Paper

Aplikasi Keamanan Dokumen Teks Menggunakan Algoritma Triple DES dan Blowfish

Author: Rachmat Aulia, Haida Dafitri

SNASTIKOM Ke 9 Tahun 2022
ISBN: 2964-1950

Aplikasi Keamanan Dokumen Teks Menggunakan Algoritma Triple DES dan Blowfish

Rachmat Aulia[1*], Haida Dafitri[2]
[1,2]Universitas Harapan Medan, Medan, Indonesia
[1]rachmataulia@unhar.ac.id, [2]haidadafitri@unhar.ac.id,

Abstrak

Perkembangan teknologi informasi yang semakin pesat memberikan tantangan besar terhadap keamanan data, informasi, dan media penyimpanannya. Jatuhnya informasi ke tangan pihak yang tidak berhak dapat menyebabkan kerugian bagi pemilik informasi, terutama pada file dokumen teks yang sering digunakan untuk berbagi informasi. Salah satu solusi dalam mengamankan data adalah dengan menerapkan teknik kriptografi, yaitu metode penyandian data yang mengubah informasi asli menjadi bentuk yang sulit dipahami melalui proses enkripsi. Penelitian ini memfokuskan pada penerapan dua algoritma kriptografi simetris, yaitu Triple DES dan Blowfish, untuk meningkatkan keamanan file dokumen teks. Algoritma Triple DES merupakan pengembangan dari algoritma DES dengan melakukan proses enkripsi sebanyak tiga kali sehingga menghasilkan panjang kunci 168 bit, yang lebih aman dibanding pendahulunya. Namun, algoritma ini memiliki kelemahan terhadap serangan key-search attack dan meet-in-the-middle attack. Sementara itu, algoritma Blowfish dikenal memiliki kinerja yang lebih baik dibanding algoritma lainnya dan belum ditemukan kelemahan signifikan dalam keamanannya. Dalam penelitian ini, kombinasi antara algoritma Triple DES dan Blowfish diterapkan dalam aplikasi pengamanan dokumen teks untuk mengatasi kelemahan masing-masing algoritma serta meningkatkan tingkat keamanan data yang dienkripsi. Hasil penelitian diharapkan mampu memaksimalkan peran kedua algoritma dalam proses enkripsi dokumen teks, sehingga data dapat terlindungi dari upaya pembobolan oleh pihak yang tidak berhak.

Kata Kunci: Kriptografi, Triple DES, Blowfish, Enkripsi, Keamanan Data, Dokumen Teks.

Abstract

The rapid development of information technology poses a major challenge to the security of data, information, and its storage media. Information falling into the hands of unauthorized parties can cause losses to the owner of the information, especially in text document files that are often used to share information. One solution to securing data is to apply cryptographic techniques, namely data encoding methods that change original information into a form that is difficult to understand through an encryption process. This study focuses on the application of two symmetric cryptographic algorithms, namely Triple DES and Blowfish, to improve the security of text document files. The Triple DES algorithm is a development of the DES algorithm by carrying out the encryption process three times to produce a key length of 168 bits, which is more secure than its predecessor. However, this algorithm has weaknesses against key-search attacks and meet-in-the-middle attacks. Meanwhile, the Blowfish algorithm is known to have better performance than other algorithms and no significant weaknesses in its security have been found. In this study, a combination of the Triple DES and Blowfish algorithms is applied in a text document security application to overcome the weaknesses of each algorithm and increase the level of security of the encrypted data. The research results are expected to be able to maximize the role of the two algorithms in the process of encrypting text documents, so that data can be protected from hacking attempts by unauthorized parties.

Keywords: Cryptography, Triple DES, Blowfish, Encryption, Data Security, Text Documents

1. PENDAHULUAN

Saat ini berbagai macam teknik digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak terhadap hak akses informasi tersebut, maka diperlukan suatu cara untuk mengamankan data dan informasi. Salah satunya adalah dengan cara merubah data tersebut ke dalam bentuk data yang lain yang tidak dapat dimengerti dalam bentuk penyandian data dengan teknik kriptografi. Perkembangan teknologi informasi yang semakin cepat juga memberikan tantangan terhadap masalah keamanan data, informasi, dan media penyimpananya. Jatuhnya informasi ketangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi tersebut. Terutama pada file-file dokumen teks yang digunakan untuk saling berbagi informasi.

ISBN: 2964-1950

Berdasarkan pada masalah keamanan data yang dapat merugikan pihak yang memiliki otoritas, solusi yang diberikan adalah dengan memanfaatkan sebuah teknik kriptografi. Teknik kriptografi adalah sebuah teknik yang dapat mengacak atau meyandikan sebuah informasi menjadi informasi yang sulit bahkan tidak dipahami melalui sebuah proses yang di namakan dengan enkripsi [1]. Proses enkripsi pada teknik kriptografi mengandalkan sebuah perhitungan algoritma yang telah ditentukan setiap jenisnya. Saat ini banyak bermunculan algoritma kriptografi yang terus dianalisis, dicoba dan disempurnakan untuk mencari algoritma yang dianggap memenuhi standar keamanan. Beberapa algoritma kriptografi yang dikenal antara lain DES, Rijndael, Blowfish, RC4, Affine Cipher ,Vigenere Cipher, Enigma, IDEA dan lainnya. Pada pembahasan skripsi ini algoritma yang dipakai adalah algoritma simetri Triple DES dan Blowfish.

Algoritma Triple DES adalah pengembangan dari algoritma DES, di mana algoritma DES menggunakan panjang kunci 56 bit yang dirasa cukup untuk menjalankan teknik enkripsi yang aman. Tetapi seiring berjalanya waktu kemampuan perhitungan komputer semakin bertambah sehingga menjadikan cara membobol keamanan data dengan cara brute force menjadi lebih mungkin dilakukan. Mengatasi hal tersebut dilakukanya implemantasi algoritma DES sebanyak 3 kali. Proses tersebut menyebabkan panjang kunci menjadi 168 bit, sehingga algoritma Triple DES ini lebih aman dari pendahulunya [2]. Sedangkan penelitian yang dilakukan Thakur dan Kumar dalam menganalisa peforma algoritma Blowfish menyatakan bahwa Blowfish memiliki kinerja yang lebih baik daripada algoritma enkripsi umum lainnya yang digunakan. Akan tetapi setiap algoritma pasti memiliki sebuah kelemahan baik algoritma Triple DES dan Blowfish yang akan diterapkan sebagai pengamanan dokumen teks.

Kelemahan pada algoritma Triple DES dapat diserang menggunakan key-search attack dan exploit known serta cara yang ampuh untuk serangan Triple DES adalah dengan metode meet in the middle attack. Sedangkan pada algoritma Blowfish belum diketahui titik lemah keamananya sejauh ini [3]. Besar kemungkinan serangan-serangan tersebut akan terus dikembangkan sesuai kemajuan teknologi sekarang untuk memecahkan data asli dari cipher kedua algoritma yang dibahas. Oleh karena itu dibutuhkanya kombinasi penerapan algoritma yang akan menambah tingkat keamanan data informasi yang akan dienkrispi.

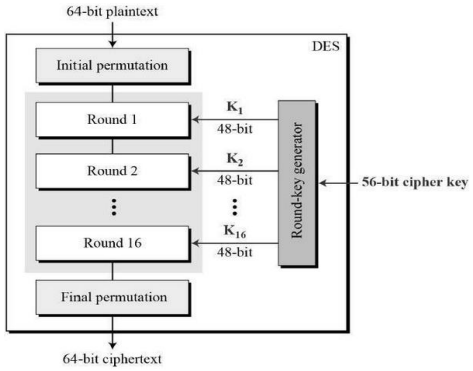
Algoritma Tripe DES pada dasarnya adalah algoritma DES yang diulangi sebanyak 3 kali enkripsi dan dekripsi. Data Encryption Standard (DES) adalah cipher blok simetris-kunci yang diterbitkan oleh National Institute of Standard and Technology (NIST). DES adalah implementasi dari Cipher Feistel. Menggunakan 16 ronde struktur Feistel. Ukuran blok adalah 64-bit. Meskipun, panjang kunci adalah 64-bit, DES memiliki panjang kunci efektif 56 bit, karena 8 dari 64 bit kunci tidak digunakan oleh algoritma enkripsi [4].

DES mentransformasikan input 64 bit dalam beberapa tahap enkripsi ke dalam output 64 bit. DES termasuk block cipher, dengan tahapan dan kunci yang sama, DES digunakan untuk membalik enkripsi. Kunci internal pada algoritma DES dibangkitkan dari kunci eksternal (external key) 64 bit [5].

Tiga tahapan besar dalam DES yaitu:

1. Plaintext yang berukuran 64 bit dipermutasi dengan matriks permutasi awal.
2. Hasil permutasi awal kemudian di-enciphering sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.
3. Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan (invers initial permutation atau IP-1) menjadi blok ciphertext.

Struktur Umum DES digambarkan dalam ilustrasi berikut :



Gambar 1. Struktur DES

Bruce Schneier merancang blowfish pada tahun 1993 sebagai alternatif cepat dan gratis untuk algoritma enkripsi yang ada. Sejak itu telah dianalisis jauh, dan perlahan-lahan mendapatkan penerimaan sebagai algoritma

ISBN: 2964-1950

enkripsi yang kuat. Algoritma Blowfish memiliki banyak kelebihan. Sangat cocok dan efisien untuk implementasi perangkat keras dan tidak ada lisensi yang diperlukan. Operator dasar algoritma Blowfish termasuk pencarian tabel, penambahan dan XOR. Tabel ini mencakup empat tabel S-Box dan P-array. Blowfish menyandikan suatu data berdasarkan putaran Feistel, dan desain fungsi-F yang digunakan berjumlah suatu penyederhanaan prinsip-prinsip yang digunakan dalam DES untuk menyediakan keamanan yang sama dengan kecepatan dan efisiensi yang lebih besar dalam perangkat lunak. Blowfish adalah cipher blok 64 bit dan disarankan sebagai pengganti DES. Blowfish adalah algoritma cepat dan dapat mengenkripsi data pada mikroprosesor 32-bit (Singh dan Singh, 2013).

Enkripsi data terjadi melalui jaringan Feistel 16-putaran. Setiap putaran terdiri dari kunci yang tergantung permutasi, dan substitusi bergantung pada kunci dan data. Semua operasi adalah XOR dan tambahan pada kata-kata 32-bit. Satu-satunya operasi tambahan adalah empat pencarian data array terindeks per putaran (Bruce Schneier).

Subkunci:

Blowfish menggunakan sejumlah besar subkunci. Kunci-kunci ini harus diprediksi sebelumnya enkripsi atau dekripsi data apa pun (Bruce Schneier).

1. P-Array terdiri dari 18 subkey 32-bit yaitu P1,P2….P18.
2. Ada 4 elemen S-Box yang masing-masing terdiri dari 256 entri yaitu:

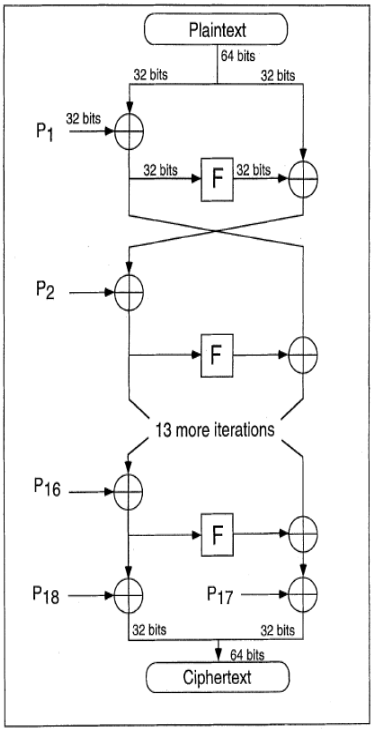
S1,0, S1,1,…..S1,255;

S2,0, S2,1,…..S2,255;

S3,0, S3,1,…..S3,255;

S4,0, S4,1,…..S4,255;

Adapun blok diagram dari enkripsi algoritma Blowfish adalah sebagai berikut :



Gambar 2. Blok Diagram Blowfish

2. METODE PENELITIAN

ISBN: 2964-1950

2.1 Analisis Permasalahan

Keamanan data teks rahasia sangat rentang terhadap penyerangan untuk membocorkan teks tersebut. Apalagi teks rahasia didistribusikan melalui jaringan internet, dimana internet merupakan jaringan publik yang dapat diakses oleh siapa saja. Berdasarkan tersebut dibutuhkan sebuah teknik pengamanan data teks sebelum dikirimkan kepada penerima. Pengamanan data teks rahasia dapat mengandalkan teknik kriptografi. Berdasarkan rumusan masalah pada bab sebelumnya dan paparan di atas, masalah yang terjadi adalah bagaimana sebuah teks rahasia yang belum disandikan dapat diamankan dengan teknik kriptografi sebelum didistribusikan kepada penerima yang berhak. Teknik kriptografi akan mengacak data teks rahasia menjadi data yang tidak dapat dipahami ketika di baca. Metode yang digunakan dalam pembahasan ini adalah sebuah dua algoritma kriptografi simetri yaitu algoritma Triple DES dan Blowfish. Pengamanan data teks rahasia dilakukan dengan proses enkripsi dua kali. Enkripsi pertama plaintext dilakukan dengan algoritma Triple DES sehingga menghasilkan ciphertext pertama, kemudian dilanjutkan dengan enkripsi kedua dengan algoritma Blowfish. Hasil enkripsi algoritma Blowfish merupakan ciphertext akhir yang akan dikirim kepada penerima. Sedangkan proses dekripsi pertama dilakukan dengan algoritma Blowfish, kemudian dilanjutkan dengan dekripsi kedua menggunakan algoritma Triple DES sehingga didapatkan plaintext awal.

2.2 Analisis Enkripsi Algoritma Triple DES

Contoh kasus proses hitungan manual menggunakan algoritma Triple DES. Berikut diuraikan contoh penerapan algoritma TDES dalam menyandikan sebuah teks "HARAPAN1". Pesan akan di konversi ke dalam bentuk bilangan biner terlebih dahulu di mana akan terdiri dari 64 – bit blok teks, proses enkripsi dengan algoritma Triple DES terdiri dari 16 iterasi (putaran). Misalkan dalam satu blok plaintext adalah sebagai berikut :
Plaintext = HARAPAN1
Kunci = wisudaya
Proses enkripsi Triple DES pada pembahasan ini adalah mode E_DES, E_DES, E_DES (EEE) dengan jenis kunci K1=K2=K3.
Secara matematis satu putaran DES dinyatakan sebagai :
Li = Ri-1
Ri = Li-1 f(R1-1,Ki)
Sebelum melakukan proses enkripsi Triple DES, terlebih dahulu membangkitan 16 kunci yang akan dilakukan sebanyak 16 iterasi sebagai berikut :
1. Pembangkitan Kunci Pertama (K1)
Kunci 1 = wisudaya dalam hexadesimal 77, 69, 73, 75, 64, 61, 79, 61
Rubah kunci 1 kedalam biner. Sehingga menghasilkan nilai biner :
01110111 01101001 01110011 01110101 01100100 01100001 01111001 01100001
Generate kunci biner menggunakan tabel permutasi kompresi PC-1 berdasarkan tabel 2.1 bab landasan teori. Kompresi 64 bit menjadi 56 bit dengan membuang 1 bit (parity bit) pada tiap blok kunci DES. Sehingga didapatkan kunci hasil kompresi PC-1 sebagai berikut :
0000000 0111111 1111111 1110100 0000010 1000110 0101000 0101101
Hasil dari kompresi kunci menggunakan tabel PC-1 di pecah menjadi 2 bagian yaitu C0 dan D0.
C0 = 0000000 0111111 1111111 1110100
D0 = 0000010 1000110 0101000 0101101

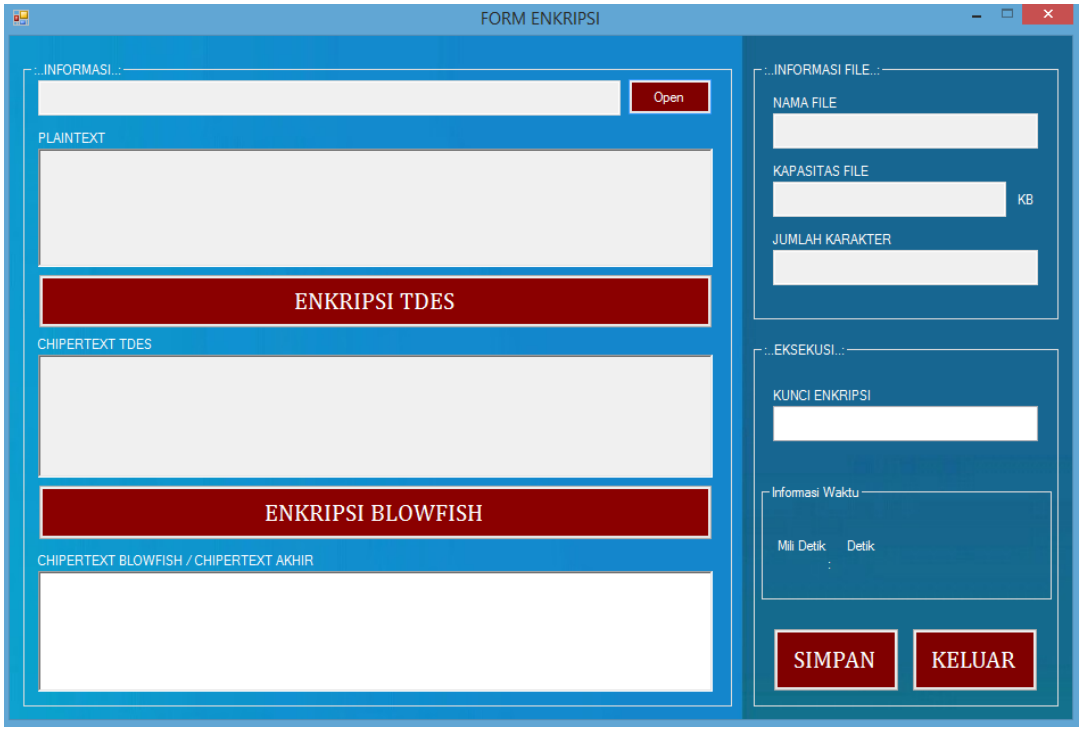
Kemudian lakukan operasi pergesaran kekiri C0 dan D0 menggunakan tabel pergesaran bit dengan 16 puratan.

Iterasi	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Putaran Bit	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

3. HASIL DAN PEMBAHASAN

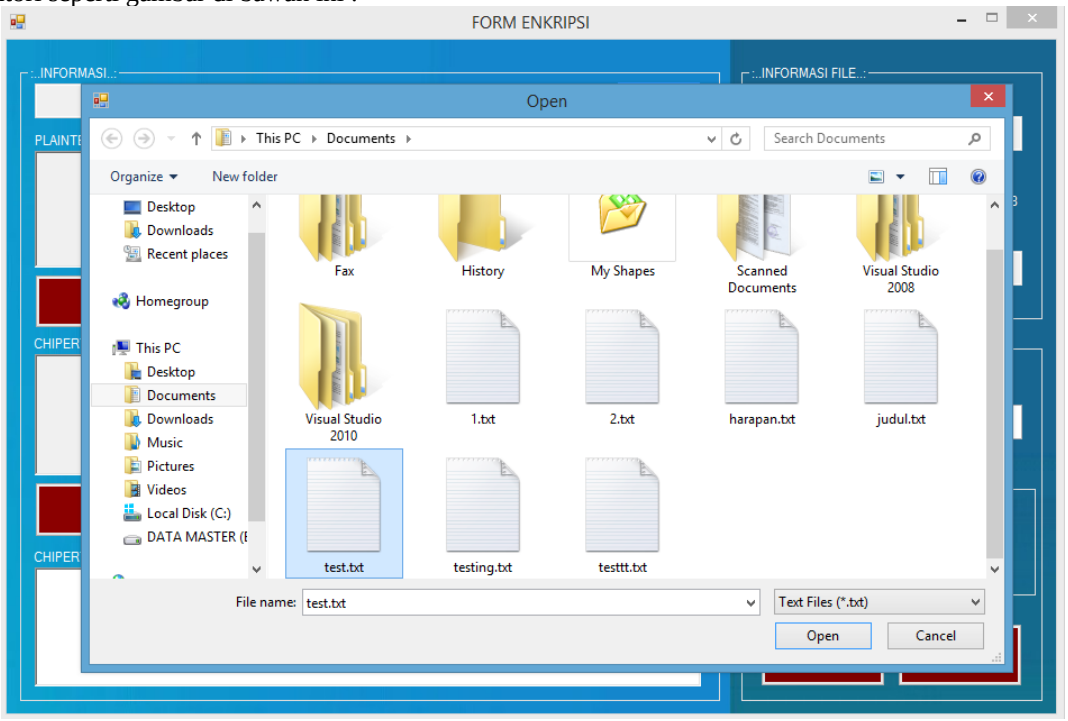
Adapun proses user melakukan enkripsi terdiri dari user melakukan pencarian file text, kemudian melakukan pemasukan kunci enkripsi yang diinginkan, memilih button ENKRIPSI TDES dan dilanjutkan dengan ENKRIPSI BLOWFISH serta proses menyimpan file chipertext hasil enkripsi. Adapun proses tersebut dapat dilihat pada gambar di bawah ini :
1. Memilih File Plaintext
Proses pertama yang dilakukan user didalam form enkripsi adalah melakukan pemilihan file plaintext dengan menekan button Open seperti gambar di bawah ini:

ISBN: 2964-1950



Gambar 3. Proses Memilih File Plaintext

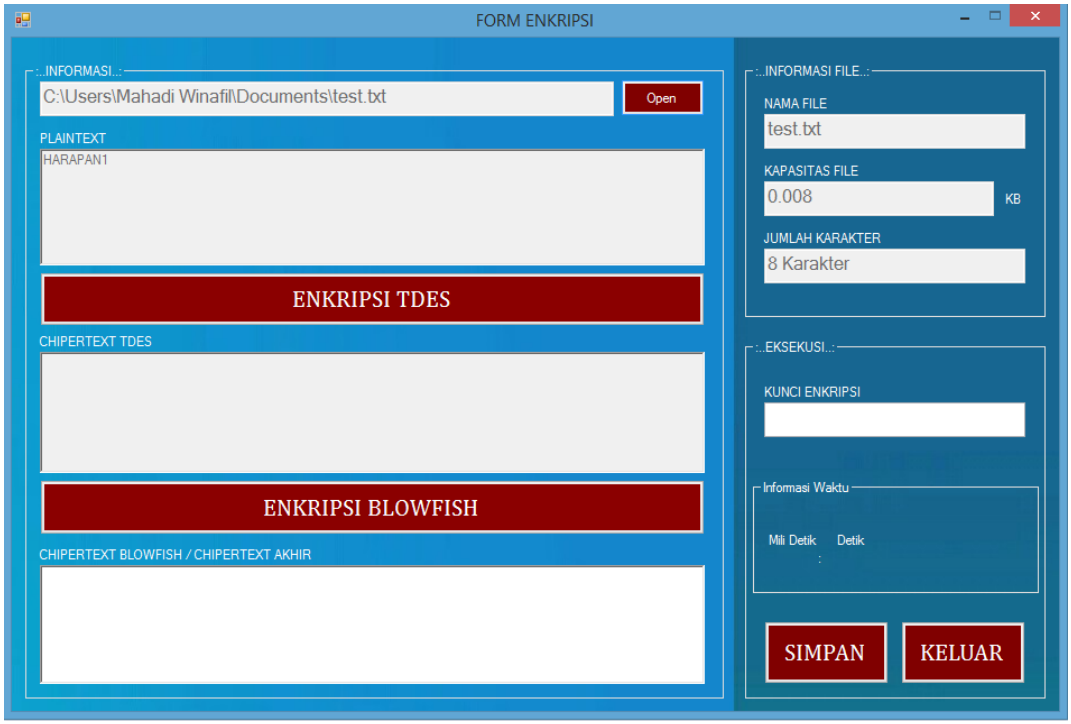
Berdasarkan pada gambar di atas, klik button open untuk menampilkan form pencarian file plaintext pada didirektori seperti gambar di bawah ini :



Gambar 4. Tampilan Form Pencarian Plaintext

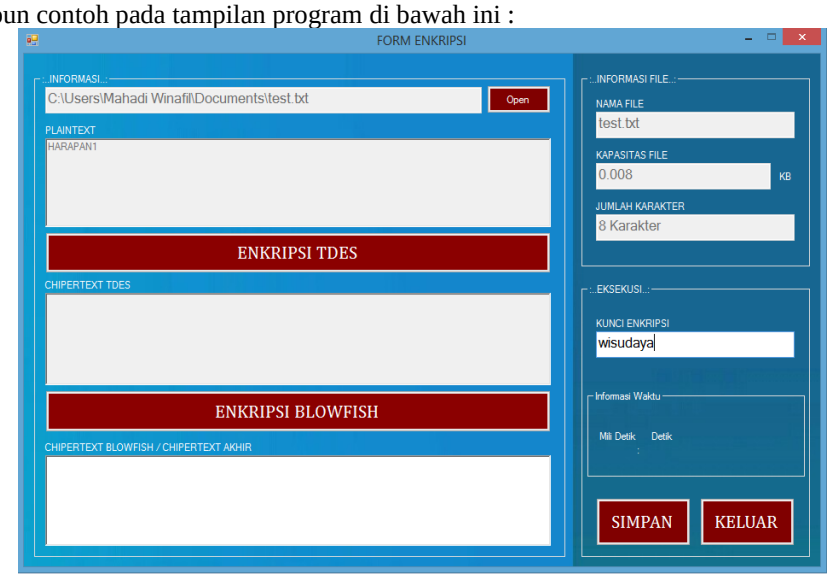
User hanya memilih file text yang akan dienkripsi dan klik button open, sehingga akan tampil informasi isi file text pada textbox seperti gambar di bawah ini :

ISBN: 2964-1950



Gambar 5. Informasi File Plaintext

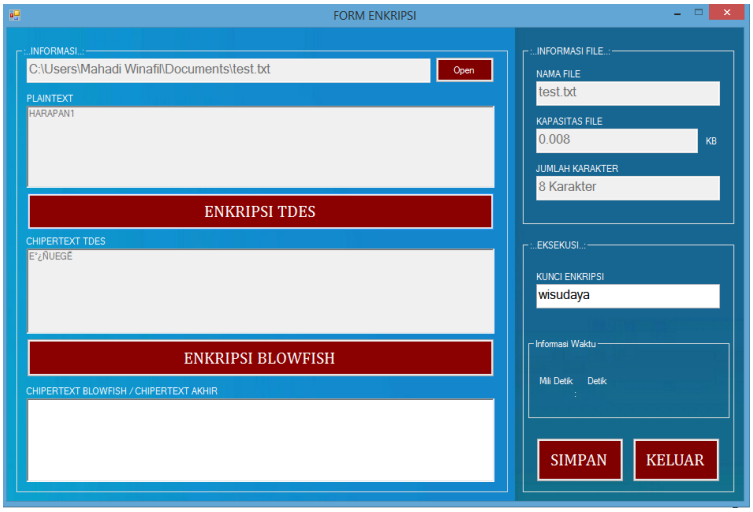
Berdasarkan pada gambar 5 di atas, untuk memulai proses enkripsi terlebih dahulu memasukan kunci yang diinginkan. Adapun contoh pada tampilan program di bawah ini :



Gambar 6. Proses Memasukan Kunci Enkripsi

Proses selanjutnya adalah melakukan enkripsi berdasarkan algoritma Triple DES seperti gambar di bawah ini :

ISBN: 2964-1950



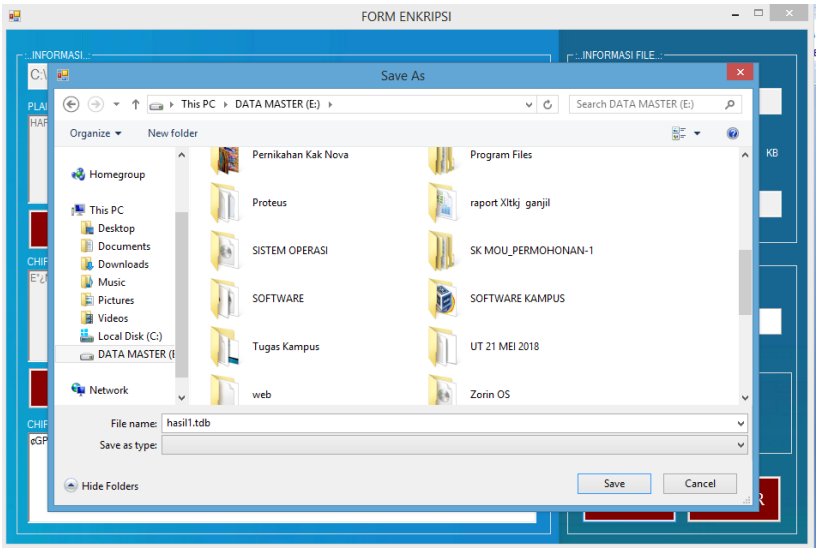
Gambar 7. Enkripsi Berdasarkan Algoritma TDES

Berdasarkan pada gambar di atas, untuk memulai proses enkripsi pertama dilakukan dengan klik button ENKRIPSI TDES, sehingga didapatkan prachipertext Triple DES yang kemudian dilanjutkan pada enkripsi kedua dengan algoritma Blowfish untuk menghasilkan chipertext akhir seperti gambar di bawah ini :

Gambar 9. Enkripsi Berdasarkan Algoritma Blowfish

Berdasarkan pada gambar 4.7 di atas, untuk memulai proses enkripsi kedua dilakukan dengan klik button ENKRIPSI BLOWFISH, sehingga didapatkan chipertext akhir.

Hasil enkripsi dapat disimpan dengan melakukan meklik button SIMPAN seperti gambar di bawah ini :



Gambar 10. Proses Penyimpanan Chipertext

Dari beberapa proses pengujian sistem aplikasi, adapun hasil pengujian tersebut dapat dilihat pada tabel di bawah ini :

Tabel 1. Hasil Pengujian Enkripsi

No	Panjang Karakter	Waktu Enkripsi (Second)	Keterangan
1	8 Karakter	0,3 MiliDetik	Berhasil Enkripsi
2	150 Karakter	1,2 Detik	Berhasil Enkripsi
3	350 Karakter	3 Derik	Berhasil Enkripsi

4. KESIMPULAN

Berdasarkan hasil dari implementasi sistem yang telah dilakukan pada bab sebelumnya, dapat diambil kesimpulan bahwa:

1. Proses Enkripsi dan dekripsi berhasil dilakukan dengan baik pada file teks dengan format .txt menggunakan algoritma Triple DES dan Blowfish.
2. Pada hasil enkripsi berupa chipertext, program berhasil menyamarkan plaintext kedalam bentuk string yang tidak dapat dibaca dan dipahami, sehingga manusia tidak memahami artinya.
3. File teks dengan string yang terlalu panjang tidak dapat didekripsi dengan baik oleh algoritma Blowfish, hal ini dikarenakan banyak string yang terbuang disaat algoritma blowfish mengenkripsi chipertext hasil enkripsi Triple DES.
4. Waktu yang dibutuhkan untuk proses enkripsi dan dekripsi file bervariasi. Hal ini dipengaruhi oleh panjangnya karakter file yang diinputkan.

DAFTAR PUSTAKA

[1] R. Munir, *Kriptografi*. Bandung: INFORMATIKA, 2006.

[2] A. Wijaya and A. Gunawan, “Penggunaan QR Code Sarana Penyampaian Promosi Dan Informasi Kebun Binatang Berbasis Android,” *Bianglala Inform.*, vol. Vol.4, no. No.1, pp. 16–21, 2016, [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/Bianglala/article/viewFile/586/477

[3] J. Thakur and N. Khumar, “DES, AES ad Blowfish: Symmetric Key Cryptography Algorithm Simulation Based Performance Analysis,” vol. 1, 2011.

[4] Mohtashim, “Triple DES.” Accessed: Apr. 10, 2014. [Online]. Available: https://www.tutorialspoint.com/cryptography/triple_des.htm

[5] R. Primartha, "Penerapan Enkripsi dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)," *Sist. Inf.*, vol. 3, 2011.

[6] P. Singh and K.Singh, "Image Encryption And Decryption Using Blowfish Algorithm In Matlab", International Journal of Scientific & Engineering Research, Vol. 4, pp.150-154, 2013

[7] S. Prabowo, (2018, Jan,2). Kriptografi-Jenis Jenis Serangan dalam Kriptografi [online]. Available:http://www.sigitprabowo.id/2013/01/kriptografi-jenis-jenis-serangandalam.html

[8]Stefano, (2016, Apr.7). Algoritma 3DES (Triple Data Encryption Standard) Available:https://piptools.net/algoritma-3des-triple-data-encryption-standard