ENKRIPSI DATA AUDIO MENGGUNAKAN METODE KRIPTOGRAFI RSA

Awang Harsa K[1)], Andi Yusika R[2)], Asfami Ansharie[3)]

[1,2,3]Teknik Informatika, STMIK Widya Cipta Dharma
[1,2,3]Jl. Porf. M. Yamin No.25, Samarinda, 75123
E-mail : awangkid@gmail.com[1)], yu5h1k4@gmail.com[2)], asfami93@gmail.com[3)]

ABSTRAK

Penerapan Metode RSA pada Enkripsi Data *Audio*, merupakan bentuk penelitian untuk membuktikan bahwa Metode Kriptografi dapat digunakan untuk pencarian solusi, khususnya pada permasalahan kerahasian data. Tujuan dari penelitian ini adalah merancang dan membangun sebuah aplikasi yang dapat menyelesaikan masalah enkripsi data untuk merahasiakan sebuah data dengan menggunakan dua kunci yaitu, proses enkripsi dengan menggunakan kunci *public* dan kunci *Private* digunakaan untuk melakukan proses dekripsinya, dengan menggunakan bahasa pemrograman *Visual Basic .NET*. Dalam penelitian ini, teknik pengumpulan data yang digunakan adalah studi pustaka. Metode pengujian yang digunakan adalah metode pengujian *White-Box* yang digunakan untuk menguji *listing Coding* Proses enkirpsi dan dekripsinya, *Black Box* digunakaan untuk menguji apakah aplikasi berjalan dengan algoritma kunci yang sesuai, menguji daya tahan hasil enkripsi data apakah bisa di enkripsi dengan metode kriptografi lainnya.

Dengan menggunakan tahapan pengembangan *Prototype* yaitu *Tahapan* Perancangan Antarmuka, *Implementasi,* Pengujian Sistem, agar dalam membangun Aplkasi Enkripsi Data *Audio* menggunakan Kriptografi RSA dengan terstruktur. Aplikasi ini dapat menjadi salah satu media alternatif untuk Keamanan data.

Kata Kunci: *Microsoft Visual Studio Ultimate* 2012*, Kriptografi,* Enkripsi Data *Audio,* Metode RSA..

1. PENDAHULUAN

Keamanan pada komputer lebih mengarah kepada keamanan data yang tersimpan di dalam komputer tersebut. Salah satu cara untuk mengamankan data komputer adalah melakukan enkripsi pada sebuah data atau *file* yang kita anggap penting. Teknik enkripsi ini adalah teknik untuk merubah bentuk data, sehingga orang lain tidak mengetahui bentuk asli dari data tersebut.

Untuk melakukan pengiriman data secara *manual*, sangat memungkinkan diketahui oleh orang lain. Untuk mengirimkan data yang bersifat rahasia, maka diperlukan teknik enkripsi untuk merubah bentuk data tersebut agar tidak mudah dibaca atau dilihat oleh orang lain. Setelah melalui teknik enkripsi, data yang telah dirubah tetap dapat terlihat. Tetapi data yang telah melalui proses enkripsi memiliki bentuk yang telah berubah dari bentuk aslinya. Data adalah keterangan tertulis mengenai sesuatu fakta yang masih berdiri sendiri, belum mempunyai arti sebagai kelompok, belum terhubung satu sama lain, dan belum diolah sesuai keperluan tertentu.

Dalam penelitian ini data yang akan dienkripsi adalah data *audio* karena enkripsi data *audio* relatif berukuran kecil jadi proses enkripsi menjadi lebih cepat, enkripsi relatif ringan, *file audio* sering digunakan sebagai pesan pribadi untuk orang-orang tertentu pada saat ini.

Teknik enkripsi yang digunakan untuk mengenkripsi sebuah data adalah dengan metode RSA yang lebih menekankan proses enkripsi dan dekripsi yang memiliki dua kunci yaitu *private-key* kunci yang digunakan untuk mengdekripsi data pada pemilik data dan hanya pemilik data yang tau kunci ini, sedangkan *public-key* adalah kunci yang dapat disebarkan secara luas tanpa harus khawatir karena kunci rahasia tersebut hanya dapat di dekripsi hanya oleh pengirim dan penerima.

2. RUANG LINGKUP PENELITIAN

Permasalahan difokuskan pada :

1. Dalam pembuatan aplikasi ini hanya akan membahas mengenai penyandian pada *file audio*.
2. Format *file audio* yang dapat dienkripsi dengan aplikasi ini adalah *file* yang berekstensi mp3,wav,wma,ogg.
3. Maksimal karakter kunci yang digunakan adalah 3 digit, hal ini dilakukan agar proses enkripsi tidak memakan waktu yang terlalu lama.
4. Karakter kunci yang digunakan hanya angka saja.
5. Bilangan Prima yang digunakan untuk kunci p dan q harus menghasilkan nilai 1 menggunakan perhitungan fpb.
6. Proses dekripsi menghasilkan *chiperteks* yang berekstensi *file* rsafile.
7. *File Audio* yang telah dienkripsi hanya dapat didekripsi kembali ke bentuk semula dengan menggunakan perhitungan kunci yang telah ditentukan saat melakukan enkripsi.

.

3. BAHAN DAN METODE

Adapun bahan dan metode yang gunakan dalam penelitian ini yaitu:

3.1 Kriptografi

Menurut Dony, (2008). Kriptografi (*Cryptography*) berasal dari bahasa Yunani yaitu dari kata *Crypto* dan *Graphia* yang berarti penulisan rahasia. Kriptografi adalah suatu ilmu yang mempelajari penulisan secara rahasia. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptology*. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah.

Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data asli (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali.*Ciphertext* inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, *ciphertext* tersebut ditranformasikan kembali ke dalam bentuk *plaintext* agar dapat dikenali. Proses tranformasi dari *plaintext* menjadi *ciphertext* disebut proses *Encipherment* atau enkripsi (*encryption*), sedangkan proses mentransformasikan kembali *ciphertext* menjadi *plaintext* disebut proses dekripsi (*decryption*).Untuk mengenkripsi dan mendekripsi data. Kriptografi menggunakan suatu algoritma (*cipher*) dan kunci (*key*). *Cipher* adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi data. Sedangkan kunci merupakan sederetan *bit* yang diperlukan untuk mengenkripsi dan mendekripsi data.

Algoritma kriptografi modern tidak lagi mengandalkan keamanannya pada kerahasiaan algoritma tetapi kerahasiaan kunci. *Plaintext* yang sama bila disandikan dengan kunci yang berbeda akan menghasilkan *ciphertext* yang berbeda pula.

3.2 Jenis Algoritma Kriptografi

Algoritma kriptografi dibagi atas dua golongan yaitu di halaman berikut :

1. *Symmetric Algorithms*

Algoritma kriptografi simeteris atau disebut juga algoritma kriptografi konvensioanl adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Proses enkripsi-dekripsi algoritma kriptografi simetris dapat dilihat pada gambar dibawah ini :

Gambar 1. Algoritma Kriptografi Simetris

Algoritma kriptografi simeteris dibagi menajdi 2 kategori yaitu algoritma aliran (*Stream Ciphers*) dan algoritma blok (*Block Ciphers*). Pada algoritma aliran, proses penyandiannya berorientasi pada satu *bit* atau satu *byte* data. Sedang pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan *bit* atau *byte* data (per blok).

2. *Asymmetric Algorithms*

Algoritma kriptografi nirsimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Algoritma ini disebut juga algoritma kunci umum (*public key algorithm*) karena kunci untuk enkripsi dibuat umum (*public key*) atau dapat diketahui oleh setiap orang, tapi kunci untuk dekripsi hanya diketahui oleh orang yang berwenang mengetahui data yang disandikan atau sering disebut kunci pribadi (*private key*). Proses enkripsi-dekripsi algoritma asimetris dapat dilihat pada gambar dihalaman berikutnya :

Gambar 2. Algoritma Kriptografi Asimetris

Pada algoritma *public key* ini, semua orang dapat mengenkripsi data dengan memakai *public key* penerima yang telah diketahui secara umum. Akan tetapi data yang telah terenkripsi tersebut hanya dapat didekripsi dengan menggunakan *private key* yang hanya diketahui oleh penerima.

3.3 Dasar Matematika Kriptografi

Dasar-dasar matematika yang digunakan kriptografi adalah Pembagi Bersama Besar, Aritmatika Medulo.

1. Pembagi Bersama Terbesar (PBB)

Menurut Renaldi (2012) Jika a dan b adalah dua bilangan bulat tidak nol. Pembagi bersama terbesar (PPB-*Greatest Common Divisor* atau GCD*)* dari a dan b adalah bilangan bulat terbesar d sedemikian sehingga d | a dan d | b.

2. Aritmetika modular

Menurut Arif (2008), Aritmetika modular merupakan operasi matematika yang banyak diimplementasikan pada metode kriptografi. Pada metoda kriptografi *asymatric*, Dalam kriptografi modular, *domain* yang digunakan adalah *subset* dari bilangan bulat dan bersifat *finite* (terbatas, besarnya *domain* merupakan bilangan bulat). *Domain* dari aritmatika modular adalah {0, 1, 2,….,n-1}. dimana n adalah besarnya *domain.* Aritmatika disebut dengan aritmatika modulo n, dengan pertambahan dan perkalian seperti aritmatika biasa menghasilkan bilangan yang termasuk didalam *domain.* Jika hasil merupakan bilangan diluar *domain* maka bilangan harus dikurangi dengan kelipatan n sampai menghasilkan bilangan didalam *domain.*

3. Algoritma Euclidean

Menurut Renaldi (2012) Algoritma euclidean merupakan suatu algoritma yang digunakan untuk mencari *Greatest Common Divisor* (GCD) atau biasa dikenal dengan Pembagi Bersama Terbesar (PBB) dari dua bilangan, khususnya untuk bilangan-bilangan yang sangat besar sehingga tidak perlu mencari faktorisasi prima dari kedua bilangan tersebut. Algoritma euclidean ini biasanya diperkenalkan kepada mahasiswa yang sedang mempelajari mata kuliah teori bilangan tetapi tidak jarang juga soal-soal olimpiade matematika dan ujian universitas membutuhkan cara ini untuk menyelesaikan soal yang diberikan. Oleh karena itu Istana Matematika ingin menjelaskan tentang pengertian dari algoritma yang menarik ini algoritma euclidean.

4. Bilangan Prima

Menurut Rinaldi (2012), Bilangan Bulat Postif yang mempunyai aplikasi penting dalam ilmu komputer dan matematika diskrit adalah bilangan prima. Bilangan prima adalah bilangan bulat postif yang lebih besar dari 1 yang habis dibagi oleh 1 dan dirinya sendiri.

Sebagai contoh, 23 adalah bilangan prima karena ia hanya habis dibagi oleh 1 dan 2, karena bilangan prima

harus lebih besar dari 1, maka barisan bilangan prima dimulai dari angka 2 selanjutnya 3,5,7,11,13, …. Seluruh bilangan Prima adalah bilangan ganjil kecuali 2 yang merupakan bilangan genap.

Bilangan selain prma disebut bilangan komposit (*composite*). Misalnya 20 adalah bilangan komposit karena dapat dibagi oleh 2, 4,5, dan 10, selain nilai 1 dan 20 itu sendiri.

3.4 Algoritma RSA

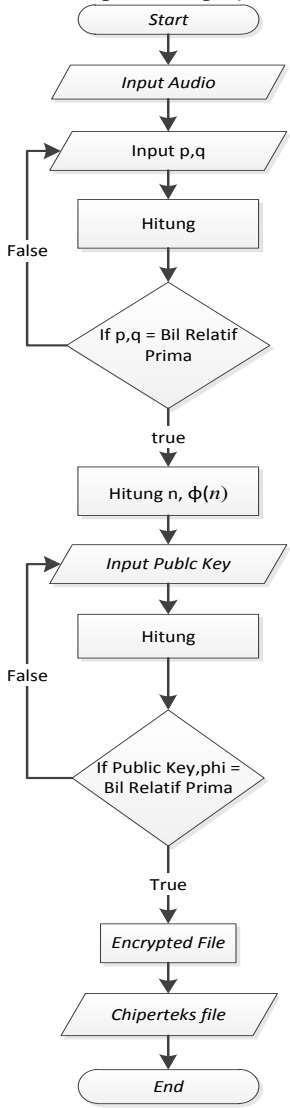
Menurut Rinaldi (2012), Algoritma ini pertama kali dikenalkan oleh ketiga orang yaitu Ron Rivest, Adi Shamir, dan Len Adleman pada tahun 1976, mereka bertiga adalah peneliti dari MIT (*Massachussets Institute of Technology*), mereka memperkenalkan algoritma ini untuk mengirimkan kunci rahasia kepada penerima. Pengiriman kunci rahasia pada saluran publik (telepon, pos, *internet*) sangat tidak aman. Oleh karena itu, kunci harus dikirim melalui saluran kedua yang benar-benar aman. Saluran kedua tersebut umunya lambat dan mahal.

Algoritma ini tidak berdasarkan pada proses enkripsi dan dekripsi, melainkan lebih kepada proses matematika yang dilakukan untuk menghasilkan kunci rahasia yang dapat disebarkan secara bebas tanpa harus khawatir karena kunci rahasia tersebut hanya dapat didekripsi hanya oleh pengirim dan penerima pesan. Dasar dari algoritma ini memfaktorkan bilangan yang besar menjadi faktor-faktor prima.

4. RANCANGAN ALGORITMA

Perancangan aplikasi Enkripsi Data Audio Menggunakan Metode Kriptografi RSA ini menggunakan *Flowchart* sebagai salah satu cara untuk mempermudah dalam pembuatan aplikasi ini.

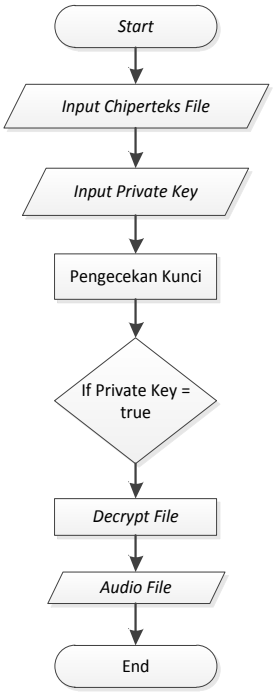
1. tahapan *flowchart* tahapan enkripsi *file audio* :



Gambar 3. *Flowchat* Enkripsi *File Audio*

Flowchart Enkripsi *File Audio* Merupakan gambaran keseluruhan diagram alir proses enkripsi yang dimulai dari memasukan *file audio* yang ingin di enkripsi, setelah *file* sudah dipilih di lanjuntkan dengan memasukan kunci yang digunakan pada tahapan ini kunci yang dimasukan adalah p dan q bilang prima yang di rahasiakan selanjutnya nilai p dan q di hitung untuk mengetahui dua nilai tersebut relatif prima atau tidak bila nilai relatif prima maka proses dilanjutkan akan tetapi bila nilai tidak relatif prima proses akan kembali ke *input* p dan q, proses kedua masukan juga *public key*. Setelah pemasukan kunci selesai lanjut ke proses hitung nilai e (Kunci Publik), φ(*n*) proses ini digunakan untuk menentukan kunci yang akan digunakan bisa dipakai atau tidak tergantung dari nilai φ(*n*) apakah relatif prima untuk bilangan e (*Public Key)* jika nilai e relatif prima terhadap φ(*n*) maka proses enkripsi bisa dilakukan dan jika tidak relative prima terhadap φ(*n*) maka aplikasi tidak akan melanjutkan ke proses selanjutnya. Proses yang terakhir proses enkripsi disini nilai *plainteks audio* akan di ubah sesuai metode RSA untuk di jadikan *file chiperteks* setelah proses selesai maka sistem akan menghasilkan *output file chiperteks* dan semua proses sudah selesai dilakukan.

2. Di bawah ini adalah tahapan *flowchart* tahapan Dekripsi *file audio* :



Gambar 4. *Flowchart* Tahapan Dekripsi *File Audio*

Pada Gambar 4 *Flowchart* Dekripsi *File Audio* Merupakan gambaran keseluruhan diagram alir proses Dekripsi yang dimulai dari memasukan *file* yang telah terenkripsi (*Chiperters File*) setelah *file* sudah dipilih di lanjuntkan dengan memasukan kunci yang digunakan pada tahapan ini kunci yang dimasukan adalah p dan q bilang prima yang di rahasiakan dan diikuti pula dengan *Private Key* pada aplikasi. Selanjutnya proses *Count Private Key* adalah proses menentukan apakah kunci *private* yang di gunakan itu benar atau tidak dengan dilakukannya perhitungan ulang pada nilai p dan q dan mangasilkan nlai n dan *phi n* maka di faktorkan nilai d (*Private Key*) untuk mencari nilai e (*Public Key*) bila hasilnya sesuai maka proses dekripsi bisa dilakukan. Dan di tahap terakhir proses pendekripsian *file* yang dimana *file chiperteks* dikembalikan seperti *file* awal dan aplikasi menghasilkan *output file audio* yang tadinya terenkripsi dan semua proses selesai.

5. IMPLEMENTASI

Tahap implementasi atau tahap membangun sistem menjadi nyata dan mengkodekan aplikasi. Adalah Tampilan Antarmuka (*Interface*)

merupakan tahapan yang bertujuan mengubah hasil dari rancangan sistem menjadi bentuk nyata. Pada saat pertama kali aplikasi dijalankan maka akan muncul sebuah tampilan seperti gambar di bawah ini.

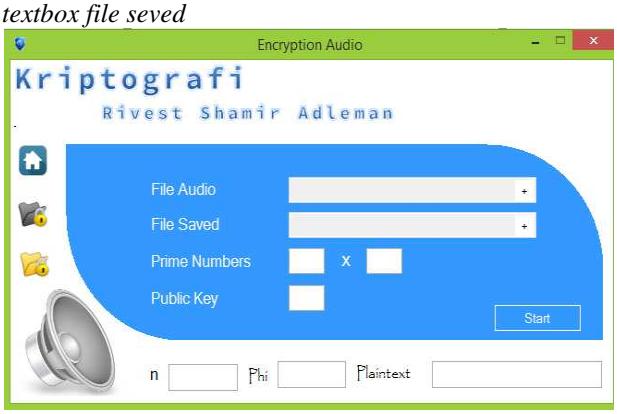
2. Tampilan Awal *From*

Di bawah ini adalah tampilan awal *from* enkripsi *file audio* yang menampilkan tiga *button Home, button encrypt, button decrypt.*

Gambar 5. Tampilan Awal *From*

3. Tampilan *Frame* Enkripsi

Tampilan *Frame* Enkripsi bila di aktifkan terdapat dua *button* tambahan yaitu *button Browse* yang terdapat dalam textbox *file audio* dan *button change* didalam *textbox file seved*



Gambar 6. Tampilan *Frame Enkripsi*

4. Tampilan *Frame* Dekripsi

Tampilan *Frame* dekripsi bila di aktifkan terdapat dua *button* tambahan yaitu *button Browse* yang terdapat dalam textbox *file audio* dan *button change* didalam *textbox file seved*

Gambar 7. Tampilan *Frame Dekripsi*

5. Pecobaan Menggunakan Aplikasi

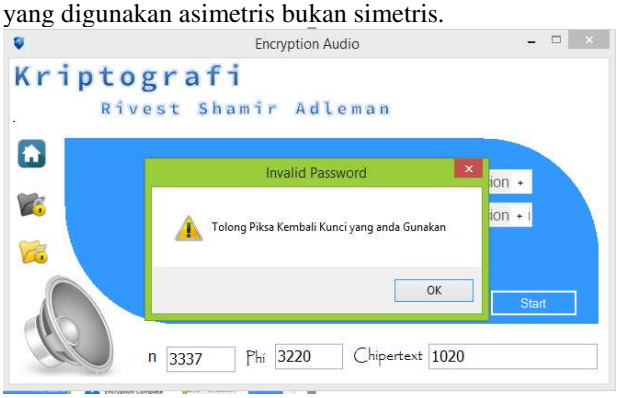
Pengujian algoritma kunci yang digunakan bertujuan untuk mengetahui apakah aplikasi yang dibangun ini telah sesuai dengan metode dan algoritma yang digunakan.

Gambar 8. Percobaan Enkripsi Menggunakan Kunci Publik

Proses Enkripsi berhasil dengan menggunakan variabel nilai sebagai berikut :

p = 47 q = 71 Publik Key = 79

Percobaan selanjutnya proses dekripsi yang mengunakan kunci yang sama/kunci publik dan aplikasi tidak mengizinkan kunci tersebut karena algoritma kunci yang digunakan asimetris bukan simetris.



Gambar 9. Percobaan Dekripsi Menggunakan Kunci Publik

Percobaan selanjunnya proses dekripsi menggunakan kunci privat dan proses dekripsi pun bisa dilakukan.

Gambar 10. Proses Dekripsi Menggunakan Kunci *Pirvate*

6. KESIMPULAN

Dengan adanya hasil penelitian yang dilakukan dan berdasarkan uraian uraian yang dibahas dalam bab-bab sebelumnya, maka dapat ditarik kesimpulan bahwa :

1. Metode RSA yang diaplikasikan pada aplikasi ini dapat berfungsi dengan baik serta menggunakan kunci publik untuk enkripsi dan kunci privat untuk dekripsi.
2. Waktu yang digunakan untuk melakukan proses enkripsi tergantung dari Ukuran *File* dan digit kunci yang digunakan.
3. Enkrip tidak dapat berfungsi pada format audio yang terdaftar di aplikasi.
4. Semakin besar ukuran *file audio*, maka semakin lama waktu estimasi proses enkripsi, hal ini dikarenakan lamanya proses perhitungan.
5. Implementasi enkripsi rsa *file audio* hanya menghasilkan *file* yang berbeda yang tak bisa digunakan sama sekali.

7. SARAN

Adapun saran-saran yang dapat dikemukakan yaitu sebagai berikut :

1. Dalam Pemrosesan Enkripsi dan Dekripsi kunci yang digunakan masih tergolong biasa maka lebih baik lagi untuk kunci di enkripsikan menggunakan metode yang berbeda.
2. Aplikasi dapat di kembangkan ke operasi sistem *handphone* seperti android dan *windows phone*.
3. Kunci yang digunakan dalam implementasi masih tergolong lemah karena pendeknya jumlah karakter, maka diharapkan untuk penelitian yang lebih lanjut ada metode pembangkitan karakter.

8. DAFTAR PUSTAKA

Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi*. Penerbit : ANDI. Yogyakarta.

Arif 2008. *Kriptografi visual pada biner dan citra berwarna serta pengembangannya dengan setenografi*

Munir, Rinaldi 2012, *Matematika Diskrit Revisi Kedua*, Informatika, Bandung

Nugroho Adi. *Rekayasa Perangkat Lunak Berorientasi Objek Dengan Metode USDP*. Yogyakarta: Andi, 2010

Prayudi, Yudi, Idham Halik. 2005. *Studi Analisis Algoritma Rivest Code 6 (RC6) Dalam Enkripsi/Dekripsi Data*. Seminar Nasional Aplikasi Teknologi Informasi 2005 (SNATI 2005), Yogyakarta.

Simarmata. Janner. 2010, *Rekayasa Perangkat Lunak,* Andi Offset, Yogyakarta.

Tri Rahajoeningroem, Muhammad Aria, 2011, *Studi Dan Implementasi Algoritma RSA untuk Pemangamanan Data Transkrip Akademik Mahasiswa*, Jurnal Teknik Elecktro majalah ilmiah unikom Vol 8, Universitas Komputer Indonesia

Widya, Abdul Kadir. 2009. *Dasar Perancangan dan Implementasi Database Relasional. Yogyakarta : Andi Offset.*

Yunizar, Muhammad. 2011. *Teknik Uji Coba Black Box dan White Box.* Universitas Gunadarma. Jakarta