JURNAL HOAQ
TEKNOLOGI INFORMASI

ISSN : 2337-5280

HOAQ

High Education Of Organization Archive Quality

JURNAL	Volume 7	Nomor 2	HAL 520-602	KUPANG,	ISSN 2337-5280

DEWAN REDAKSI

Alamat Sekretariat/Redaksi:

Lembaga Penelitian,Publikasi dan Pengembangan pada Masyarakat
STIKOM Uyelindo Kupang
Jl. Perintis Kemerdekaan 1, Kayu Putih,Kupang,NTT,Indonesia.
Telp.(0380)8554501, Fax (0380)8554500
Email : lp3muyelindo@uyelindo.ac.id
http://www.uyelindo.ac.id

Jurnal Hoaq merupakan Jurnal Ilmiah untuk menampung hasil penelitian yang berhubungan dengan bidang sains dan teknologi. Bidang penelitian yang dimaksud adalah Soft Computing, Mobile Computing, dan Rekayasa Perangkat Lunak.

Jurnal Hoaq diterbitkan oleh Lembaga Penelitian,Publikasi dan Pengembangan pada Masyarakat, Bekerja sama dengan Program Studi Teknik Informatika dan Program Studi Sistem Informasi STIKOM Uyelindo Kupang. **Redaksi** mengundang para professional dari dunia usaha, pendidikan dan peneliti untuk menulis mengenai perkembangan ilmu di bidang **Teknologi Informasi.**

Jurnal Hoaq diterbitkan 2(dua) kali dalam 1(satu) tahun pada bulan Mei dan Desember

JURNAL HOAQ -TEKNOLOGI INFORMASI

DAFTAR ISI

PENERAPAN ALGORITMA RSA PADA SISTEM KRIPTOGRAFI *FILE AUDIO* MP3

Ngakan Nyoman Diarse[1], Kristoforus Jawa Bendi[2]

[1,2]Program Studi Informatika, Universitas Katolik Musi Charitas
Jl. Bangau No. 60 Palembang
e-mail :[1]ngakannyoman19@gmail.com,[2]kristojb@gmail.com

ABSTRACT

The problem of data security is one of the important aspect of information technology. One solution that can be used to maintain data security is cryptography. Cryptography is a field of knowledge that use mathematical equations to perform encryption and decryption of data either by applying algorithms asymmetry such as the DSA (Digital Signature Algorithm), RSA, DH (Diffie-Hellman), ECC (Elliptic Curve Cryptography), and Cryptography Quantum. Of the many asymmetric algorithms are made, the most popular algorithm is the RSA algorithm. Security RSA algorithm lies in the difficulty of factoring large prime numbers are relative. To prove the security of the RSA algorithm is needed media as the data to be secured like the MP3 audio format.

The MP3 format is one of the audio format most commonly used in the storage of audio data, because data is stored resemble the original data when recorded, and has a size that is not too large compared to other formats. Applications cryptographic system created in order to implement the RSA algorithm for encryption and decryption of MP3 audio files. The result is the application of a cryptographic system can encrypt the MP3 audio file can then decrypt back MP3 audio files that have been encrypted. MP3 audio files are encrypted still playable but his voice was not audible to the human ear so that the necessary application to decrypt the MP3 audio file to be played as before.

Keywords: *Cryptographic System, RSA Algorithm, Audio MP3 File*

1. PENDAHULUAN

Teknologi informasi merupakan salah satu hal penting dalam peradaban manusia untuk mengatasi sebagian masalah derasnya arus informasi.Selain memiliki potensi dalam memfilter data dan mengolah menjadi informasi, teknologi informasi mampu menyimpannya dalam jumlah kapasitas jauh lebih banyak dari cara-cara manual. Salah satu pekerjaan manusia yang akan sangat terbantu dengan hadirnya teknologi informasi, dengan keuntungan yang ditawarkan yaitu pekerjaan manusia dalam mengamankan data [5].

Masalah keamanan data merupakan salah satu aspek penting dalam teknologi informasi. Salah satu solusi yang dapat digunakan untuk menjaga keamanan data yaitu dengan melakukan proses enkripsi dan dekripsi guna membuat data ataupun informasi tidak dapat dibaca atau dimengerti oleh orang lain, kecuali untuk penerima yang berhak atau memiliki kunci. Teknik pengamanan data dengan proses enkripsi dan dekripsi dikenal dengan istilah kriptografi [6].

Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi maupun dekripsi data. Teknik ini digunakan untuk merubah data biasa dengan kunci tertentu menjadi data yang tidak diketahui oleh orang lain kecuali bagi orang yang berhak. Kriptografi telah menjadi bagian penting dalam dunia teknologi informasi saat ini.Hampir semua penerapan teknologi informasi menggunakan kriptografi sebagai alat untuk menjamin kemanan data dan kerahasiaan informasi. Karena kriptografi menjadi ilmu yang berkembang pesat, dalam waktu singkat banyak bermunculan algoritma-algoritma baru yang dianggap lebih unggul dari pada pendahulunya, salah satunya adalah algoritma asimetri seperti Algoritma DSA (*Digital Signature Algorithm*), Algoritma RSA (*Rivest Shamir Adleman*), Algoritma DH (*Diffie-Hellman*), Algoritma ECC (*Elliptic Curve Cryptography*), dan Kriptografi Quantum. Dari sekian banyak algoritma asimetri yang dibuat, algoritma yang paling populer adalah algoritma RSA.Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan prima yang relatif besar.Selama belum ada algoritma yang berhasil memecahkan pemfaktoran bilangan prima yang besar, maka selama itu keamanan algoritma RSA tetap terjamin [1].

Untuk membuktikan keamanan algoritma RSA maka diperlukan media sebagai data yang akan diamankan. Pengamanan data dapat dilakukan pada semua *format* multimedia yang ada dalam komputer seperti *format* teks, *format* gambar, *format audio*, dan *format video*. Bahkan untuk *format audio* dan sebagainya asalkan *file-file* tersebut mempunyai bit-bit data yang dapat dimodifikas, maka *file* tersebut dapat diamankan dengan algoritma RSA seperti *format audio* MP3. *Format audio* MP3 adalah salah satu *format audio* yang paling sering digunakan dalam penyimpanan data *audio*, karena data yang disimpan menyerupai data asli saat direkam, dan memiliki ukuran tidak terlalu besar dibandingkan *format* lain.

Berdasarkan latar belakang di atas maka diperlukan sebuah aplikasi sistem kriptografi yang dapat menerapkan algoritma RSA untuk proses enkripsi dan dekripsi *file audio* MP3. *File audio* MP3 yang telah terenkripsi nantinya masih dapat diputar tetapi suaranya tidak terdengar jelas oleh telinga manusia sehingga diperlukan aplikasi untuk mendekripsi *file audio* MP3 tersebut agar dapat diputar seperti semula.

2. TINJAUAN PUSTAKA

2.1 Kriptografi

Kriptografi berasal dari Bahasa Yunani, menurut bahasa dibagi menjadi dua kripto dan graphia, kripto berarti secret (rahasia) dan graphia berarti writing (tulisan).Menurut teminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain[7].

2.2 Algoritma RSA (Rivest Shamir Adleman)

Dari sekian banyak algoritma kriptografi kunci publik yang pernah dibuat, algoritma yang paling populer adalah algoritma RSA. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1976, yaitu : Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima.Pemfaktoran dilakukan untuk memperoleh kunci pribadi.Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin [7].Sebuah sistem kriptografi kunci publik memiliki algoritma pembangkit kunci, algoritma enkripsi dan algoritma dekripsi.Berikut adalah prosedur untuk membuat pasangan kunci :

1. Pilih dua buah bilangan prima sembarang, p dan q.
2. Hitung $r = p.q$. Sebaiknya $p \neq q$, sebab jika $p = q$ maka $r = p^2$ sehingga $\sqrt{r}$ dapat diperoleh dengan menarik akar pangkat dua dari r.
3. Hitung $\phi(r) = (p-1)(q-1)$.
4. Pilih kunci publik PK, yang relatif prima terhadap $\phi(r)$.
5. Bangkitkan kunci privat dengan menggunakan persamaan(1) berikut:

$$SK = \frac{1+m\phi(r)}{PK} \quad (1)$$

Algoritma enkripsi RSA dapat dijelaskan sebagai berikut.

Plainteks disusun menjadi blok-blok m_1, $m_2,\ldots,$ m_n sedemikian sehingga setiap blok merepresentasikan nilai di dalam rentang 0 sampai r–1. Blok plinteks x_i dienkripsi menjadi blok y_i dengan persamaan (2)

$$E_{PK}(X) = Y \equiv X^{PK} \bmod r \quad (2)$$

Algorimta dekripsi dapat dijelaskan sebagai berikut.

Setiap blok cipherteks yi didekripsi kembali menjadi blok plainteks xi dengan persamaan (3)

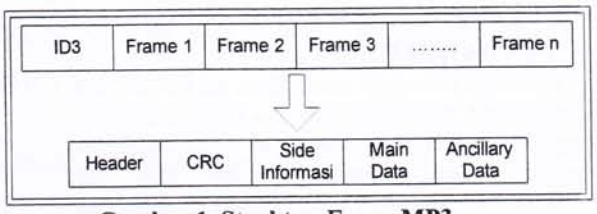
$$D_{SK}(Y) = X \equiv Y^{SK} \bmod r \quad (3)$$

Penelitian-penelitian yang menggunakan RSA sebagai algoritma kriptografi telah banyak dilakukan.RSA telah digunakan untuk mengamankan pesan dalam berbagai bentuk/media, antara lain media teks [1, 2, 4, 10, 11, 12], suara [6, 11], gambar [4, 11], dan gambar bergerak/video [4, 19].

2.3 Mpeg-1 Layer 3 (MP3)

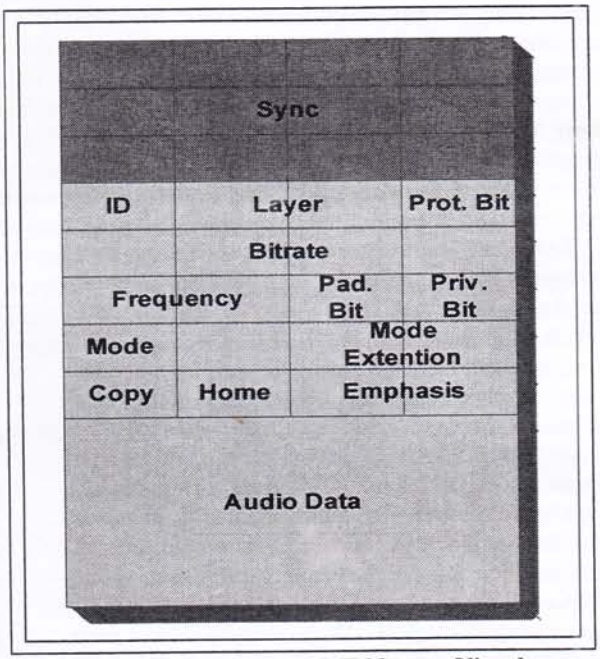
Mpeg-1 Audio Layer 3 atau lebih dikenal sebagai MP3 adalah salah satu format berkas pengodean suara yang memiliki kompresi yang baik (meskipun bersifat lossy) sehingga ukuran berkas bisa memungkinkan menjadi lebih kecil.Berkas ini dikembangkan oleh seorang insinyur Jerman Karlheinz Brandenburg.MP3 memakai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

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 *bit rate* menentukan ukuran setiap sampel maka memperbesar *bit rate*akan memperbesar ukuran dari frame tersebut. Sebuah frame terdiri dari lima bagian yaitu header, CRC, side information, main data dan terakhir ancillary data. Pada struktur frame MP3 dapat dilihat pada Gambar 1 [3].Isi header frame dapat dilihat pada Gambar 2. Sedangkan frame header MP3 secara visual dapat dilihat pada Gambar 3.Karakteristik file header dapat dilihat pada Tabel 1[8].



Gambar 1. Struktur *Frame* MP3

Gambar 2. Header Frame



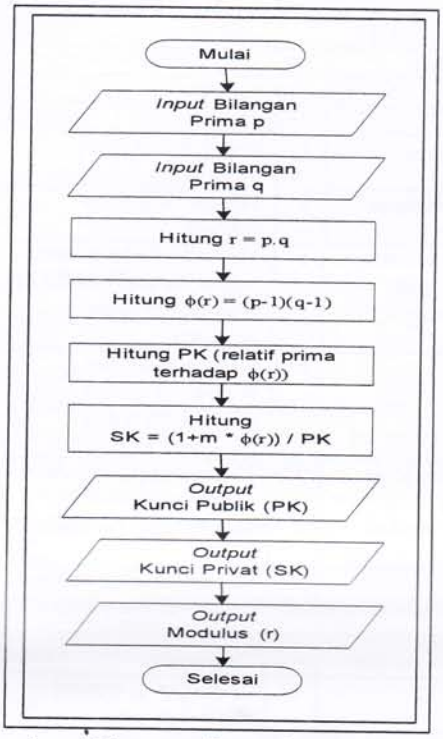
Gambar 3. Frame Header MP3Secara Visual

Tabel 1. Karakteristik *File Header*

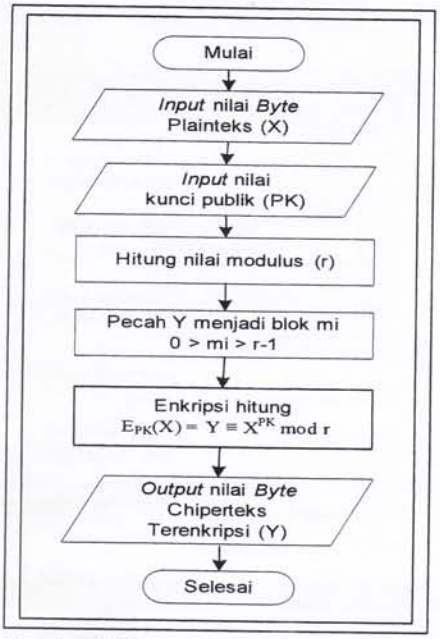
Posisi	Tujuan	Bit
A	Sinkronisasi *Frame*	11
B	Versi MPEG	2
C	Layer MPEG	2
D	Proteksi	1
E	Index *Bit rate*	4
F	Frekuensi Tingkat Sampel	2
G	*BitPadding*	1
H	*BitPrivat*	1
I	Mode *Channel*	2
J	Mode Lanjutan	2
K	*Copyright*	1
L	Originalitas	1
M	Emphasis	2

3. PEMODELAN SISTEM

Pertama-tama yang dilakukan pada tahap pemodelan sistem adalah menyusun diagram alir untuk proses pembentukan kunci (Gambar 4), proses enkripsi (Gambar 5), dan proses dekripsi (Gambar 6). Selanjutnya dilakukan pemodelan sistem dengan menggunakan *Unified Modelling Language* (UML). Pemodelan sistem mencakup *use case diagram*, *use case scenario*, *sequence diagram*, dan *activity diagram*.

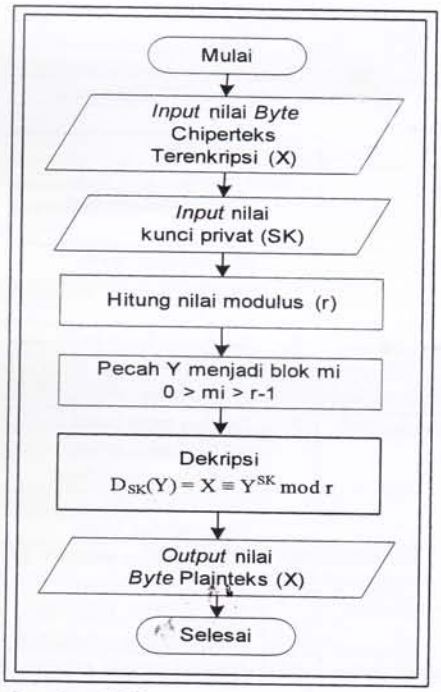


Gambar 4.Diagram alir pembentukan kunci

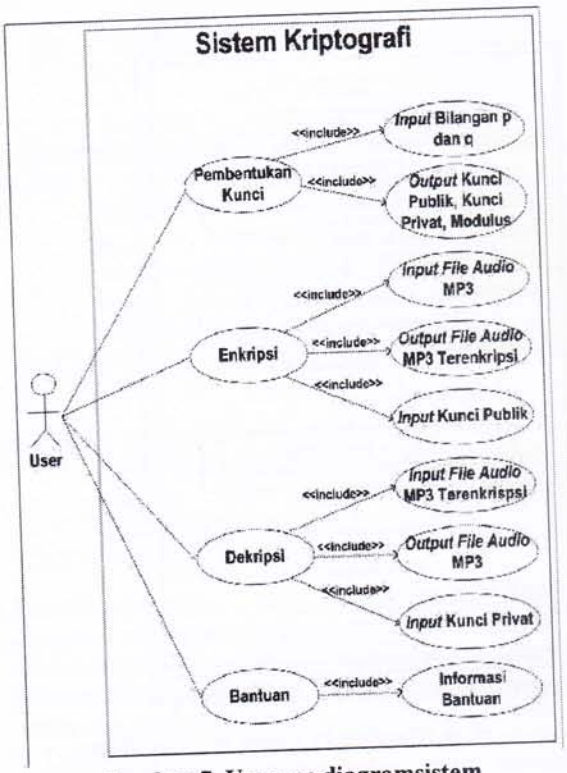


Gambar 5.Diagram alir proses enkripsi

Use case diagram (Gambar 7) sistem ini mencakup tiga aktivitas utama, yakni aktivitas pembentukan kunci, aktivitas proses enkripsi dan aktivitas proses dekripsi. Dekripsi, kondisi, dan alur proses dari tiap-tiapaktivitas dijelaskan melalui skenario *use case*(Tabel 2 s.d. Tabel 4).



Gambar 6.Diagram alir proses dekripsi



Gambar 7. Use case diagramsistem

Tabel 2. Skenario pembentukan kunci

Identifikasi			
Nama *Use Case*	Pembentukan Kunci		
Aktor	*User*		
Deskripsi	*User* melakukan pembentukan kunci		
Skenario Utama			
Kondisi Awal	Menampilkan menu utama		
Aksi Aktor		Reaksi Sistem	
		1	Menampilkan menu utama
2	Memilih menu pembentukan kunci	3	Menampilkan form pembentukan kunci
4	Menginputkan bilangan prima p dan q	5	*Textbox* p dan q terisi bilangan prima p dan q yang diinputkan
6	Menekan tombol hitung	7	*Textbox* terisi kunci publik, kunci privat, modulus yang didapat dari perhitungan pembentukan kunci
		8	Menampilkan pesan apakah anda ingin menggunakan kunci ini serta tombol ya dan tidak
9	Menekan tombol ya	10	Masuk ke menu enkripsi
Alternatif 1			
9	Menekan tombol tidak	10	Menutup pesan serta pilihan ya/tidak dan kembali ke tampilan menu pembentukan kunci
Kondisi Akhir	Menampilkan menu enkripsi jika memilih tombol ya atau melanjutkan tampilan sebelumnya jika memilih tombol tidak		

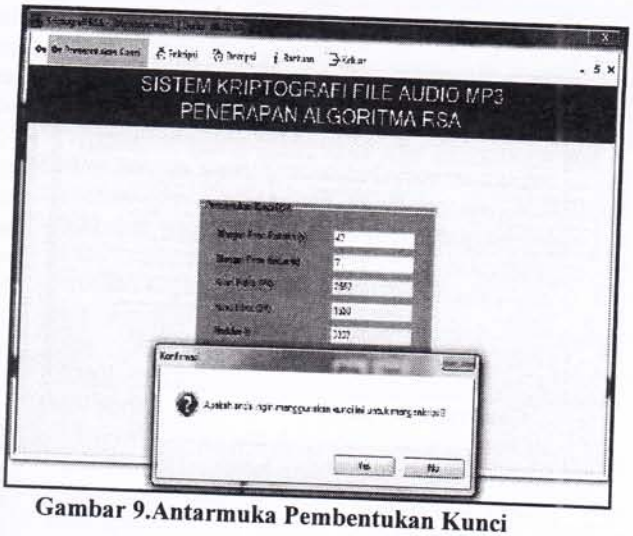
Tabel 3. Skenario proses enkripsi

Identifikasi			
Nama *Use Case*	Enkripsi		
Aktor	*User*		
Deskripsi	*User* melakukan enkripsi *file audio* MP3		
Skenario Utama			
Kondisi Awal	Menampilkan menu utama		
Aksi Aktor		Reaksi Sistem	
		1	Menampilkan menu utama
2	Memilih menu enkripsi	3	Menampilkan form enkripsi
4	Menekan tombol *browse* pada *textbox input file*	5	Membuka folder dimana tempat *file audio* MP3 tersimpan di memori komputer
		6	Kunci publik terisi otomatis di *textbox* kunci publik didapat dari pembentukan kunci
7	Menekan tombol proses	8	Proses enkripsi berjalan sampai selesai mengenkripsi *file audio* MP3
		9	Menampilkan pesan file berhasil dienkripsi dan *file audio* MP3 yang dienkripsi :
		10	Tersimpan di memori komputer
Kondisi Akhir	Menampilkan *form* menu enkripsi		

Tabel 4. Skenario proses dekripsi

Identifikasi			
Nama *Use Case*	Dekripsi		
Aktor	*User*		
Deskripsi	*User* melakukan dekripsi *fileaudio* MP3		
Skenario Utama			
Kondisi Awal	Menampilkan menu utama		
Aksi Aktor		Reaksi Sistem	
		1	Menampilkan menu utama
2	Memilih menu dekripsi	3	Menampilkan form dekripsi
4	Menekan tombol *browse* pada *textboxinputfile*	5	Membuka folder dimana tempat *fileaudio* MP3 terenkripsi tersimpan di memori computer
6	Menginputkan kunci privat	7	*Textbox* pada kunci privat terisi kunci privat yang

			diinputkan
8	Menekan tombol proses	9	Proses dekripsi berjalan sampai selesai mendekripsi *fileaudio* MP3 terenkripsi
		10	Menampilkan pesan file berhasil didekripsi kemudian *fileaudio* MP3 terenkripsi yang didekripsi
		11	Tersimpan di memori komputer
Alternatif 1			
		9	Proses dekripsi gagal apa bila kunci privat yang diinputkan salah
		10	Menampilkan pesan gagal mendekripsi *file*
Kondisi Akhir	Menampilkan form menu dekripsi jika menekan tombol ok pada pesan *file* berhasil didekripsi		



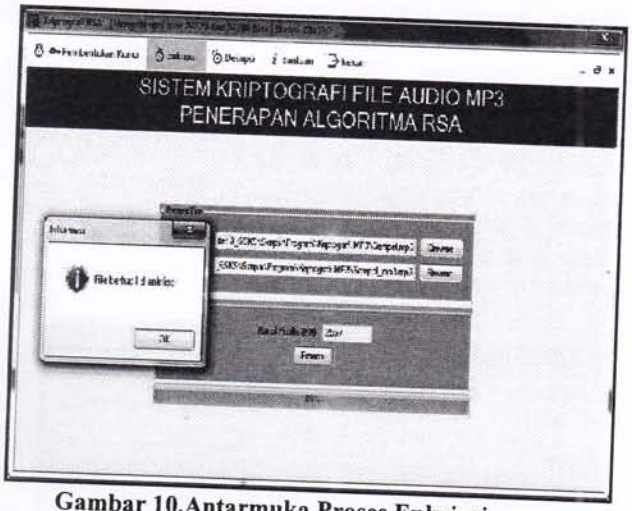
Gambar 9.Antarmuka Pembentukan Kunci

4. HASIL DAN PEMBAHASAN

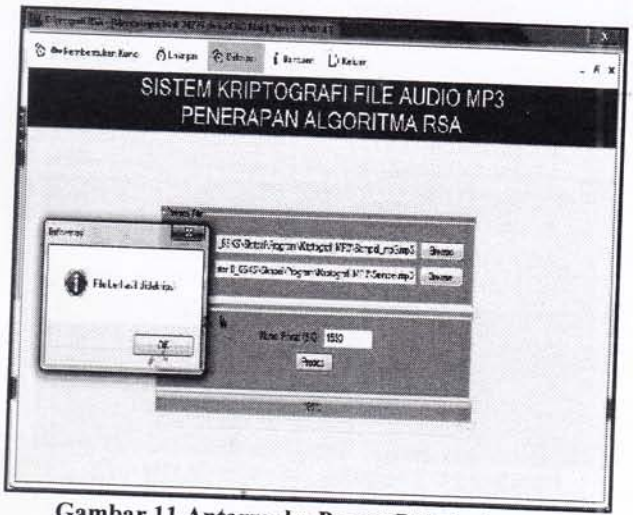
4.1 Hasil Implementasi

Sistem kriptografi RSA ini dibangun dengan menggunakan bahasa pemrograman Visual Basic, dan dijalankan pada komputer bersistem operasi Windows.Antarmuka pemakai sistem ini terdiri atas antarmuka menu utama (Gambar 8) yang berisi menu pembentukan kunci, menu enkripsi, menu dekripsi, menu bantuan, dan menu keluar (dari aplikasi).

Gambar 8.Antarmuka Menu Utama



Gambar 10.Antarmuka Proses Enkripsi

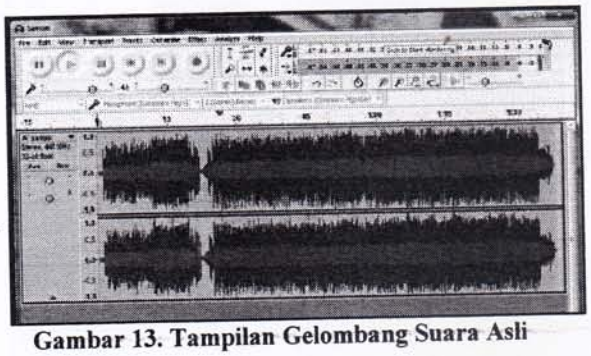


Gambar 11.Antarmuka Proses Dekripsi

Gambar 12.Antarmuka Bantuan

4.2 Pengujian Data

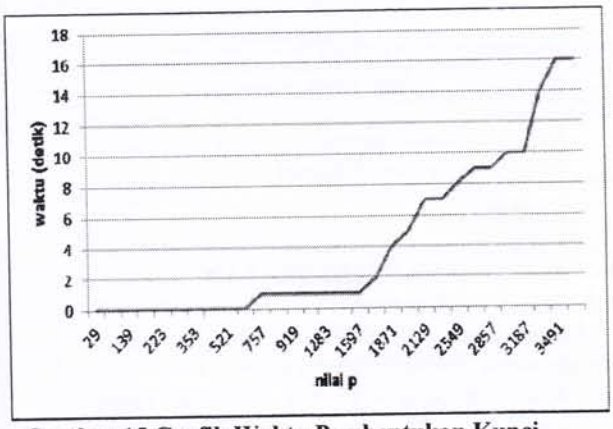
Untuk memastikan bahwa proses enkripsi dan dekripsi bekerja dengan baik, telah dilakukan perbandingan gelombang suara sebelum dan sesudah enkripsi dilakukan Gambar 13 menampilkan gelombang suara file MP3 sebelum dienkripsi, sedangkan Gambar 14 menampilkan gelombang suara setelah dienkripsi. Dari hasil pengujian terlihat bahwa ada perbedaan gelombang suara sebelum dan setelah dilakukan proses enkripsi. Hal ini berarti bahwa data asli telah mengalami perubahan setelah melalui proses enkripsi.



Gambar 13. Tampilan Gelombang Suara Asli

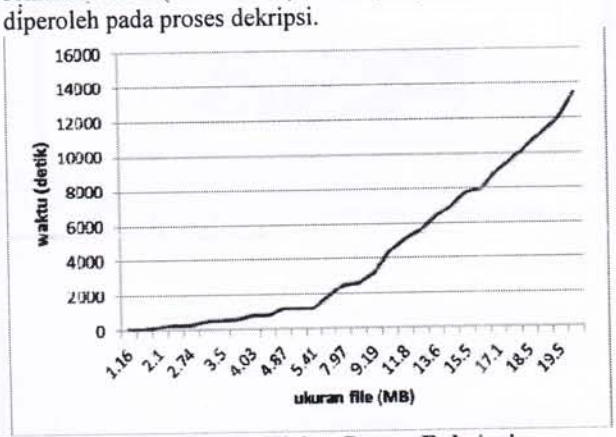
Gambar 14. Tampilan Gelombang Suara SetelahDienkripsi

Pada proses pembentukan kunci, hasil pengujian dengan 30 data sampel memperlihatkan bahwa semakin besar nilai p yang digunakan untuk membentuk kunci privat dan kunci publik, maka waktu proses yang dibutuhkan semakin lama (Gambar 15). Hal yang sama juga terjadi untuk nilai q yang semakin besar, maka waktu pembentukan kunci akan semakin lama.Hal ini berarti bahwa semakin besar nilai p atau nilai q yang digunakan, waktu komputasi yang dibutuhkan juga semakin lama.



Gambar 15.Grafik Waktu Pembentukan Kunci

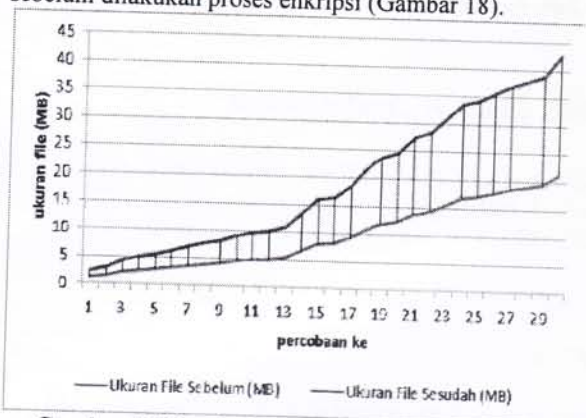
Pada proses enkripsi, hasil pengujian dengan 30 data sampel memperlihatkan bahwa waktu yang dibutuhkan untuk melakukan proses enkripsi akan semakin besar jika ukuran file yang akan dienkripsi semakin besar (Gambar 16). Hasil yang sama juga diperoleh pada proses dekripsi.



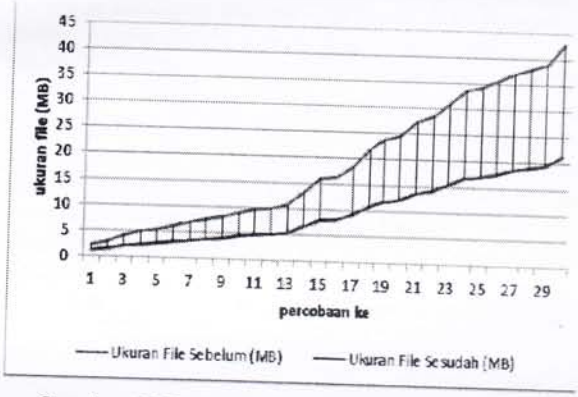
Gambar 16. Grafik Waktu Proses Enkripsi

Pengujian juga dilakukan untuk melihat perubahan ukuran file sebelum dan setelah mengalami proses enkripsi dan dekripsi. Hasil pengujian 30 data sampel menunjukkan bahwa ukuran file berubah menjadi lebih besar dari ukuran asli setelah mengalami proses enkripsi (Gambar 17). Sebaliknya pada saat dilakukan proses dekripsi

ukuran file menjadi lebih kecil atau dengan kata lain, ukuran file kembali ke ukuran semula seperti sebelum dilakukan proses enkripsi (Gambar 18).



Gambar 17.Perubahan Ukuran File Proses Enkripsi



Gambar 18.Perubahan Ukuran File Proses Dekripsi

4.3 Analisis dan Pembahasan

Berdasarkan pengujian yang dilakukan terhadap sistem kriptografi untuk file audio MP3 dengan penerapan algoritma RSA, didapatkan kesimpulan sebagai berikut :

1. Pengujian pembentukan kunci dilakukan sebanyak 30 kali uji. hasil yang didapat yaitu semakin besar p dan q bilangan prima yang digunakan maka semakin lama proses perhitungan pembentukan kunci yang dilakukan.
2. Pengujian data yang dilakukan yaitu 30 data uji. Hasil data uji yaitu besar kecilnya kapasitas *file audio* MP3 mempengaruhi lama proses enkripsi dan dekripsi. Semakin besar *file audio* MP3 yang dienkripsi maka semakin lama waktu yang dibutuhkan untuk proses enkripsinya begitu juga dengan dekripsi.
3. Proses pembentukan kunci RSA yang didapat untuk kunci publik dan kunci privat bersifat acak karna menyesuaikan hasil dari kunci publik yang relatif prima terhadap $\phi(r)$ dan semakin besar nila p dan q bilangan prima yang digunakan, semakin lama proses perhitungan pembentukan kunci RSA.
4. Proses enkripsi dan dekripsi memerlukan waktu yang cukup lama, hal ini dikarenakan proses enkripsi yang dilakukan perblok data dan dilakukan pada semua *bit* yang ada dalam MP3 mulai dari *bit header* hingga *bit* data MP3 tersebut begitu juga untuk proses dekripsinya. Jadi semakin besar kapasitas *file audio* MP3 yang dienkripsi maka semakin lama waktu proses enkripsi yang dibutuhkan begitu untuk dekripsinya.
5. *File audio* MP3 yang dienkripsi akan bertambah kapasitasnya misal *file audio* MP3 yang dienkripsi berkapasitas 1,5 MB akan mendapatkan hasil enkripsi dengan kapasitas 3 MB karena *file audio* MP3 merupakan *file audio* hasil kempresi *lossy* dan itu dikarenakan kelemahan algoritma RSA.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil pembangunan aplikasi sistem kriptografi untuk mengamankan file audio MP3 dengan penerapan algoritma RSA, maka dapat disimpulkan bahwa algoritma RSA dapat diterapkan untuk proses enkripsi dan dekripsi file audio MP3 pada aplikasi sistem kriptografi.

5.2 Saran

Adapun saran yang dapat dijadikan sebagai acuan dalam penyempurnaan penerapan algoritma RSA pada sistem kriptografi untuk file audio MP3, sebagai berikut.

1. Pada penelitian selanjutnya aplikasi sistem kriptografi ini dapat dikembangkan menjadi aplikasi berbasis android, untuk melihat apakah sistem kriptografi ini dapat efisien digunakan dalam sistem berbasis android dan mempermudah pengujian aplikasi untuk dapat dilakukan dimana saja dan kapan saja karena sistem berbasis android sudah sangat akrab dalam kehidupan masyarakat.
2. Pada skripsi ini difokuskan hanya untuk penerapan algoritmanya saja untuk mengetahui apakah algoritma RSA efektif digunakan untuk mengamankan *file audio* MP3, untuk skripsi penerapan algoritma RSA pada sistem kriptografi untuk *file audio* MP3 selanjutnya sebaiknya disertakan studi kasus untuk lebih memperjelas tujuan pembuatan aplikasi seperti studi kasus di studio rekaman musik.
3. Apabila menggunakan studi kasus sebaiknya aplikasi dirancang sesuai kebutuhan bisa juga seperti sistem kriptografi yang dibangun

difokuskan mengamankan *file audio* MP3 berupa lagu baru yang akan dirilis agar lagu tersebut tidak tersebar sebelum resmi dipublikasikan.

4. Sistem kriptografi yang dibangun dapat difokuskan pada pengamanan *file audio* MP3 berupa lagu baru yang berkualitas suara paling jernih seperti *file audio* MP3 yang mempunyai *bitrate* 320 kbps, agar tidak tersebar secara bebas yang akhirnya dapat merugikan pihak yang merilis lagu.

DAFTAR PUSTAKA

[1] Alvianto, R. A. dan Darmaji, 2015, Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android, *Jurnal Sainsdan Seni ITS Vol. 4 No.1.*

[2] Arifin, Z., 2009, Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman, *Jurnal Informatika Mulawarman Vol. 4 No. 3.*

[3] Dewi, N. K. K., 2013, Implementasi Algoritma RC6 untuk Proteksi File MP3, *Publikasi Jurnal Skripsi PJ-01.*

[4] Hamzah, R., 2011, Implementasi Algoritma RSA dan Blowfish untuk Enkripsi dan Dekripsi Data Menggunakan Delphi 7, *Skripsi*, Jurusan Teknik Informatika Universitas Islam Syarif Hidayatullah, Jakarta.

[5] Maradilla, T., 2009, Aplikasi Steganografi untuk Penyisipan Data ke dalam Citra Digital, *Universitas Gunadarma*, Jakarta.

[6] Munir, R., 2004, *Pengolahan Citra Digital dengan Pendekatan Algoritmik*,Informatika, Bandung.

[7] Munir, R., 2006, *Kriptografi*, Informatika Bandung, Bandung.

[8] Setiawan, W., 2003, Penggunaan Kode Huffman dalam Kompresi Audio MP3, *Jurnal Ilmu Komputerdan Teknologi Informasi.*

[9] Stephanus, 2013, Penerapan Algoritma Kriptografi Asimetri RSA pada Pesan Video, *Skripsi*, Jurusan Teknik Informatika Sekolah Tinggi Teknik Musi Palembang, Palembang.

[10] Syaputra, H., 2011, Aplikasi Enkripsi Data pada File Teks dengan Algoritma RSA *(Rivest Shamir Adleman), Skripsi*, Jurusan Teknik Informatika Sekolah Tinggi Teknik Musi Palembang, Palembang.

[11] Triorizka, A., 2010, Penerapan Algoritma RSA untuk Pengamanan Data dan Digital Signature .NET, *Naskah Publikasi.*

[12] Wibowo, I., Susanto B. dan Karel T. J., 2009, Penerapan Algoritma Kriptografi Asimetri RSA untuk Keamanan Data di Oracle, *Jurnal Informatika Vol. 5 No. 1.*