PERANCANGAN DAN IMPLEMENTASI CRYPTOGRAPHY DENGAN METODE ALGORITMA RC4 PADA TYPE FILE DOCUMENT MENGGUNAKAN BAHASA PEMROGRAMAN VISUAL BASIC 6.0

Ruri Hartika Zain, S. Kom, M. Kom*)

Dosen Tetap Universitas Putra Indonesia YPTK Padang
Padang – Sumatera Barat – Indonesia - 2012

Abstrak

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Terdapat banyak sekali ancaman – ancaman dari luar (outdoor), maupun ancaman dari dalam (backdoor) yang mengancam keamanan data yang disimpan pada storage device (alat penyimpanan data). Berdasarkan latar belakang masalah diatas, maka dibuat suatu sistem kriptography file menggunakan metode RC4. Analisa dan perancangan sistem kriptography dengan metode RC4 tersebut dilakukan terhadap kompleksitas algoritma pada ukuran file (space) dalam melakukan kriptography pada tipe file document. Sistem ini dibangun dengan tujuan menganalisa kompleksitas algoritma RC4 berdasarkan ukuran dalam proses kriptography. Algoritma RC4 mampu melakukan proses enkripsi dan dekripsi data, dan sekaligus mampu melakukan encode dan decode file sehingga file yang dienkripsi tersebut terdapat perubahan. Untuk tipe file document tersebut, "Semakin besar ukuran file yang akan dienkripsi, maka persentase perbedaan dengan besar ukuran file hasil enkripsi semakin kecil".

Keyword: *Criptography. Keamanan data dan RC4*

1. PENDAHULUAN

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Dalam hal ini sangat terkait dengan betapa pentingnya pesan, data, atau informasi tersebut oleh pihak atau orang yang berkepentingan, apakah pesan, data, atau informasi masih *autentikasi*. DAS (*Direct Attached Storage*) adalah tempat penyimpanan seluruh dokumen data yang ada. Di daerah DAS ini dijadikan objek yang selalu ingin di bobol oleh orang yang tidak diinginkan, seperti para *crecker* (perusak/pembobol keamanan jaringan). Pencurian/pembobolan data akan terjadi jika tidak ada pengamanan yang baik. Pembobolan data tersebut dapat berupa mencari suatu rahasia dokumen penting, merusak sistem informasi administrasi, dan masih banyak hal terjadi lagi. Untuk menghindari semua itu langkah yang harus dilakukan adalah dengan menggunakan sebuah aplikasi keamanan *cryptography* seperti penggunaan RC4 ini, agar data tersebut dapat terus terjaga dan aman. Berdasarkan latar belakang masalah di atas, maka akan dibuat suatu *criptography file* menggunakan metode RC4.

2. LANDASAN TEORI

2.1 Keamanan

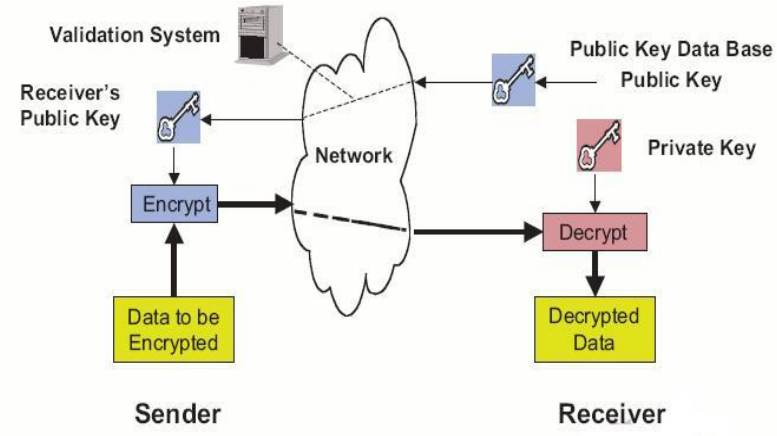
Keamanan adalah keadaan bebas dari bahaya. Istilah ini dapat digunakan dengan hubungan kepada kejahatan, dan segala bentuk kecelakaan. Keamanan merupakan topik yang luas termasuk keamananan nasional terhadap serangan *teroris*, keamanan komputer

terhadap *crecker*, keamanan rumah terhadap maling dan penyelusup lainnya, keamanan *finansial* terhadap kehancuran ekonomi dan banyak situasi berhubungan lainnya (Kristianto, 2003).

2.2 *Criptography*

Criptography berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *cripto* dan *graphia*. *Cripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. *Criptography* adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta *autentikasi* data (Menezes, Oorschot and Vanstone, 1997).

Criptography dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain.

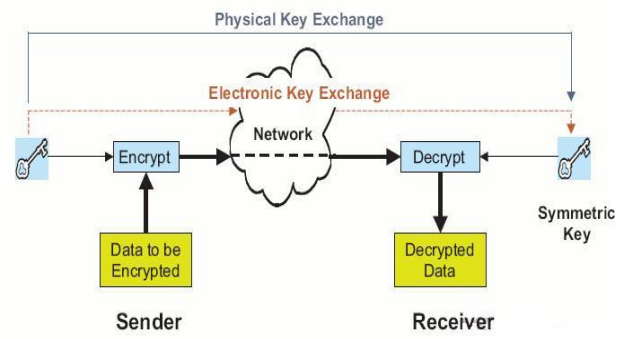


Gambar 2.1 Diagram Blok *Criptography* Simetrik

Kategori *criptography* simetris mempunyai kelebihan pada kecepatan proses datanya, juga sangat baik digunakan untuk mengamankan enkripsi data berkecepatan tinggi.

1. *Criptography* Asimetrik (Kunci–Publik)

Criptography asimetrik menggunakan dua buah kunci yang berbeda, satu buah untuk enkripsi dan satu buah untuk dekripsi, dimana kunci untuk enkripsi bersifat terbuka atau publik, sedangkan untuk dekripsi bersifat rahasia atau pribadi. Kunci publik disimpan dan didistribusikan oleh pihak yang berwenang yaitu CA (*Certified Authorizied*), dimana kumpulan dari CA adalah *Public Key Infrastruktur* (PKI). Maka katagori ini sering disebut PKI *cryptographic*. Sedangkan kunci pribadi disimpan tidak disebarkan.



Gambar 2.2 Diagram Blok *Criptography* Simetrik

Katagori *criptography* ini mempunyai kelebihan jumlah kunci sebanyak *criptography* simetrik, dan tidak membutuhkan saluran khusus untuk pertukaran kuncinya tetapi mempunyai kekurangan pada masalah kecepatan proses *cripto* data–nya.

2. *Criptography* Fungsi HASH (Satu Arah).

Fungsi HASH satu arah merupakan yang menyingkat data dan merepresentasikan menjadi bit–bit dengan menggunakan fungsi matematika untuk mengambil *input* panjang variabel dan mengubahnya kedalam urutan biner dengan panjang yang tetap. Fungsi HASH satu arah dirancang dengan kompleksitas yang tinggi, sehingga apabila terjadi perubahan satu bit saja, maka dapat mengubah nilai dari HASH yang dihasilkan. Untuk HASH yang modern menghasilkan panjang 128 bit atau lebih. Fungsi HASH ini banyak digunakan pada proses *digital signiture* untuk *data integrity*. Salah satu kegunaan Fungsi HASH yaitu untuk MAC (*Message Authentication Code*) dan HMAC yaitu kode yang dihasilkan oleh fungsi HASH untuk sebuah pesan atau data pada jaringan komputer.

2.3 Kunci Simetris

Secara umum dalam proses enkripsi dan dekripsi pada kunci simetris dikenal dua macam *cipher* berdasarkan cara kerja penyandiannya, yaitu:

1. *Stream Cipher*. *Stream cipher* adalah suatu sistem dimana proses enkripsi dan dekripsinya dilakukan dengan cara bit per bit. Pada sistem ini aliran bit kuncinya dihasilkan oleh suatu pembangkit bit acak.

2. *Block Cipher*. Sistem *block cipher* mengkodekan data dengan cara membagi *plaintext* menjadi per blok dengan ukuran yang sama dan tetap. Kemudian setiap bloknya dienkripsi atau didekripsi sekaligus.

2.4 Mekanisme Algoritma RC4

RC4 merupakan salah satu jenis *stream cipher*, yaitu memproses unit atau input data, pesan atau informasi pada satu saat. Unit atau data pada umumnya sebuah *byte* atau bahkan kadang kadang bit (*byte* dalam hal RC4). Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah *input* data, pesan atau informasi tertentu sebelum diproses, atau menambahkan *byte* tambahan untuk mengenkrip.

3. ANALISA DAN PERANCANGAN

3.1 Analisa Algoritma *Criptography* Untuk Tipe *File Document*

Tipe *file* ada 6 tipe yang terdiri dari *graphics, document, archive, multimedia, email, database* dan *finansial.* Tipe *graphics* merupakan tipe *file* yang berupa gambar atau *image* seperti .jpg, .JPEG, .tif, .bmp. Tipe *document* merupakan tipe *file* yang berupa *text* seperti .doc, .pdf, .xls, .rif. Tipe *archive* merupakan tipe *file* yang berupa *kompres* data seperti .rar, .zip. Tipe *multimedia* merupakan tipe *file* yang berupa *audio* dan *video* seperti .mp3, .mp4, .mpeg, .3gp, .DAT. Tipe *email* merupakan tipe *file* yang berupa *file* email seperti .pst. Sedangkan tipe *database* dan *finansial* merupakan tipe *file* yang berupa *database* seperti .mdb, .frx.

3.2 Analisis Algoritma RC4 Berdasarkan Ukuran *File* terhadap *Criptography* Pada *File Document*

Perhitungan matematis algoritma untuk menentukan efisiensi algoritma berdasarkan besar file. Analisa Algoritma RC4 Berdasarkan Ukuran *File* Terhadap *Criptrography*. Pada umumnya, algoritma kompresi data melakukan penggantian satu atau lebih *symbol input* dengan kode tertentu. Berbeda dengan cara tesebut, RC4 menggantikan satu deretan *symbol input* dengan sebuah bilangan *floating point*. Semakin panjang dan semakin kompleks pesan yang dikodekan, semakin banyak bit yang diperlukan untuk keperluan tersebut.

3.3. Model Persoalan

Berdasarkan analisa yang penulis tulis maka akan dijelaskan lebih lanjut dengan contoh. Penulis akan mengambil satu contoh pada bab ini berdasarkan hasil analisa, yaitu:

3.3.1 Analisis Algoritma *Criptography* Untuk Tipe *File Document* Dengan Algoritma RC4

Untuk menunjukkan algoritma RC4 dari langkah–langkah analisa pada sub bab 2.6.1 tersebut, akan digunakan 4-bit kunci untuk menyederhanakannya. Ciptakan 4 *byte* state *array*, S_i, terdiri dari angka-angka 0 s/d 3.

3.3.2 Analisis Perbandingan Terhadap Ukuran *File* Algoritma RC4

Dari langkah–langkah analisa pada sub bab 2.6.2, algoritma RC4 berdasarkan ukuran *file* adalah sebagai berikut:

1. Tentukan *inteval* karakter yang diinisialisasikan [0…1]
2. Dari interval tentukan subinterval dari karakter yang akan di kompresi untuk melakukan proses kompresi dan dekompresi dengan cara:
   a. Tentukan *probabilitas*/frekuensi kemunculan karakter berdasarkan urutan kode ASCII

Tabel 3.1 *Probilitas*/Frekuensi Kemunculan Karakter

Karakter	Probabilitas
A	2/10
E	2/10
I	1/10
K	1/10
L	1/10
M	1/10
T	2/10

   b. Tentukan *range* tiap karakter untuk memperoleh hasil *encode* dengan menjalankan algoritma *encode.*

   Setelah *probabilitas* tiap karakter diketahui. Tiap simbol/karakter akan diberi *range* tertentu yang nilainya berkisar antara 0 dan 1, sesuai dengan probabilitas yang ada. Pada algoritma ini tidak ada ketentuan urutan penentuan segmen, asalkan antara *encode* dan *decode* melakukan hal yang sama.

Tabel 3.2. Range Karakter

Karakter	*Probabilitas*	*Range*
A	2/10	0.00 – 0.20
E	2/10	0.20 – 0.40
I	1/10	0.40 – 0.50

K	1/10	0.50 – 0.60
L	1/10	0.60 – 0.70
M	1/10	0.70 – 0.80
T	2/10	0.80 – 1.00

Setelah menentukan *range* dari setiap karakter, lakukan proses *encode* dengan menggunakan algoritma.

3.4 Perancangan Simulasi Algoritma RC4

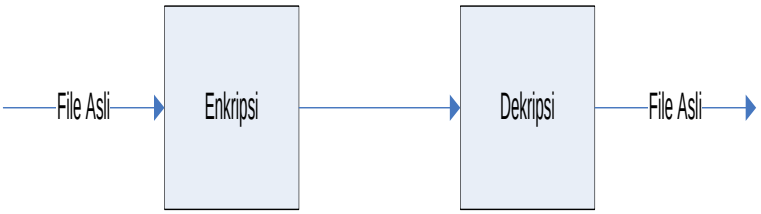
Perancangan simulasi algoritma RC4 terdiri dari deskripsi umum perangkat lunak, deskripsi umum sistem, analisis kebutuhan sistem, analisis *user* dan *output*, deskripsi fungsional, DFD, diagram alir proses, dan perancangan antar muka.

3.4.1 Deskripsi Umum Perangkat Lunak

Berikut ini akan dijelaskan tentang hasil analisis deskripsi umum perangkat lunak diantaranya deskripsi umum system, deskripsi umum kebutuhan, analisis *input* dan *output*, dan diagram alir pemrosesan algoritma RC4.

3.4.2 Deskripsi Umum System

Sistem ini bertujuan untuk memberikan gambaran yang jelas mengenai implementasi algoritma RC4 dengan melakukan perbandingan terhadap berbagai tipe *file*.



Gambar 3.1 Dekripsi Umum System

3.4.3 Fungsi Produk

Aplikasi yang akan dikembangkan dan akan dibuat memiliki fungsi utama yaitu: Dapat melakukan proses enkripsi *file* untuk berbagai *type* dan dapat pula melakukan proses dekripsi sesuai dengan mekanisme.

3.4.4 Analisis Kebutuhan Sistem

Analisis kebutuhan sistem terdiri dari analisis kebutuhan perangkat keras, analisis kebutuhan perangkat lunak.

4. IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi Sistem

Implementasi merupakan tahap dimana sistem/aplikasi siap untuk dioperasikan pada keadaan yang sebenarnya sesuai dari hasil analisis dan perancangan yang telah dilakukan, sehingga akan diketahui apakah sistem/aplikasi yang dirancang benar – benar dapat menghasilkan tujuan yang ingin dicapai.

4.1.1 Pengertian dan Tujuan Implementasi

Implementasi merupakan tahap kelanjutan dari tahap penyeleksian rancangan setelah didesain. Pada tahap ini menerapkan sistem/aplikasi yang didesain kebahasa pemrograman yang sesuai,sehingga akan diperoleh hasil yang diinginkan.

Tujuan implementasi antara lain :

1. Menyelesaikan desain sistem/aplikasi yang ada dalam dokumen

perancangan yang telah disetujui.

2. Menguji dan mendokumentasikan progam – program atau prosedur – prosedur dari dokumen perancangan sistem/aplikasi yang telah disetujui.
3. Memastikan bahwa pemakai dapat mengoperasikan sistem/aplikasi.
4. Mempertimbangkan bahwa sistem/aplikasi memenuhi permintaan pengguna (user) yaitu dengan menguji secara keseluruhan.
5. Memastikan bahwa konversi ke sistem/aplikasi yang baru berjalan dengan benar yaitu dengan membuat rencana, mengontrol aplikasi.

Langkah – langkah yang dibutuhkan dalam implementasi sistem/aplikasi adalah sebagai berikut ini :

1. Menyelesaikan rancangan sistem/aplikasi
2. Mendapatkan hardware dan software yang sesuai.
3. Menguji, mengontrol dan mendokumentasikan program komputer.
4. Memilih dan melatih pemakai (traning user).
5. Menyelesaikan buku manual pemakai (manual book).
6. Menguji sistem/aplikasi.
7. Mendapatkan persetujuan.

4.1.2 Perancangan Lingkungan Implementasi

Pada prinsipnya setiap desain sistem/aplikasi yang telah dirancang memerlukan sarana pendukung yaitu berupa peralatan – peralatan (*hardware*) yang sangat berperan dalam menunjang penerapan sistem/aplikasi yang telah didesain terhadap pengolahan data. Komponen – komponen yang dibutuhkan antar lain *hardware*, yaitu kebutuhan perangkat keras komputer dalam pengolahan data kemudian *software*, yaitu kebutuhan akan perangkat lunak berupa sistem/aplikasi untuk mengoperasikan sistem/aplikasi yang telah didesain.

4.1.4 Hasil Implementasi

Hasil analisis dan perancangan yang telah dipindahkan ke kode program menghasilkan sebuah aplikasi yang dibuat dalam program dan antar muka pada RC4.

4.1.4.1 Antarmuka Menu Utama RC4

Form RC4 File Encription merupakan tampilan untuk membuat *project* baru. *Form* ini berisikan fasilitas menu *editor* yang terdiri dari *file, kunci, Encode*, dan menu *tentang*. Pada *form* ini terdapat juga *image list* dan *toolbar*. *Toolbar* ini berisikan *image list* yang membantu atau untuk mempermudah pengaksesan suatu fungsi secara cepat. Pada intinya fungsi *toolbar* ini sama halnya pada menu *editor* tersebut.

4.2 Pengujian

Pengujian merupakan salah satu tahap didalam menemukan kesalahan – kesalahan program yang mungkin terjadi. Sebelum program diaplikasikan terlebih dahulu harus melalui pengujian agar kesalahan dapat diminimalisasikan sekecil mungkin.

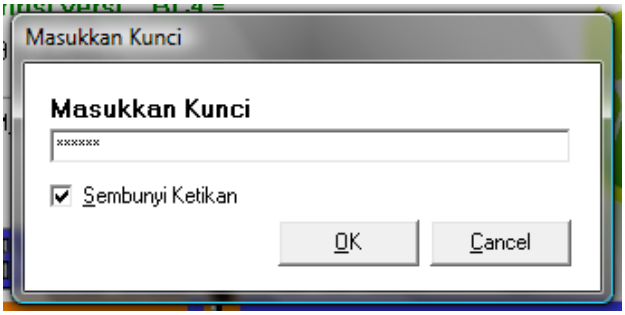
Penulis akan mengujikan salah satu tipe file yaitu file .pdf dengan nama file cryptography.pdf yang besar filenya adalah sebesar 207.750 Bytes.

a. Pengujian Terhadap File cryptography.Pdf

Langkah – langkah untuk melakukan pengujian terhadap algoritma RC4 adalah sebagai berikut :

1. Pertama kali sebelum melakukan proses enkripsi terlebih dahulu klik tombol file > select, kemudian pilih lokasi data *file* yang akan dienkripsikan.

2. Untuk melakukan dekripsi, setelah melakukan enkripsi, terakhir yaitu melakukan proses dekripsi. Terlebih klik tombol *file>select* untuk membuka *file* .pdf yang telah dienkripsi.



Gambar 4.1 Proses key Dekripsi

4.3 Hasil Pengujian

Hasil pengujian yang akan ditujukan yaitu hasil pengujian terhadap parameter hasil pengujian terhadap perubahan besar *file*, hasil pengujian terhadap waktu proses enkripsi dan dekripsi.

4.3.1 Hasil Pengujian Terhadap Perubahan Besar File

Perubahan besar *file* tidak terlalu besar, dimana *file* 34.470 *byte* setelah dilakukan proses enkripsi maka ukuran *file* menjadi 32.932 bytes, jadi *file* .pdf berhasil dimampatkan ukurannya menjadi 1.538 bytes atau sebesar 4.46%. selanjutnya dapat dilihat pada tabel 4.1 dan tabel 4.2, dan gambar dibawah ini :

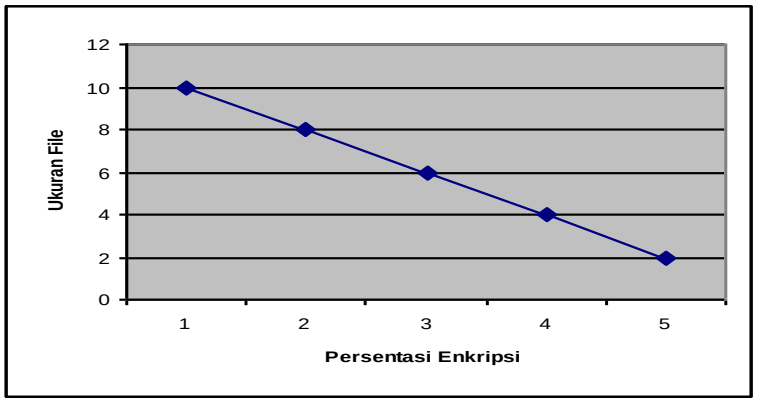
Tabel 4.1 Perubahan besar file hasil proses enkripsi tipe data .pdf

No	Nama File	Data/File Asli	Hasil Enkripsi
1	indonesia	35.069 Bytes	31.266 Bytes
2	Enkripsi_Dekripsi	78.875 Bytes	74.371 Bytes
3	cryptography	207.750 Bytes	205.822 Bytes
4	Aulia_report	580.988 Bytes	576.477 Bytes
5	Standar-ieee8021x	1.189.282 Bytes	1.182.979 Bytes

Tabel 4.2 Presentase Perubahan besar file hasil proses enkripsi tipe data .pdf

No	Nama File	Beda File	Hasil Enkripsi
1	indonesia	3.803 Bytes	10,84 %
2	Enkripsi_Dekripsi	4.503 Bytes	5,71 %
3	cryptography	1.928 Bytes	0,93 %
4	Aulia_report	4.511 Bytes	0,78 %
5	Standar-ieee8021x	6.303 Bytes	0,53 %

Secara grafik, presentase perubahan besar file hasil proses enkripsi dapat dianalogikan sebagai berikut ini :



Gambar 4.2 Grafik Perubahan Besar File tipe data .pdf

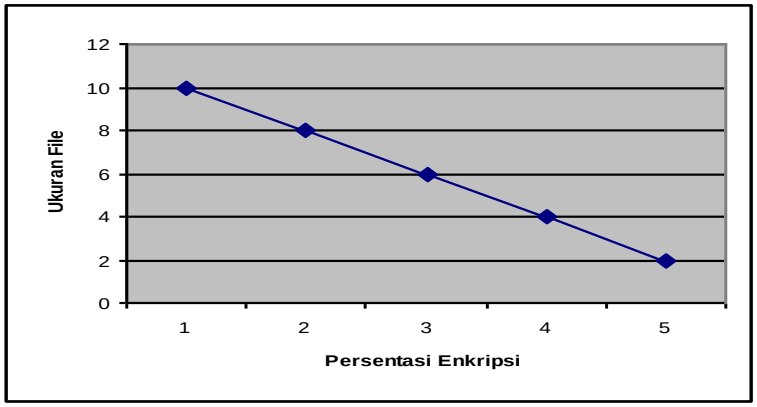
Tabel 4.3 Perubahan besar file hasil proses enkripsi tipe data .xls

No	Nama File	Data/File Asli	Hasil Enkripsi
1	Akuntansi	35.049 Bytes	31.236 Bytes
2	keuangan	78.775 Bytes	74.351 Bytes
3	Rekap gaji	207.761 Bytes	205.812 Bytes
4	Gaji 1	581.111 Bytes	576.467 Bytes
5	Gaji bulan 2	1.189.272 Bytes	1.182.969 Bytes

Tabel 4.4 Presentase Perubahan besar file hasil proses enkripsi tipe data .xls

No	Nama File	Data/File Asli	Hasil Enkripsi
1	Akuntansi	3.883 Bytes	27,85 %
2	Keuangan	4.504 Bytes	6,97 %
3	Rekap gaji	1.929 Bytes	1,83 %
4	Gaji 1	4.514 Bytes	0,51 %
5	Gaji bulan 2	6.303 Bytes	0,28 %

Secara grafik presentase perubahan besar file hasil proses enkripsi tipe data .xls dapat dianalogikan sebagai berikut ini :



Gambar 4.3 Grafik Perubahan Besar File tipe data .xls

Tabel 4.5 Perubahan besar file hasil proses enkripsi tipe data .doc

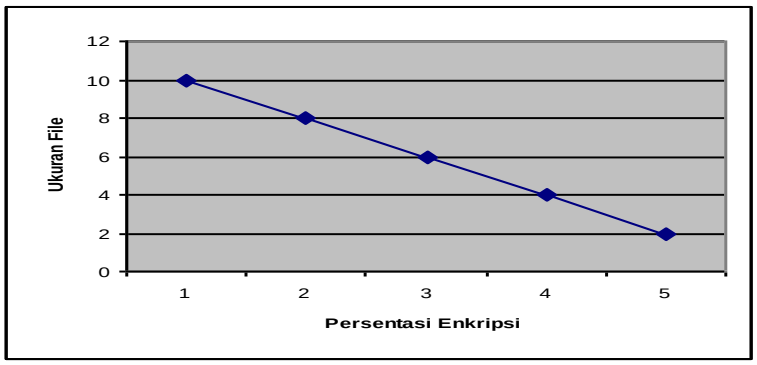
No	Nama File	Data/File Asli	Hasil Enkripsi
1	Telematika	35.069 Bytes	28.213 Bytes
2	Enkripsi-dekripsi	78.875 Bytes	71.343 Bytes

3	Maman-report	207.750 Bytes	119.822 Bytes
4	Daftar symbol	580.988 Bytes	499.476 Bytes
5	Aulia-report	1.189.282 Bytes	1.176.921 Bytes

Tabel 4.6 Presentase Perubahan besar file hasil proses enkripsi tipe data .doc

No	Nama File	Data/File Asli	Hasil Enkripsi
1	Telematika	15.223 Bytes	76,24 %
2	Enkripsi-dekripsi	31.299 Bytes	49,70 %
3	Maman-report	85.311 Bytes	46,16 %
4	Daftar Symbol	383.927 Bytes	31,73 %
5	Aulia-report	512.667 Bytes	24,16 %

Secara grafik presentase perubahan besar *file* hasil proses enkripsi tipe data .doc dapat dianalogikan sebagai berikut ini :



Gambar 4.4 Grafik Perubahan Besar File tipe data .doc

4.4 Kesimpulan Pengujian

Pengujian yang dilakukan dengan mengambil file dengan memilih direktori windows yang dienkripsi, lalu menghasilkan file hasil enkripsi dan mengembalikan hasil semula dengan melakukan proses dekripsi. Proses ini dilakukan dengan algoritma RC4. berdasarkan hasil pengujian RC4 diperoleh kesimpulan sebagai berikut ini :

1. Perubahan Besar *File*. Algoritma RC4 mampu melakukan proses enkripsi dan dekripsi data, dan sekaligus mampu melakukan pengompresan data sehingga data yang dienkripsi tersebut terdapat perubahan.
2. Berdasarkan Tipe File. Berdasarkan pengujian diatas yang telah dilakukan yaitu dengan penggunaan aplikasi/sistem enkripsi dengan metode algoritma RC4, maka diperoleh hasil kesimpulan pengujian sebagai berikut ini
   a. Tipe File .Pdf, maka dapat ditarik sebuah kesimpulan bahwa : ”Semakin besar ukuran file yang akan dienkripsi, maka persentase perbedaan dengan besar ukuran file hasil enkripsi semakin kecil”.
   b. Tipe File .xls, maka dapat ditarik sebuah kesimpulan bahwa : ”Semakin besar ukuran file yang akan dienkripsi, maka persentase perbedaan dengan besar ukuran file hasil enkripsi semakin kecil”. Untuk tipe file .jpg ini juga, semakin besar ukuran file yang akan dienkripsi tersebut, semakin kecil juga perbedaan antara ukuran file asli data yang akan dienkripsi dengan ukuran file yang telah dienkripsi.
   c. Tipe File .doc, maka dapat ditarik sebuah kesimpulan bahwa : ”Semakin besar ukuran file yang akan dienkripsi, maka persentase perbedaan dengan besar ukuran file hasil enkripsi semakin kecil”. Namun untuk tipe file .doc ini, semakin besar

ukuran file yang akan dienkripsi tersebut, maka semakin besar perbedaan antara ukuran file asli data yang akan dienkripsi dengan ukuran file yang telah dienkripsi.

5. PENUTUP

Berdasarkan pembahasan yang dilakukan dari penyusunan tugas akhir ini, dapat diambil kesimpulan sebagai berikut:

a. Algoritma RC4 mampu melakukan proses enskripsi dan deskripsi data, dan sekaligus mampu melakukan pengompresan data sehingga data dienskripsi tersebut terdapat perubahan.
b. Semakin besar ukuran *file* yang akan dienkripsi, maka persentase perbedaan besar ukuran *file* hasil enkripsi semakin kecil.
c. Pada tipe *file document* yang telah dilakukan pengujian sebelumnya, maka letak perbedaan ukuran *file* yang semakin baik adalah pada tipe *file* .doc.
d. Tipe *file* .doc memiliki hemat ukuran *file* yang cukup banyak di bandingkan dengan tipe *file document* lainnya.

DAFTAR PUSTAKA

H.M, Jogiyanto. 1989. Analisa dan Disain Sistem Informasi. Yogyakarta: Andi Offset.

Adi Kurniadi. 1999. *Pemprograman Microsoft visual basic 6.0*. Jakarta: Alex media Komputindo.

Andi Offset, Wahana Komputer Semarang, *Memahami MODEL ENKRIPSI & SECURITY DATA*. Yogyakarta. 2003.

Kristianto, Andi. 2003. *KEAMANAN DATA pada JARINGAN KOMPUTER*. Yogyakarta: Gava Media.