Pengamanan File Mp3 Dengan Menggunakan Metode Triple Data Encryption Standar (Triple Des)

Dermawan Hendrik Gulo
Mahasiswa Program Studi Teknik Informatika STMIK Budidarma Medan; JL. Sisingamangaraja No.338 Simpang Limun Medan
e-mail : dermawangulo@gmail.com

Abstrak

Perkembangan dunia musik saat ini, telah memicu produksi terhadap file-file MP3. File-file MP3 yang sangat bebas untuk di distribusikan saat ini menimbulkan makin mudahnya tindakan penggandaan yang seharusnya hanya dapat dilakukan oleh pihak produksi. Salah satu upaya yang dilakukan adalah meminimalisir tindakan penggunaan MP3 tersebut dengan cara melakukan penyandian, sehingga orang lain hanya dapat menggandakan saja, tetapi tidak bisa menggunakan MP3 tersebut secara utuh. Salah satu teknik yang dipakai untuk mengatasi masalah tersebut adalah menerapkan teknik kriptografi dengan tujuan terhindar dari penggandaan file MP3 oleh pihak-pihak yang tidak berkepentingan.

Metode Triple DES (Triple Data Encryption Standard) merupakan perkembangan dari metode DES didalam Kriptografi. Pada dasarnya algoritma yang digunakan sama, hanya pada Triple DES dikembangkan dengan melakukan enkripsi dengan implementasi algoritma DES sebanyak tiga kali. Triple DES memiliki tiga buah kunci yang berukuran 168-bit (tiga kali kunci 56-bit dari DES). Pada algoritma Triple DES dibagi menjadi tiga tahap, setiap tahapnya merupakan implementasi dari algoritma DES. Tahap pertama, plainteks yang diinputkan dioperasikan dengan kunci eksternal pertama (K1) dan melakukan proses enkripsi dengan menggunakan algoritma DES.

Kata Kunci : *File Mp3, Triple Des, Enkripsi Dan Dekripsi*

Abstract

The development of the music world today, has triggered the production of MP3 files. MP3 files that are very free to distribute nowadays make it even easier for duplication actions that should only be done by the production. One effort made is to minimize the use of MP3 action by means of encoding, so that others can only copy it, but can not use the MP3 as a whole. One of the techniques used to overcome these problems is to apply cryptographic techniques with the aim of avoiding the duplication of MP3 files by unauthenticated parties.

Triple DES method (Triple Data Encryption Standard) is the development of DES method in Cryptography. Basically the algorithm used the same, only on Triple DES developed by performing encryption with DES algorithm implementation three times. Triple DES has three 168-bit keys (three 56-bit keys from DES). In the Triple DES algorithm is divided into three stages, each stage is an implementation of the DES algorithm. The first stage, the inputted plaintext is operated with the first external key (K1) and performs the encryption process using the DES algorithma.

Keywords : *MP3 files, Triple DES, Encryption and Decryption*

1. PENDAHULUAN

Perkembangan dunia musik saat ini, telah memicu produksi terhadap *file-file* MP3. *File-file* MP3 yang sangat bebas untuk di distribusikan saat ini menimbulkan makin mudahnya tindakan penggandaan yang seharusnya hanya dapat dilakukan oleh pihak produksi. Salah satu upaya yang dilakukan adalah meminimalisir tindakan penggunaan MP3 tersebut dengan cara melakukan penyandian, sehingga orang lain hanya dapat menggandakan saja, tetapi tidak bisa menggunakan MP3 tersebut secara utuh. Salah satu teknik yang dipakai untuk mengatasi masalah tersebut adalah menerapkan teknik kriptografi dengan tujuan terhindar dari penggandaan *file* MP3 oleh pihak-pihak yang tidak berkepentingan.

Niluh Kadek K.D (2013 : 1) Penggunaan *file* berupa *audio digital* berformat MP3 saat ini cukup populer dan mudah untuk dinikmati. *File* MP3 selain memberi kemudahan dalam penyebaran, juga memberi kemudahan dalam penggandaan yang kemudian dapat digunakan secara negatif tanpa memperhatikan aspek hak cipta. Untuk itu diperlukan suatu aplikasi yang bisa mengenkripsi file tersebut sehingga tidak mudah untuk digandakan, sehingga file yang sudah dienkripsi tidak dapat diputar atau dimainkan dengan sempurna. Salah satu teknik yang digunakan adalah dengan menerapkan teknik kriptografi, sehingga mampu menjaga kerahasiaan dari file tersebut yang sifatnya rahasia.

2. METODE PENELITIAN

Dalam penyusunan laporan dibutuhkan data yang sangat akurat dan objektif agar dapat dilaksanakan pembahasan dan pengevaluasian serta penyimpulan untuk lebih mengerti dan memahami isi dari penyusunan laporan tersebut. Di dalam pengumpulan data yang akurat ini, penulis menggunakan beberapa metode untuk memperoleh data tersebut.

2.1 Keamanan

Keamanan secara umum adalah kondisi dimana keadaan bebas dari bahaya. Suatu informasi dikatakan aman apabila informasi yang diterima dan disampaikan bebas dari gangguan pihak yang tidak berwenang (Bambang Supradono, 2009, 4). Perkembangan dunia teknologi semakin mengkhawatirkan para penerima informasi untuk berkomunikasi. Informasi sekarang ini merupakan suatu kebutuhan bagi masyarakat luas. Hal ini secara langsung dapat dilihat dari perilaku masyarakat yang selalu butuh akan informasi yang direalisasikan melalui berbagai hal seperti berlangganan koran, majalah, dan lain-lain. Kemudahan masyarakat untuk mendapatkan informasi karena informasi berkembang dengan sangat pesat mengikuti perkembangan dunia. Sama halnya dengan teknologi, informasi berkembang seraya mengikuti perkembangan teknologi. Perkembangan informasi membuat informasi itu menjadi hal yang sangat penting dan membutuhkan keamanan untuk melindungi informasi.

2.2 Kriptografi

Kriptografi berasal dari dua kata Yunani, yaitu *Crypto* yang berarti rahasia dan *Grapho* yang berarti menulis. Secara umum kriptografi dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu pesan. Kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasian, keutuhan data dan otentikasi entitas (Rafki Sadikin, 2012). Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan atau data (Rinaldi Munir 2006). Jadi, kriptografi adalah ilmu yang mempelajari cara-cara penyandian pesan atau informasi dengan menggunakan teknik matematika agar terhindar dari pihak-pihak yang ingin mengetahui sebuah informasi yang bersifat rahasia.

2.3 Algoritma Triple Data Encryption Standar

Algoritma enkripsi atau dekripsi *Triple* DES seperti algoritma kriptografi lainnya yaitu memiliki algoritma umum. *Triple* DES merupakan suatu algoritma pengembangan dari algoritma DES.

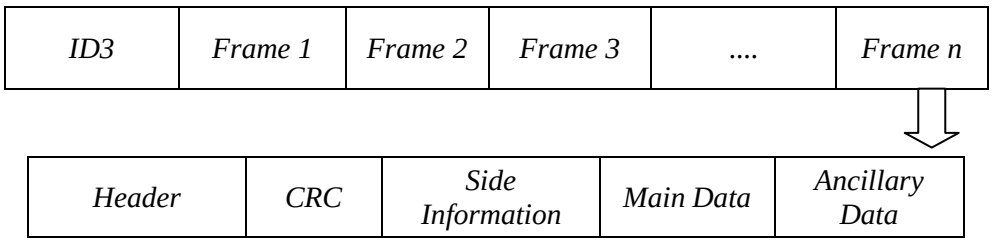
Triple DES memiliki 3 buah kunci yang berukuran 168-*bit* (tiga kali 56 *bit* dari DES). Pada algoritma *Triple* DES dibagi menjadi tiga tahap, setiap tahapnya merupakan implememntasi dari algoritma DES, tahap tersebut antara lain :

1. Plainteks yang diinputkan dioperasikan dengan kunci eksternal pertama (K1) dan melakukan proses enkripsi dengan menggunakan algoritma DES, sehingga menghasilkan pra- chipherteks pertama.
2. Pracipherteks pertama yang dihasilkan pada tahap pertama, kemudian dioperasikan dengan kunci eksternal kedua (K2) dan melakukan proses enkripsi atau proses dekripsi (tergantung cara pengenkripsian yang digunakan) dengan menggunakn algoritma DES. Sehingga menghasilkan Pra- cipherteks kedua.
3. Pracipherteks kedua yang dihasilkan pada tahap kedua, dioperasikan dengan kunci eksternal ketiga (K3) dan melakukan proses enkripsi dengan menggunakan algoritma DES, sehingga menghasilkan cipherteks (C).

2.4 File MP3

MPEG-1 Audio *Layer 3* atau lebih dikenal sebagai MP3 adalah salah satu format berkas pengkodean suara yang memiliki kompresi yang baik (meskipun bersifat *lossy*) sehingga ukuran berkas bisa memungkinkan menjadi lebih kecil [2]. Berkas ini dikembangkan oleh seorang insinyur *Jerman Karlheinz Brandenburg*. MP3 memakai pengodean *Pulse Code Modulation* (PCM). MP3 mengurangi jumlah *bit* yang diperlukan dengan menggunakan model *psychoacoustic* untuk menghilangkan komponen-komponen suara yang tidak terdengar oleh manusia.

File MP3 tersusun dari banyak *frame* MP3, yang terdiri dari sebuah *header* dan sebuah blok data. Setiap *frame* secara umum menyimpan 1152 sampel audio selama 26 ms. Artinya *frame rate* yang dihasilkan sekitar 38 fps. Dengan tambahan setiap *frame* dibagi menjadi 2 unit yang menyimpan 576 sampel. Karena *bitrate* menentukan ukuran setiap sampel maka memperbesar *bitrate* akan memperbesar ukuran dari *frame* tersebut. Sebuah *frame* terdiri dari lima bagian yaitu *header* , *CRC*, *side information*, *main data* dan terakhir *ancillary data.*



2.4.1 Struktur File MP3

Semua *file* MP3 dibagi menjadi *fragmen* kecil yang disebut *frames*. Setiap *frame* menyimpan 1.152 sampel suara dan berlangsung selama 26 ms. Ini berarti bahwa *frame rate* akan menjadi sekitar 38 fps. Sebagai tambahan *frame* dibagi menjadi dua *granule*/butiran, masing-masing mengandung 576 sampel. Karena *bitrate* menentukan ukuran pada setiap sampel,maka apabila meningkatkan *bitrate* akan meningkatkan ukuran *frame*. Ukuran juga tergantung pada frekuensi sample dengan rumus berikut

$$\frac{144*\text{bitrate} + \text{padding [bytes]}}{\text{samplefrequency}}$$

Padding mengacu pada sebuah *bit* yang khusus dialokasikan di awal *frame*. Hal ini digunakan dalam beberapa *frame* untuk memenuhi persyaratan *bitrate* dengan jelas. Jika *bit* padding diatur setara dengan 1 *byte*. Sebagai catatan bahwa ukuran *frame* harus berupa angka / integer.Struktur *file* MP3 terdiri dari 5 bagian, *header, CRC, side information*, main data dan *ancillary* data.

3. HASIL DAN PEMBAHASAN

3.1 Analisa

Keamanan merupakan aspek yang sangat penting dalam proses pengiriman informasi yang sifatnya rahasia. Karena informasi sangat rentan terhadap pencurian ataupun penyadapan. Oleh karena itu, keamanan sangat penting untuk mencegah informasi tersebut sampai pada pihak-pihak lain yang tidak berkepentingan yang mengakibatkan terjadinya kebocoran atau penyalahgunaan data dan informasi.

Dalam kriptografi terdapat beberapa algoritma yang dapat menyandikan data dan informasi. Salah satunya adalah algoritma *triple DES* yang dapat mencegah terjadinya penyadapan ataupun kebocoran informasi. Algoritma *triple DES* ini termasuk kategori yang rumit, karena proses enkripsinya mengulang sebanyak tiga kali algoritma *DES* dan menggunakan tiga buah kunci yang bersifat bebas (misalnya K1, K2 dan K3) ataupun dua buah kunci (K1, K2 dan K3= K1). Tingkat ketergantungan cipherteks terhadap kunci pada algoritma ini sangat tinggi, karena salah satu huruf, maka akan berakibat kesalahan pada cipherteks dan untuk menambah tingkat kerumitan dalam pemecahan ciphertek disarankan menggunakan tiga buah kunci yang berbeda.

3.2 Penerapan Metode Triple DES pada pengamanan File MP3

Secara umum, *Triple* DES dengan 2 buah kunci mempunyai panjang kunci 2 x 56 *bit* = 112 *bit*, jauh lebih pendek dari pada *Triple* DES yang mempunyai panjang kunci 3 x 56 *bit* = 168 *bit*.

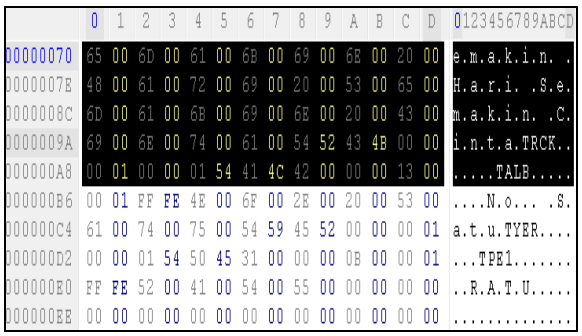
Melalui perangkat lunak MP3 *Frame Editor*, maka MP3 dapat dilihat biner dari setiap nya. Prosesnya setelah biner di dapatkan, maka biner tersebut yang akan dienkripsi dan didekripsikan nantinya.

Berikut adalah struktur MP3 dengan judul “Semakin hari semakin cinta.MP3”.

Tabel 1 Struktur *frame* dari lagu MP3

Frame 1 Layer	Frame 2 Layer	Frame 3 Layer	Speed (Kbps)	Bitrate value
1101	1101	1101	32	0001
11674	11674	11674	64	0010
11607	11607	11607	96	0011
11707	11707	11707	128	0100
111890	111890	111890	160	0101
1129080	1129080	1129080	192	0110
113790987	113790987	113790987	224	0111
11456859568	11456859568	11456859568	256	1000
11590679854	11590679854	11590679854	288	1001
1258580298756	1258580298756	1258580298756	320	1010

Dari tabel diatas maka akan ditampilkan frame dari MP3 tersebut, dan akan dilakukan perhitungan seperti pada tabel 1. Setelah *frame* dari lagu MP3 tersebut didapat maka langkah selanjutnya adalah mengubah struktur *frame* tersebut yang terdiri dari 3 buah *layer* kedalam angka *biner*. Cara kerjanya dapat dilihat seperti dibawah ini:



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	0123456789ABCD
00000070	65	00	6D	00	61	00	6B	00	69	00	6E	00	20	00	e.m.a.k.i.n. .
0000007E	48	00	61	00	72	00	69	00	20	00	53	00	65	00	H.a.r.i. .S.e.
0000008C	6D	00	61	00	6B	00	69	00	6E	00	20	00	43	00	m.a.k.i.n. .C.
0000009A	69	00	6E	00	74	00	61	00	54	52	43	4B	00	00	i.n.t.a.TRCK..
000000A8	00	01	00	00	01	54	41	4C	42	00	00	00	13	00	.....TALB.....
000000B6	00	01	FF	FE	4E	00	6F	00	2E	00	20	00	53	00	....N.o... .S.
000000C4	61	00	74	00	75	00	54	59	45	52	00	00	00	01	a.t.u.TYER....
000000D2	00	00	01	54	50	45	31	00	00	00	0B	00	00	01	...TPE1.......
000000E0	FF	FE	52	00	41	00	54	00	55	00	00	00	00	00	..R.A.T.U.....
000000EE	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

Maka didapat data data dalam bentuk *format biner* yang dapat ditulis sebagai berikut:

Tabel 2 hasil konversi *frame* ke bilangan biner

Bitrate value	Frame 1 Layer	0	1	2	3	4	5	6	7	8	9
0001	1101	01	00	01	10	00	00	00	00	01	01
0010	11674	00	00	00	01	10	00	01	11	01	10
0011	11607	10	11	00	01	00	00	00	00	01	01
0100	11707	11	01	00	00	00	01	11	00	00	01
0101	111890	10	11	00	01	00	00	00	00	01	01
0110	1129080	00	00	00	01	10	00	01	11	01	10
0111	113790987	10	11	00	01	00	00	00	00	01	01
1000	11456859568	11	01	00	00	00	01	11	00	00	01
1001	11590679854	00	00	00	01	10	00	01	11	01	10
1010	1258580298756	10	11	00	01	00	00	00	00	01	01

3.2.*1 Pemilihan Kunci*

Ada dua pilihan untuk pemilihan kunci eksternal algoritma *Triple* DES, yaitu:

a. K_1, K_2, dan K_3 adalah kunci-kunci yang saling bebas
   $\mathbf{K_1 \neq K_2 \neq K_3 \neq K_1}$
b. K_1 dan K_2 adalah kunci-kunci yang saling bebas, dan K_3 sama dengan K_1
   $\mathbf{K_1 \neq K_2}$ dan $\mathbf{K_3 = K_1}$

Dari rumus diatas tampak bentuk pergantian karakter dari masing-masing huruf, jadi di *enkripsi* akan menjadi pesan maka langkah selanjutnya adalah menyisipkan pesan tersebut kedalam MP3 dengan menggunakan algoritma *Triple* DES, diasumsikan besar MP3 adalah 402554 *byte*.

Bit *plaintext* seluruhnya :

$\mathbf{K_1 \neq K_2 \neq K_3 \neq K_1}$

	=	01000110	01010010	01000001	01001110
		01000011	01001001	01010101	01010011 ⊕
Hasil XOR	=	00000101	00011011	00010100	00011101
Jumlah *key*	=	5	1B	14	1D
Kunci Eksternal	=	00001010	00110110	00101000	00111010
		C	36	28	3A

Notasi Hexadesimal	=	C	36	28	3A
$\mathbf{K_1 \neq K_2 \neq K_3 \neq K_1}$					
	=	01000011	01001001	01010101	01010011
		01000011	01001001	01010101	01010011 ⊕
Hasil XOR	=	00000000	00000000	00000000	00000000
Jumlah *key*	=	0	0	0	0
Kunci Eksternal	=	00000000	00000000	00000000	00000000
		0	0	0	0
Notasi Hexadesimal	=	0	0	0	0
$\mathbf{K_1 \neq K_2 \neq K_3 \neq K_1}$					
	=	01011111	01001101	01000001	01001110
		01000011	01001001	01010101	01010011 ⊕
Hasil XOR	=	00011100	00000100	00010100	00011101
Jumlah *key*	=	1C	4	14	1D
Kunci Eksternal	=	00111000	00001000	00101000	00111010
		38	8	28	3A
Notasi Hexadesimal	=	38	8	28	3A
$\mathbf{K_1 \neq K_2 \neq K_3 \neq K_1}$					
	=	01010101	01010010	01010101	01001110
		01000011	01001001	01010101	01010011 ⊕
Hasil XOR	=	00010110	00011011	00000000	00011101
Jumlah *key*	=	16	1B	0	1D
Kunci Eksternal	=	00101100	00110110	00000000	00111010
		2C	36	0	3A
Notasi Hexadesimal	=	2C	36	0	3A
$\mathbf{K_1 \neq K_2 \neq K_3 \neq K_1}$					
	=	01000111	01011111	01000001	01001101
		01000011	01001001	01010101	01010011 ⊕
Hasil XOR	=	00000100	00010110	00010100	00011110
Jumlah *key*	=	4	16	14	1E
Kunci Eksternal	=	00001000	00101100	00101000	00111100
		8	2C	28	3C
Notasi Hexadesimal	=	8	2C	28	3C
$\mathbf{K_1 \neq K_2 \neq K_3 \neq K_1}$					
	=	01010000	01000101	01010010	01000001
		01000011	01001001	01010101	01010011 ⊕
Hasil XOR	=	00010011	00001100	00000111	00010010
Jumlah *key*	=	13	C	7	12
Kunci Eksternal	=	00100110	00011000	00001110	00100100
		26	18	E	24
Notasi Hexadesimal	=	26	18	E	24

Jadi *Ciphertext* sebelum digeser adalah : 5 1B 14 1D, 0 0 0 0, 1C 4 14 1D, 16 1B 0 1D, 4 16 14 1E, 13 C 7 12, ⟶ Hexadesimal.
dan *Ciphertext* adalah : C 36 28 3A, 0 0 0 0, 38 8 28 3A, 2C 36 0 3A, 8 2C 28 3C, 26 ~~18 E~~ 24 Hexadesimal.

Berikut ini adalah hasil perhitungan dari algoritma *Triple DES* dengan proses *Deskripsi* adalah sebagai berikut:

Cipherteks-nya : 5 1B 14 1D, 0 0 0 0, 1C 4 14 1D, 16 1B 0 1D, 4 16 14 1E, 13 C 7 12,

Jmlh bit setiap kelompok : 32

4. KESIMPULAN

Beberapa kesimpulan yang dapat diambil penulis setelah merancang dan menyelesaikan penelitian ini adalah :

1. Menerapkan metode *triple DES* pada enkripsi *file* MP3 menggunakan tiga kata kunci. *File* MP3 akan dibaca dalam bentuk bilangan biner terlebih dahulu kemudian dengan menggunakan ketiga kata kunci tersebut akan di-xor-kan dengan setiap bilangan biner yang didapatkan pada file MP3 sehingga menghasilkan data yang berbeda dengan data awal. Demikian halnya dengan proses deskripsi juga menggunakan tiga kunci yang sama seperti pada kata kunci enkripsi.
2. Merancang aplikasi untuk enkripsi dan deskripsi menggunakan *Visual Basic .NET 2008*. Metode *Triple DES* diterapkan ke dalam *coding Visual Basic .NET 2008* dengan algoritma yang disesuaikan dengan cara enkripsi dan deskripsi metode *Triple DES*. Perancangan juga menggunakan *tools*, *textbox*, *button*, *function* yang disediakan oleh *service* visual basic .NET 2008.

DAFTAR PUSTAKA

[1] Hidayat, Akik, (2010), "Enkripsi dan Dekripsi Data Dengan Algoritma 3 DES (Triple Data Encryption Standar)".
[2] K.D, Niluh Kadek, dkk. (2013). Implementasi Algoritma RC6 Untuk Proteksi File MP3.
[3] Munir, Rinaldi "Kriptografi", Penerbit Informatika, Bandung, 2006
[4] Sadikin, Rifki "Kriptografi Untuk Keamanan Jaringan" Penerbit Andi, Yogyakarta, 2012