IMPLEMENTASI ALGORITMA RC4 UNTUK PROTEKSI FILE MP3

Kirman

Sistem Informasi, FakultasTeknik, Universitas Muhammadiyah Bengkulu
Jl. Bali Po Box 118 Kota Bengkulu 38119 Indonesia

kirman@umb.ac.id

Abstrak: Beberapa tahun belakangan ini, tingkat pembajakan hak cipta musik dan lagu di beberapa negara di dunia seperti Brazil, Cina, India, Mexico, Pakistan, Indonesia, Paraguay, Rusia, Spanyol, Ukraina mencapai angka yang tinggi. Sebagai contoh di Indonesia sendiri, di tahun 1996 Asosiasi Industri Rekaman Indonesia (ASIRI) mencatat 20 juta keping Compact Disc (CD) album musik bajakan beredar, 12 tahun kemudian atau di tahun 2008 jumlahnya membengkak hingga 550 juta keping. Rasio peredaran album CD musik bajakan dan legal di tahun 2007 bahkan telah mencapai 96% : 4%, angka ini diprediksikan akan terus bertambah . Salah satunya adalah penggunaan *file* berupa *audio digital* yang saat ini cukup populer dan mudah untuk dinikmati, yaitu *file* berformat MP3. Salah satu metode *enkripsi* yang terkenal adalah metode RC4. RC4 pertama kali dibuat oleh Ron Rivest di Laboraturium RSA pada tahun 1987. RC4 (*Rivest Cipher* 4) adalah sebuah *synchrone streamcipher*, yaitu *cipher* yang memiliki kunci simetris dan mengenkripsi *plainteks* secara digit per digit atau *byte* per *byte* dengan cara mengkombinasikan dengan operasi biner (biasanya *XOR*) dengan sebuah angka semiacak. Berdasarkan hasil pembahasan dan pengujian dapat diambil kesimpulan adalah Aplikasi Enkripsi dan Deskripsi dengan algoritma *RC4* menggunakan sistem operasi *windows* 8 yang merubah sistem *windows*32 yaitu bagian *Shell32.* Dokumenter sebut akan dibaca oleh suatu modul baca file masukan yang fungsinya membagi file MP3 kedalam beberapa blok data yang akan diproses oleh modul berikutnya, dimana setiap blok data terdiri atas 64 bit. Dari hasil pengujian yang berekstensi *.mp3 enkripsi dan deskripsi berhasil dilakukan dengan memberikan informasi nama file, ukuran bytes, dan estimasi waktu.
Kata Kunci: Pembajakan, Hak Cipta, Algoritma RC4, MP3

Abstract: ***In recent years, the rate of copyright piracy of music and songs in several countries in the world such as Brazil, China, India, Mexico, Pakistan, Indonesia, Paraguay, Russia, Spain, Ukraine reached high numbers. For example in Indonesia alone, in 1996 the Recording Industry Association of Indonesia (ASIRI) recorded 20 million pieces of Compact Disc (CD) of pirated music albums circulating, 12 years later or in 2008 the number swelled up to 550 million pieces. The distribution ratio of CD albums to pirated and legal music in 2007 has even reached 96%: 4%, this figure is predicted to continue to grow. One of them is the use of files in the form of digital audio that is currently quite popular and easy to enjoy, the file format MP3. One of the well known methods of encryption is the RC4 method. RC4 was first created by Ron Rivest at the RSA Laboratory in 1987. RC4 (Rivest Cipher 4) is a synchronous streamcipher, a cipher that has a symmetric key and encrypts plaintext digitally per digit or byte per byte by combining with binary operations (usually XOR) with a semi track number. Based on the results of the discussion and testing can be concluded is Application Encryption and Description with RC4 algorithm using windows 8 operating system that change sistemwindows32 that is part of Shell32, Documentary call will be read by a module read input file function to divide MP3 file into some data block to be processed by the next module, where each data block consists of 64 bits, From the test results berekstensi * .mp3 encryption and description successfully done by providing information file name, bytes size, and time estimation.***
Keywords: ***Piracy, Copyright, AlgorithmRC4, MP3***

I. PENDAHULUAN

Multimedia dapat diartikan sebagai teknologi yang menggabungkan berbagai sumber media (teks, grafik dan suara) untuk menyampaikan atau membuat sesuatu sebagai perantara atau suatu bentuk komunikasi. Multimedia seringkali

digunakan dalam dunia hiburan. Salah satunya adalah penggunaan *file* berupa *audio digital* yang saat ini cukup populer dan mudah untuk dinikmati, yaitu *file* berformat MP3.

Beberapa tahun belakangan ini, tingkat pembajakan hak cipta musik dan lagu di beberapa negara di dunia seperti Brazil, Cina, India, Mexico, Pakistan, Indonesia, Paraguay, Rusia, Spanyol, Ukraina mencapai angka yang tinggi. Sebagai contoh di Indonesia sendiri, di tahun 1996 Asosiasi Industri Rekaman Indonesia (ASIRI) mencatat 20 juta keping Compact Disc (CD) album musik bajakan beredar, 12 tahun kemudian atau di tahun 2008 jumlahnya membengkak hingga 550 juta keping. Rasio peredaran album CD musik bajakan dan legal di tahun 2007 bahkan telah mencapai 96% : 4%, angka ini diprediksikan akan terus bertambah . Salah satunya adalah penggunaan *file* berupa *audio digital* yang saat ini cukup populer dan mudah untuk dinikmati, yaitu *file* berformat MP3 [1].

File MP3 selain memberi kemudahan dalam penyebaran, juga memberi kemudahan dalam penggandaan. Kemudahan tersebut akhirnya dapat digunakan secara negatif tanpa memperhatikan aspek hak cipta. *File* MP3 yang seharusnya menjadi properti legal dari produsen dan secara legal dimiliki oleh orang yang telah membelinya bisa dengan mudah disalahgunakan oleh pihakpihak yang tidak bertanggung jawab. Untuk itu diperlukan suatu cara untuk memproteksi *file* tersebut, salah satunya adalah dengan enkripsi. *File* MP3 yang telah terenkripsi tidak dapat diputar/dimainkan dengan sempurna sehingga diperlukan aplikasi untuk mendekripsi *file* tersebut agar dapat dimainkan seperti semula.

Salah satu metode *enkripsi* yang terkenal adalah metode RC4. RC4 pertama kali dibuat oleh Ron Rivest di Laboraturium RSA pada tahun 1987. RC4 (*Rivest Cipher* 4) adalah sebuah *synchrone streamcipher*, yaitu *cipher* yang memiliki kunci simetris dan mengenkripsi *plainteks* secara digit per digit atau *byte* per *byte* dengan cara mengkombinasikan dengan operasi biner (biasanya *XOR*) dengan sebuah angka semiacak [2].

RC4 merupakan metode enkripsi tercepat dibandingkan dengan DES, Triple DES, Blowfish-256, AES-128, dan AES-256. RC4 memiliki banyak kelemahan antara lain, tingginya peluang untuk menghasilkan array S yang sama ataupun berulang dan *Bit-Flipping Attack*. Akan tetapi bisa diatasi dengan memperbanyak bit kunci, mengubah cara pengisian *K-array*, menggunakan IV dalam setiap kunci, serta mengacak plainteks sebelum dienkripsi untuk mencegah terjadinya bit-flipping attack [3].

II. LANDASAN TEORI

A. Algoritma

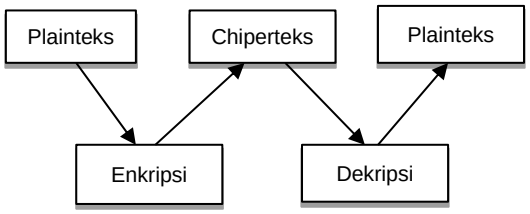
Algoritma adalah urutan langkah-langkah yang dinyatakan dengan jelas dan tidak rancu untuk memecahkan suatu masalah (jika ada pemecahannya) dalam waktu rentang tertentu. Artinya, setiap langkah harus dapat dikerjakan dan mempunyai efek tertentu. Langkah-langkah yang tidak dapat dikerjakan dan tidak menghasilkan efek tertentu tidak dapat disebut sebuah algoritma. Efek-efek setiap langkah pada akhirnya akan memecahkan masalah secara keseluruhan [4].

B. Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *kryptos* yang artinya “yang tersembunyi” dan *graphein* yang artinya “tulisan”, jadi kriptografi adalah seni dan ilmu untuk menjaga keamanan data. Dan ahlinya disebut sebagai *cryptographer*. *Cryptanalst* merupakan orang yang melakukan

cryptanalysis, yaitu seni dan ilmu untuk membuka *ciphertext* menjadi *plaintext* tanpa melalui cara yang seharusnya. Data yang dapat dibaca disebut *plaintext* dan teknik untuk membuat data tersebut menjadi tidak dapat dibaca disebut *enkripsi.* Data hasil dari enkripsi disebut *ciphertext,* dan proses untuk mengembalikan *ciphertext* menjadi *plaintext* disebut *dekripsi.* Cabang matematika yang mencakup kriptografi dan *cryptanalysis* disebut *cryptology* dan pelakunya disebut *cryptologist* [5].

Secara umum, kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (plainteks) dengan suatu kunci tertentu menggunakan suatu metode enkripsi tertentu sehingga menghasilkan suatu informasi baru (chiperteks) yang tidak dapat dibaca secara langsung. Chiperteks tersebut dapat dikembalikan menjadi informasi awal (plainteks) melalui proses deskripsi. Urutan proses kriptografi secara umum dapat dilihat pada Gambar 1.



Gambar 1. Urutan proses kriptografi

Kriptografi berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptanalisis. Kriptanalis (*cryptanalysis*) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks, tanpa memerlukan kunci yang digunakan. Pelakunya disebut dengan kriptanalis. Jika seorang kriptopgrafer (istilah bagi pelaku kriptografi) mentransformasikan plainteks ke cipherteks dengan menggunakan kunci, maka sebaliknya seorang kriptanalis berusaha memecahkan cipherteks tersebut untuk menemukan plainteks atau kunci.

C. Algoritma RC4

Secara luas pada sistam keamanan seperti prorokol *SSL* (*Secure Socket Layer*). Algoritma kriftografi ini sederhana dan mudah di implementasikan. RC4 dibuat oleh Ron Rivest dari laboratorium RSA (*RC* adalah sinkatan dari *Ron's Code*). RC4 membangkitkan aliran kunci (*keystream*) yang kemudian di-XOR-kan dengan plainteks pada waktu enkripsi (atau di-XOR-kan dengan bit-bit cipherteks pada waktu dekripsi). Tidak seperti *chiper* aliran yang memproses data dalam bit, RC4 memproses data dalam ukuran *byte* (1 *byte* = 8 bit). Untuk membangkitkan aliran kunci, *chipper* menggunakan status internal yang terdiri dari 2 bagian:

1. Permutasi angka 0 sampai 255 di dalam larik S_0, S_1, ……., S_{255}. Permutasi merupakan kunci *U* dengan panjang variable.
2. Dua buah pencacah indeks, *i* dan *j* [6].

Sistem sandi RC4 menggunakan state, yaitu larik byte berukuran 256 yang terpermutasi, dan tercampur oleh kunci. Kunci enkripsi juga dan tercampur oleh kunci. Kunci enkripsi juga merupkan larik byte berukuran 256. Sebelum melakukan enkripsi, dan dekripsi, sistem sandi RC4 melakukan inisialisasi terhadap state dengan Algoritma, algoritma ini dosebut dengan penjadwalan kunci *(key scheduling).*

D. MP3

Pada tahun 1987, IIS mulai bekerja mencari cara untuk mengkodekan audio digital berdasarkan daya tangkap pendengaran. Proyek tersebut dinamakan proyek EU147. Dalam proyek tersebut IIS bekerjasama dengan Universitas Erlanggen (Prof. Dieter Seitzer). Akhirnya IIS berhasil menemukan teknik pengkodean yang kemudian distandarkan sebagai ISO-MPEG Audio Layer-3 (MPEG-1: IS 11172-3 dan MPEG-2: IS 13818-3)

File MP3 terdiri dari bagian-bagian kecil yang

disebut frame. Biasanya tiap frame dapat berdiri sendiri. Tiap frame memiliki *Header* yang berisi informasi frame tersebut. Pada file MPEG tidak ada header file, karena itu memotong file MPEG bisa dilakukan dimana saja selama masih dalam batasan frame. Lain halnya pada MP3, beberapa frame bisa merupakan bagian yang saling tergantung [7]. Untuk membaca informasi mengenai file MPEG dapat dilakukan dengan membaca header dari frame pertama. Tapi untuk file MPEG yang menggunakan Variable *bit rate/ bitrate switching*, informasi dari frame berubah-ubah. Variable bit rate akan didapatkan file yang lebih kecil tanpa menurunkan kualitas suara.

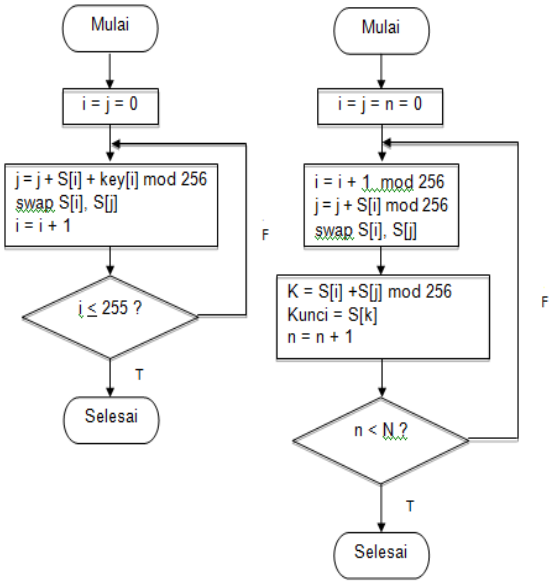
Header terdiri dari empat *byte* (32 bit) dan terletak dibagian awal dari frame yang bersangkutan. Sebelas *byte* yang pertama adalah singkronisasi frame dan ke-sebelas bit ini selalu bernilai 1. Bit ke-dua belas sampai bit ke-tiga puluh dua berisi informasi mengenai versi dari MPEG, layer, proteksi, bitrate, frekuensi cuplik, mode (stereo/mono) dan emphasis.

Data source adalah memori untuk menyimpan file MP3. Memori tersebut bisa berupa harddisk, CD-ROM atau komponen semi konduktor. Beberapa player MP3 yang ada di pasaran memakai flash memory untuk penyimpanan file. Kelebihan dari flash memori adalah ukurannya yang kecil dan ringan. kekurangannya adalah harga tiap byte nya masih lebih mahal jika dibandingkan dengan harddisk atau CD-ROM.

III. METODE PENELITIAN

A. *Flowchart RC4 MP3*

Algoritma RC4 mengenkripsikan 4 *byte* block data dengan memprosesnya melalui 2 aturan proses yang berbeda yaitu membuat *array* dan membuat set kunci.



Gambar 2. *Flowchart* pembangkit kunci RC4

Langkah- langkah pada membuat array dan membuat set kunci akan dijelaskan sebagai berikut:

Buat array state Ai berukuran 4 byte, yang memiliki nilai 1 sampai dengan 4:

1	2	3	4
1	6	1	6

Iterasi 1

A = (0 + A[0] + B [0]) mod 4

= (0 + 0 + 1) mod 4 = 1

Swap (A[0], A[1])

1	0	2	3

Iterasi 2

A = (1 + A[1] + B [1]) mod 4

= (1 + 0 + 6) mod 4 = 3

Swap (A[1], A[2])

1	3	2	0

Iterasi 3

A = (2 + A[2] + B [2]) mod 4

= (2 + 2 + 1) mod 4 = 1

Swap (A[2], A[1])

1	2	3	0

Iterasi 4

A = (3 + A[3] + B [3] 0 mod 4

= (3 + 0 + 6) mod 4 = 1

Swap (A[3], A[1])

1	0	3	2

Untuk mengenkripsi file MP3, Maka file MP3 tersebut dikonversikan kedalam bilangan biner yang nantinya akan di-XOR-kan dengan kunci. Sebagai contoh sebuah file MP3 berukuran 2 KB yang akan di enkripsi dengan panjang *array* S dan K sebanyak 16 Bit, maka:

2 KB = 2048 byte, Sehingga setiap blok sebanyak 16 bit diisi dengan angka 2048 yang disebut dengan plainteksnya.

Agar bisa di-XOR-kan dengan kunci, maka harus diubah kedalam bilangan biner.

2048 : 2 = 1024 sisa hasil bagi = 0
1024 : 2 = 512 sisa hasil bagi = 0
512 : 2 = 256 sisa hasil bagi = 0
256 : 2 = 128 sisa hasil bagi = 0
128 : 2 = 64 sisa hasil bagi = 0
64 : 2 = 32 sisa hasil bagi = 0
32 : 2 = 16 sisa hasil bagi = 0
16 : 2 = 8 sisa hasil bagi = 0
8 : 2 = 4 sisa hasil bagi = 0
4 : 2 = 2 sisa hasil bagi = 0
2 : 2 = 1 sisa hasil bagi = 0
1 : 2 = 0 sisa hasil bagi = 1

didapatkan chiperteksnya. Pada dekripsi maka hasil dari enkripsi atau chiperteksnya, akan didekripsi kembali dengan kunci yang sama, sehingga didapatkan kembali plainteks yang asli.

B. Model Pengembangan Sistem

Dalam mengembangkan sistem berbasis komputer perlu dilakukan tahapan-tahapan pengembangan. *Incremental* model adalah model pengembangan sistem pada *software engineering* berdasarkan *requirement software* yang dipecah menjadi beberapa fungsi atau bagian sehingga model pengembangannya secara bertahap. Model ini pun juga memiliki tahapan-tahapan untuk perancangan perangkat lunaknya, yaitu:

1. *Analisis*, Analisis adalah proses tahapan awal yang dilakukan pada incremental model adalah penentuan kebutuhan atau analisis kebutuhan.
2. *Design*, Design adalah tahap selanjutnya, perancangan software yang terbuka agar dapat diterapkan sistem pembangunan per bagian pada tahapan selanjutnya.
3. *Code*, setelah melakukan proses desain selanjutnya ada pengkodean.
4. *Test*, merupakan tahap pengujian dalam model ini.

IV. HASIL DAN PEMBAHASAN

C. Hasil

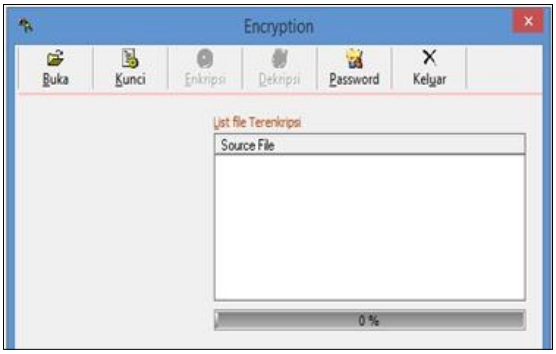
1. Tampil *Password Admi*n

Pada tampilan *password admin* berfungsi sebagai tampilan filter keamanan aplikasi adapun tampilan dapat dilihat pada gambar dibawah ini:

Gambar 3. Tampilan administrator *login*

a. Tampilan Menu Utama

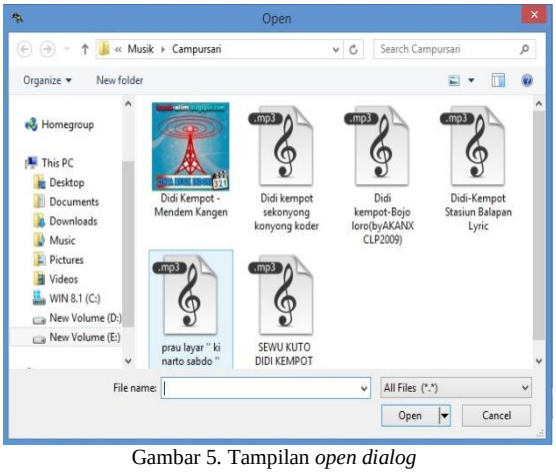
Pada tampilan menu utama, berfungsi sebagai navigator meliputi tombol buka, kunci, enkripsi, dekripsi, password dan keluar. Adapun tampilan menu utama dapat dilihat pada gambar dibawah ini:



Gambar 4. Tampilan menu utama

b. Tampilan *Open Dialog*

Pada tampilan dibawah ini, adalah fungsi open dialog, yang berfungsi sebagai untuk membuka file yang akan dienkripsi dan deekripsi. Adapun tampilan open dialog dapat dilihat pada gambar di bawah ini.



Gambar 5. Tampilan *open dialog*

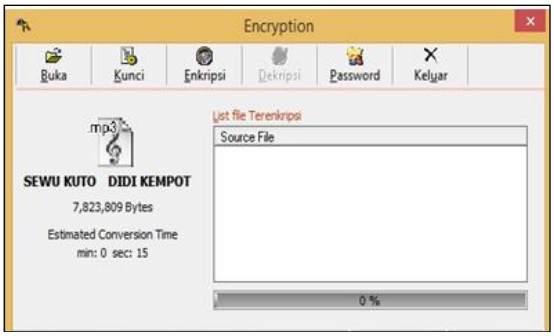
c. Tampilan Kunci

Tampilan kunci merupakan tampilan pengaturan kunci dari enkripsi dan dekripsi, adapun tampilan kunci dapat dilihat pada gambar dibawah ini.

Gambar 6. Tampilan kunci

d. Tampilan Enkripsi

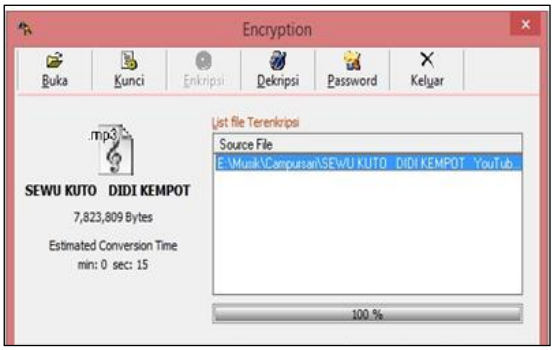
Tampilan enkripsi merupakan tampilan penyandian kode dengan algoritma RC4, dimana tampilan ini menampilkan informasi nama file, ukuran byte file, dan estimasi waktu dalam penyandian file. Adapun tampilan enkripsi dapat dilihat pada gambar dibawah ini.



Gambar 7. Tampilan enkripsi file *.mp3

e. Tampilan Deskripsi

Tampilan dekripsi merupakan tampilan membuka penyandian kode dengan algoritma RC4, dimana tampilan ini menampilkan informasi nama file, ukuran *byte file*, dan estimasi waktu dalam membuka penyandian file. Adapun tampilan dekripsi dapat dilihat pada gambar dibawah ini.



Gambar 8. Tampilan Dekripsi File *.mp3

D. Pembahasan

a. Hasil

1. Pengujian

Tabel 1 Hasil Pengujian Enkripsi dan Dekripsi

Ekstensi File	Byte	Waktu
MP3	323.809	Sec : 15

Berdasarkan dari pengujian diatas, bahwa file dengan ekstensi *.mp3 memiliki kecepatan sec: 15.

2. Black Box Testing

Tabel 2. Hasil Pengujian Sistem *Black Box*

Proses yang di uji	Skenario Pengujian	Hasil yang di harapkan	Ket
Tampilan login	1. Nama benar sedangkan Password Salah 2. Password benar sedangkan Nama Salah 3. Nama dan Password benar	1. Akan muncul pemberitahuan password salah 2. Akan muncul pemberitahuan nama salah 3. Akan tampil menu utama	Sesuai
Tampilan menu utama	Memiliki 6 menu, yaitu buka Kunci, enkripsi, dekripsi, password dan keluar	Setiap menu memiliki submenu, dan setiap submenu akan tampil form yang diinginkan	Sesuai
Tampilan enkripsi	1. Pilih drive yang akan dipilih 2. Pilih file yang akan dienkripsi	Akan muncul box dialog nama dan password	Sesuai
Tampilan Dekripsi	1. Pilih drive yang akan dipilih 2. Pilih file yang akan didekripsi	Akan muncul box dialog nama dan passsword	Sesuai

3. Hasil Pengujian

a. Aplikasi Enkripsi dan Deskripsi dengan algoritma *RC4* menggunakan sistem operasi *windows* 8 yang merubah sistem *windows*32 yaitu bagian *Shell32*.
b. Dokumen tersebut akan dibaca oleh suatu modu lbaca file masukan yang fungsinya membagi file MP3 kedalam beberapa blok data yang akan diproses oleh modul berikutnya, dimana setiap blok data terdiri atas 64 bit.
c. Dari hasil pengujian yang berekstensi *.mp3 enkripsi dan deskripsi berhasil dilakukan dengan memberikan informasi nama file, ukuran bytes, dan estimasi waktu.

V. KESIMPULAN DAN SARAN

A. *Kesimpulan*

Berdasarkan hasil pembahasan dan pengujian dapat diambil kesimpulan, antara lain:

1. Aplikasi Enkripsi dan Deskripsi dengan algoritma *RC4* menggunakan sistem operasi *windows* 8 yang merubah sistem*windows*32 yaitu bagian *Shell32*.
2. Dokumenter sebut akan dibaca oleh suatu modul baca file masukan yang fungsinya membagi file MP3 kedalam beberapa blok data yang akan diproses oleh modul berikutnya, dimana setiap blok data terdiri atas 64 bit.
3. Dari hasil pengujian yang berekstensi *.mp3 enkripsi dan deskripsi berhasil dilakukan dengan memberikan informasi nama file, ukuran bytes, dan estimasi waktu.

B. *Saran*

1. Disarankan adanya pengembangan system yaitu aplikasil ebih kompleks dengan algoritma dan bahasa pemograman tertentu.
2. Disarankan aplikasi ini dikembangkan pada sistem *android* sehingga timbul permasalahan yang harus ada solusi yang tepat.

REFERENSI

[1] Dewi, N. K. (2013). Implementasi Algoritma RC6 Untuk Proteksi File MP3. *Publikasi Jurnal Skripsi*, 1-7.

[2] Lausa, A. D. (2011).Pembajakan Musik danlagu Secara Digital: Sebuah kajian Yuridis Berdasarkan Perjanijian Internasional Tentang Perlindungan Karya Seni dan Sastra

[3] Hakim, E. L., Khairil, & Utami, F. H. (2014). Aplikasi Enskripsi dan Deskripsi Data Menggunakan Algoritma RC$ dengan Menggunakan Bahasa Pemrograman PHP, *Jurnal Media Infotama Vol. 10 No. 1*, 1-7.

[4] Wahid, F. (2003). *Dasar- Dasar Algoritma & Pemrograman.* Yogyakarta: Andi Yogyakarta.

[5] Prayudi, Y., & Halik, I. (2005). Studi dan Analisis Algoritma Rivest Code 6 (RC6) dalam Enskripsi/diskripsi Data. *Aplikasi Teknologi Informasi*, 149-158.

[6] Munir, R. (2006). *Kriftografi*. Bandung: Informatika Bandung.

[7] Hartanto, D. (2005). Sekelumit Tentang Format MP3 dan MP3 Player. 1-4.