskrit pada grup pergandaan bilangan bulat modulo prima, dengan mengambil nilai bilangan prima yang besar, maka upaya pemecahan pesan akan sangat sukar.[2]

Adapun penelitian lainnya yang berkaitan dengan algoritma ElGamal adalah penelitian Eko Ariwibowo” Aplikasi Pengamanan Dokumen Office Dengan Algoritma

 e-ISSN: 2338-5197

Kriptografi Kunci Asimetris ElGamal", Universitas Ahmad Dahlan Yogyakarta. Dalam penelitian ini disimpulkan bahwa Implementasi program ini menghasilkan suatu aplikasi yang mengubah isi dokumen (plaintext) yang berupa text, table dan gambar menjadi kode-kode yang tidak dikenal (ciphertext).[3]

Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi.

3. METODE PENELITIAN

Pengumpulan data dilakukan untuk memperoleh data yang dibutuhkan dalam sebuah program aplikasi. Dalam penelitian ini teknik pengumpulan data yang dilakukan adalah:

Metode kepustakaan dan Browsing/Penelusuran Internet. Metode kepustakaan dimaksudkan untuk mendapatkan data-data yang diperlukan dalam hal menelaah dan menganalisis kenyataan yang ada pada obyek penelitian, yaitu dengan cara mengumpulkan , mempelajari dan memahami buku-buku referensi serta laporan tugas akhir yang berhubungan dengan penelitian ini.Metode wawancara Merupakan metode yang dilakukan dengan mengajukan pertanyaan atau tanya jawab secara langsung dengan steakholder yang terlibat di dalam system. Observasi Yaitu pengumpulan data melalui pengamatan secara langsung terhadap cara kerja para pengguna fitur pengamaanan file data yaitu algoritma sistem kriptografi kunci umum metode algoritma ElGamal, dilakukan dengan maksud untuk mengetahui tentang cara, prosedur atau sistem kriptografi kunci umum dan pengumpulan data secara langsung, sehingga dapat mengetahui segala permasalahan yang berkaitan dengan sistem kriptografi kunci umum dengan algoritma ElGamal. Running dan Mengamati Program Kriptografi Untuk mendapatkan kekurangan dan kelebihan suatu program kriptografi yang sudah dibangun maka salah satu caranya adalah dengan memberikan quisioner atau angket untuk mengetahui sejauh mana aplikasi ini nantinya akan sangat berguna atau tidak.

4. HASIL DAN PEMBAHASAN

4.1 Analisa Kebutuhan Sistem

Dari penelitian ini dihasilkan sebuah program aplikasi enkripsi dan dekripsi elgamal yang dibangun menggunakan visual basic. Aplikasi ini dapat digunakan oleh user baik secara umum maupun untuk suatu organisasi atau perusahaan. Aplikasi ini dirancang untuk mengenkripsi perpindahan file data yaang akan dimankan. User diberi kebebasan untuk mengamankan data file itu, bisa berupa dta file bebentuk rtf, txt, dn pesan singkat. Hasil dari penelitian akan menghasilkan sebuah program aplikasi yang:

a. Dapat mengubah file asli menjadi file yang terenkrikpsi di mana isi file tidak dapat dibaca.
b. Dapat mengembalikan file yang tidak bisa dibaca menjadi file aslinya dengan metode elgamal tanpa merusak dan mengubah isi file tersebut.
c. Dapat mengubah pesan asli berupa plaintext menjadi chipertext yaitu berupa kode-kode yang tidak bisa terbaca.

 e-ISSN: 2338-5197

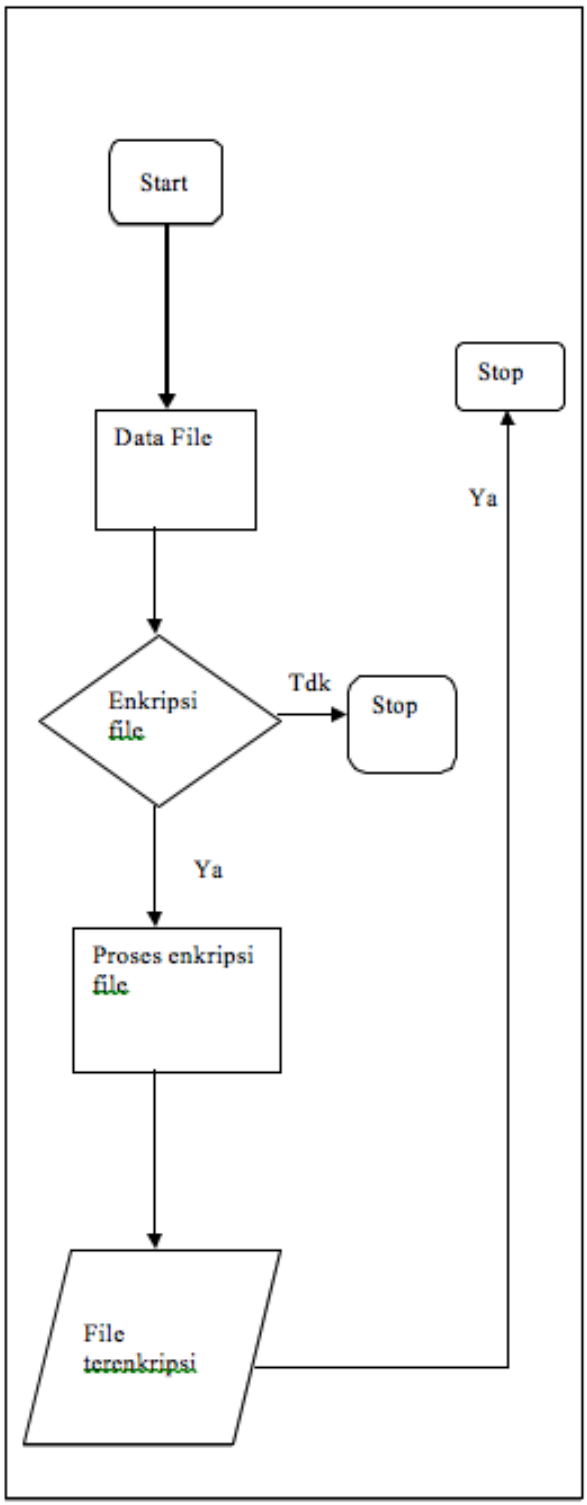
4.2 Perancangan

a. Flowchart

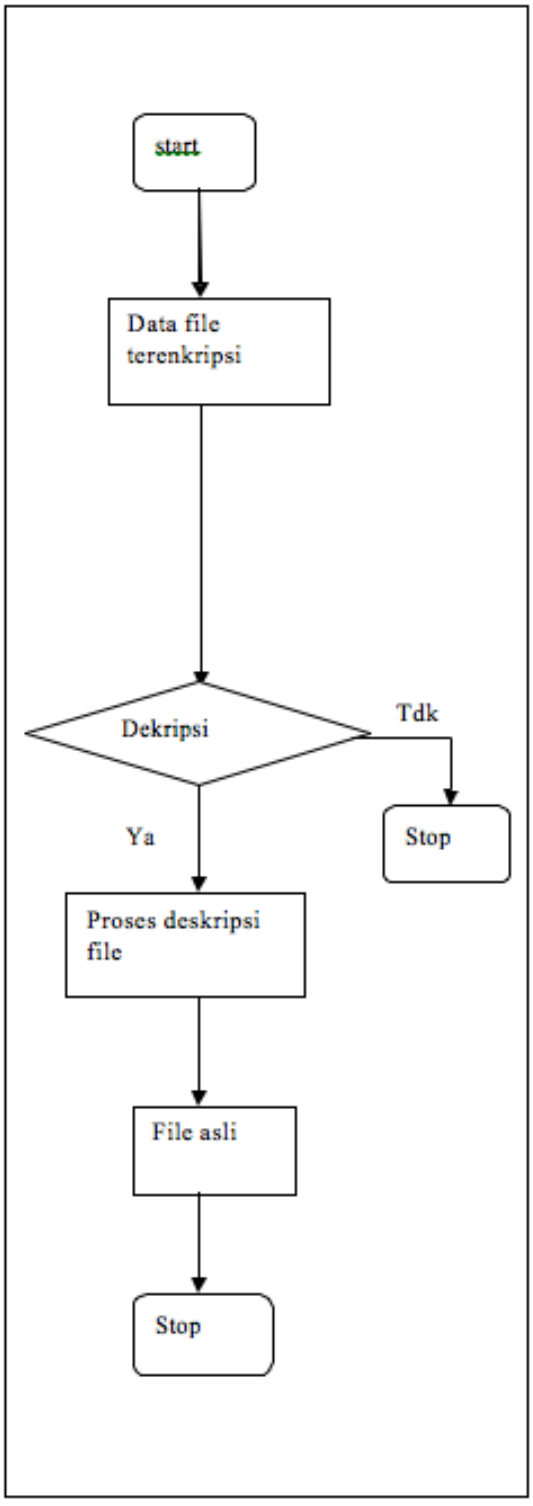
Dalam penelitian ini flowchart dibuat untuk mengetahui dan merancang arah aliran program yang akan dibuat, agar sistem yang dibuat dapat berjalan sebagai mana mestinya dan menghasilkan output berupa hasil dari pengiriman baik itu berupa pesan maupun file yang diinputkan. Dalam penelitian ini proses enkripsi dan dekripsi perpindhan file data baik itu rtf, txt, dan pesan singkat menggunakan salah satu metode kriptografi, yaitu Elgamal. Pada Gambar 1 (a) dan 1

(b) menunjukan proses enkripsi file dan proses dekripsi file. Adapun flowchart proses enkripsi file dan proses dekripsi file adalah sebagai berikut :

 e-ISSN: 2338-5197



Gambar 1 (a) proses enkripsi file



Gambar 1 (b) proses dekripsi file

b. Perancangan Struktur Menu

Sebelum merancang form dan program yang akan dibuat terlebih dahulu dibuat rancangan struktur menu programnya. Tahap ini dilakukan agar diperoleh sistem yang efektif dan efisien sehingga pengguna lebih mudah memakainya.

 e-ISSN: 2338-5197

c. Perancangan Input-Output

Tahap perancangan input-output merupakan tahapan perancangan interface, agar program aplikasi dapat berinteraksi dengan baik dengan user. Sehingga output yang dikeluarkan sesuai dengan harapan yang diinginkan oleh user. Setelah pembuatan struktur menu diatas akan dirancang tiga form, yaitu form utama,form enkripsi,form dekripsi.

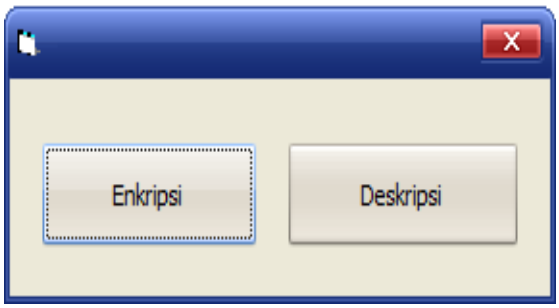
5. IMPLEMENTASI PROGRAM

5.1 Form dan coding

Bahasa pemrograman Visual Basic akan sangat mendukung proses perancangan form yang telah ditentukan sebelumnya. Dalam penelitian ini kita akan menggunakan Visual Basic sebagai compilernya. Dalam pembuatan aplikasi ini diperlukan 3 form seperti yang sudah mmdirencanakan pada rancangan yang ada di atas antara lain adalah form menu utama, form enkripsi dan form dekripsi.

5.2 Menu Utama

Pada menu utama ini memiliki fungsi untuk menampilkan tampilan awal program yang memudahkan penggunanya. Seperti proses enkripsi dan deskripsi yang ada pada pada menu utama, berikut adalah Gambar 2 yang menampilkan tampilan menu utama dari program ini.



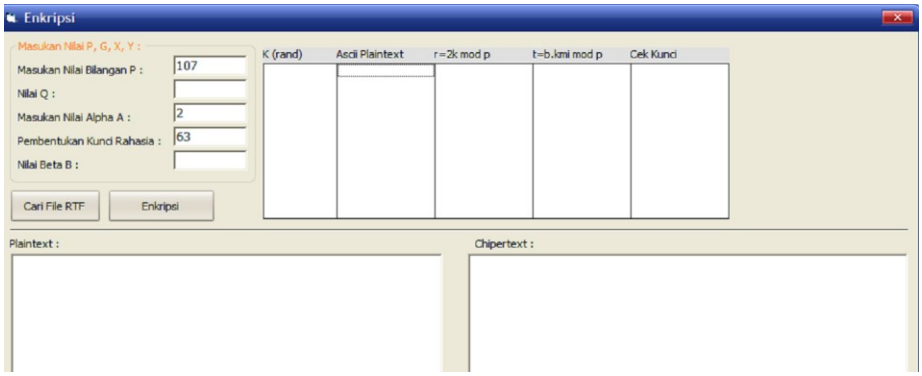
Gambar 2 Tampilan Menu Utama

5.3 Enkripsi perpindahan data file

Selanjutnya pada form enkripsi perpindahan data file digunakan untuk membuka komponen yang ada pada form enkripsi seperti mengenkripsi pesan/file yang sudah di sediakan ada form enkripsi file.

Berikut adalah Gambar 3 tampilan form enkripsi.

 e-ISSN: 2338-5197

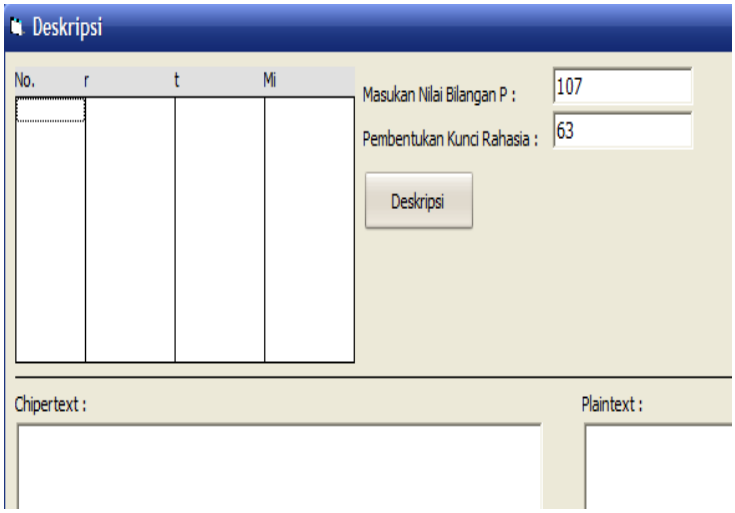


Gambar 3 Tampilan form enkripsi

5.4 Deskripsi perpindahan data file

Sama seperti halnya proses enkripsi pada proses deskripsi akan melalui beberapa fungsi yang ada pada aksi tombol deskripsi yaitu dengan membuka file yang sudah terenkripsi sekaligus mengembalikan file asli yang telah di enkripsi tadi.

Adapun tampilan form dekripsi dapat diliihat seperti Gambar 4 seperti yang ada di bawah ini.



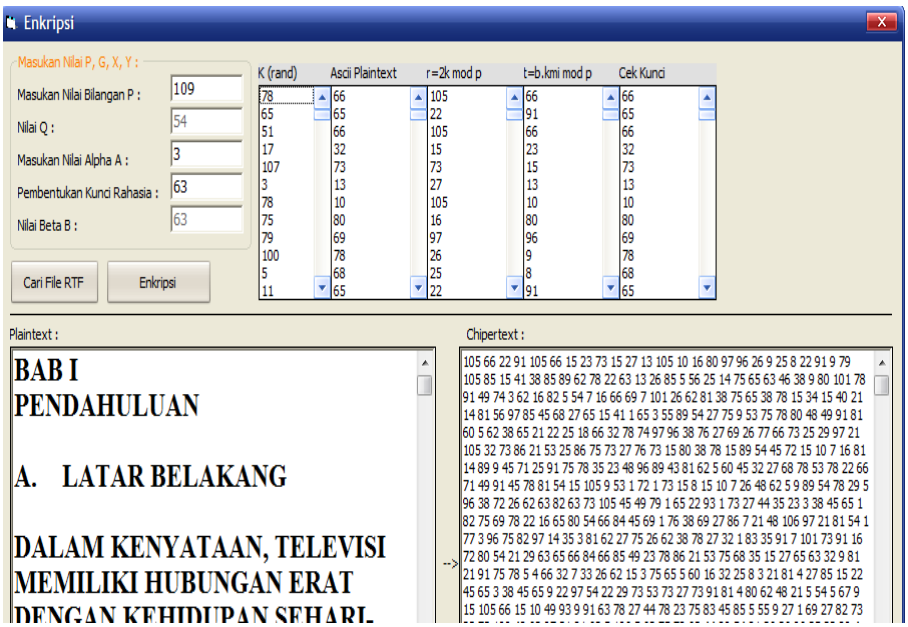
Gambar 4 Tampilan form Dekripsi

6. HASIL PROGRAM

6.1 Form Enkripsi

Langkah yang dilakukan setelah muncul menu utama seperti ini adalah memilih enkripsi untuk menjalankan program ini dengan klik tombol enkripsi maka otomatis akan langsung masuk ke sistem berikutnya. Pada Gambar 5 Tampilan Form Enkripsi adalah sebagai berikut:

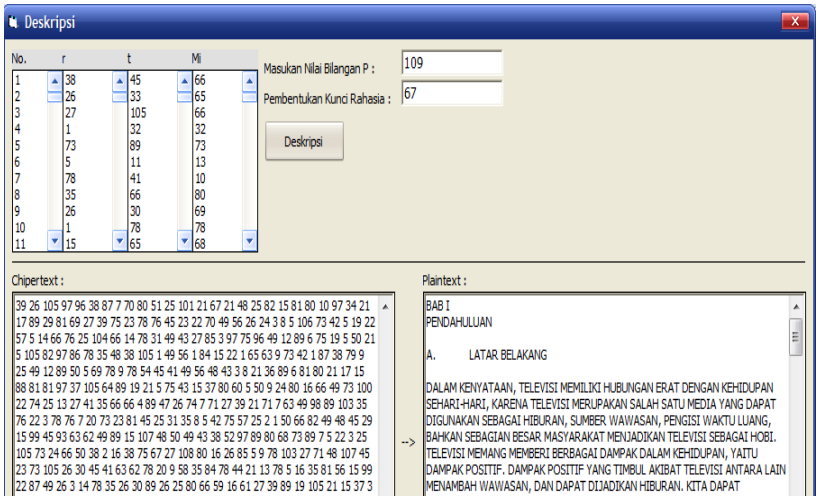
 e-ISSN: 2338-5197



Gambar 5 Tampilan Form Enkripsi

6.2 Form Dekripsi

Selanjutnya adalah ketika selesai mengenkripsi hasil dari enkipsi tadi maka akan langsung beralih ke form Deskripsi. Setelah itu akan menghasilkan Form Deskripsi seperti yang diinginkan, seperti pada Gambar 6 Tampilan Form Dekripsi sebagai berikut :



Gambar 6 Tampilan Form Dekripsi

7. KESIMPULAN

Berdasarkan hasil penelitian dan pebahasan dapat disimpulkan beberapa hal sebagai berikut:

 e-ISSN: 2338-5197

a. Telah dihasilkan suatu aplikasi untuk pengamanan pesan dan file menggunakan bahasa pemrograman Visual Basic dengan proses enkripsi dan deskripsi pada perpindahan data file.
b. Proses pengujian aplikasi menggunakan metode black box test dan alpha test aplikasi diujikan kepada responden, hasilnya adalah proses enkripsi dan deskripsi telah sesuai dengan kaidah algoritma kritografi El-Gamal.
c. Implementasi program ini menghasilkan suatu aplikasi yang dapat mengubah file asli menjadi file terenkripsi yang tidak dapat dibaca isi filenya dan mengembalikannya kembali menjadi file aslinya tanpa merubah dan merusak isi filenya.
d. Implementasi program ini menghsilkan aplikasi yang dapat mengubah data file menjadi kode-kode yang tidak terbaca dan mengembalikan kembali menjadi pesan aslinya.

8. DAFTAR PUSTAKA

[1] (Online) http://informatika.web.id/algoritma-elgamal.htm Diakses tanggal 20 Februari 2010
[2] Ifanto, Mukhammad. 2009. Metode Enkripsi Dan Dekripsi Dengan Menggunakan Algoritma Elgamal. Bandung: Institut Teknolgi Bandung.
[3] Ariwibowo, Eko. 2008. Aplikasi Pengamanan Dokumen Office Dengan Algoritma Kriptografi Kunci Asimetris ElGamal. Yogyakarta : Universitas Ahmad Dahlan Yogyakarta.
[4] Sapty Rahayu .2005. Cryptografi (e-book online) http://cryptografi/124p/04/final0.1.
[5] Ariyus, Dony " Pengantar Ilmu Kriptografi" Penerbit Andi 2008.
[6] Pratama, Satya Fajar. 2007. " Algoritma Elgamal untuk keamanan Aplikasi e-mail " Program Studi Teknik Informatika, Institut Teknologi Bandung.
[7] Munir, Rinaldi. 2004. Algoritma RSA dan ElGamal. (online) http://www.alg2.kriptografi/if5054/398/88/. Diakses tanggal 2 Juli 2009 Rinaldi, Munir " Kriptografi " Penerbit Informatika oktober 2006.
[8] Sanjaya, Rita Aprilia. 2010. Metode Enkripsi Dan Dekripsi Menggunakan Algoritma ElGamal, S-1. STIKOM . Banyuwangi
[9] LPKBM Matkom Madcoms. 2006. CV. Andi Offset(Andi) Visual Basic 6.0, http;//laporan metopen/Visual Basic 6.0 Komputer.htm
[10] Ladjamudin, Al Bahra Bin. Rekayasa Perangkat Lunak Graha Ilmu, Yogyakarta. 2006