ENKRIPSI FILE AUDIO MP3 DAN WAV MENGUNAKAN METODE KRIPTOGRAFI RSA (RIVEST SHAMIR ADLEMAN) DAN ELGAMAL

Puspita sari¹, Fifi Safitri², Ajeng Listianingrum³, Nurfika Sari⁴, M. Arif Hasan⁵
^{1,2,3,4,5}Teknik Informatika, Universitas Lancang Kuning.

Jl.Yos Sudarso KM.8, Umban sari, Kec.Rumbai, Rumbai,Pekanbaru, Riau 28266
puspitap36@gmail.com, fifisafitri@gmail.com, ajenglistianingrum@gmail.com, nurfikasarinist@gmail.com, m.arif@unilak.ac.id

ABSTRAK

Perkembangan yang terjadi teknologi digital diikuti dengan perkembangan masyarakat yang mudah menciptakan file maupun mengakses file di media digital, dan mendokumentasikan file yang kita miliki. Hal tersebut dapat berbahaya untuk file yang kita ciptakan. Keamanan, dan kerahasiaan sebuah file sangatlah penting. Seringkali kita saat mengirim data kepada seseorang file tersebut tidak hanya sampai ke penerima, tetapi orang lain juga menerimanya, mereka melakukan penyadapan atau pembajakan supaya juga menerima data dari si pengirim. Untuk mengatasi hal tersebut, diperlukan aplikasi pengaman file salah satu nya file audio. . Ada beberapa algoritma kriptografi yang menggunakan algoritma kunci publik yaitu RSA(Rivest Shamir Adleman) dan ElGamal. Pertama file audio akan di enkripsikan kedalam metode RSA (Rivest Shamir Adleman) dan dari hasil plaintext nya akan di dapat ciphertext dari RSA kemudian ciphertext metode RSA tadi akan di deskripsikan menggunakan metode ElGamal. Bahasa pemrograman yang dipakai adalah menggunakan Java Netbeans dan data yang diolah adalah file WAV dan MP3. Berdasarkan penelitian terdahulu, metode RSA(Rivest Shamir Adleman) dan ElGamal dapat mengamankan file-file kita terutama file audio.

Kata Kunci : *Kriptografi, RSA, ElGamal, Asimetris, MP3, WAV.*

1. Pendahuluan

Kriptografi berasal dari bahasa Yunani yang terdiri dari kata *cryptos* yang memiliki arti tersembunyi dan *graphein* yang berarti menulis. Kriptografi merupakan bidang ilmu komputer dan matematika yang berfokus pada teknik keamanan komunikasi antara dua pihak. Maka dengan adanya kriptografi dapat mengamankan file dari serangan atau pencurian dari orang yang akan mencuri data kita[1]

Keamanan data lebih mengarah kepada keamanan file, baik yang kita simpan di laptop maupun di handphone kita masing-masing. Cara agar file kita aman tanpa ada yang mengakses adalah dengan memberi pengaman atau sandi pada file kita tersebut, teknik ini disebut teknik enkripsi. Teknik ini adalah teknik yang mengubah bentuk file kita sehingga orang yang menyadap tidak mengetahui bentuk file kita.

Pengiriman file secara manual memungkinkan file tersebut akan diketahui oleh orang asing yang tidak berhak untuk mengakses ataupun melihatnya. Jika kita ingin mengirim file yang memiliki kerahasiaan, maka diperlukan keamanan file yang akurat agar tidak sembarang orang bisa melihat ataupun mengakses file kita. File adalah sebuah informasi, baik informasi pribadi maupun informasi publik yang tersimpan di dalam sebuah penyimpanan. File bisa berupa audio, dokumen, foto, dll. Penelitian kali ini file yang akan diteliti adalah file audio. Teknik ini digunakan dengan menggunakan metode RSA (Rivest Shamir Adleman) dan ElGamal.

Dari penjelasan di atas muncul sebuah masalah, yaitu bagaimana membuat suatu file yang kita miliki terjaga keamanannya dan tidak semua orang bisa mengaksesnya, maka tujuan dari penelitian ini adalah membuat suatu aplikasi yang bisa mengenkripsi atau merahasiakan file audio yang kita miliki, agar file yang kita kirim aman sampai ke penerima tujuan.

2. Tinjauan Pustaka

A. Tinjauan Penelitian Terdahulu

Dalam penelitian ini kami melihat beberapa referensi jurnal terdahulu yang bertujuan untuk memperkaya mengenai pembahasan penelitian yang kami lakukan. Ada beberapa referensi jurnal penelitian dalam

penelitian ini yang berhubungan dengan RSA dan ElGamal itu sendiri.

- a. Jurnal pertama diambil dari Jurnal Nasional Teknologi Informatika dan Jaringan dan diteliti oleh Raja Nasrul Fuad dan Haikal Nando Winata pada tahun 2017 pada era saat ini pengamanan untuk file audio terutama file wav sangat berkembang pesat, sehingga pertukaran data dan informasi sangat mudah dilakukan, dan kita sering kebobolan dalam pengamanan data kita sendiri. Data yang kita miliki harus memiliki keamanan, jika kita tidak mengamankan data kita maka akan sangat beresiko bagi kita, karena data yang kita miliki akan disadap atau dicuri. Algoritma RSA ini merupakan algoritma kriptografi yang sangat sering dipakai oleh peneliti-peneliti lainnya, dan juga untuk mengecek apakah RSA ini masih aman digunakan untuk kunci keamanan pada file.[2]. Kelemahan pada jurnal ini adalah aplikasi yang dipakai pada masih sangat sederhana, tools yang digunakan juga masih sederhana, sehingga perlu dikembangkan lagi untuk memperindah atau untuk menjadi referensi bagi peneliti lainnya.
- b. Jurnal kedua diteliti pada tahun 2019. Jurnal ini berisi tentang sebuah penelitian yang bertujuan untuk mengukur tingkat kecepatan kriptografi hybrid, terdiri dari algoritma simetris blowfish dan algoritma asimetris RSA, dengan beberapa type data seperti dokumen, foto, audio, dan video. Hasil dari penelitian ini adalah algoritma hybrid memiliki performa yang tidak jauh berbeda dari algoritma blowfish dan membuat

proses enkripsi dan deskripsi data lebih aman dengan keunggulan dari algoritma RSA.

- c. Penelitian diteliti oleh awan aarsa k, andi yusika r, asfami ansharie
Tujuan dibuatnya penelitian jurnal ini adalah membuat sebuah aplikasi keamanan file dan merahasiakan file dan data menggunakan kunci yaitu dengan public key dan privat key. Public key untuk enkripsi dan privat key untuk deskripsi. Bahasa pemrograman yang dipakai adalah menggunakan visual basic.net, di penelitian ini menggunakan metode white box testing yaitu untuk menguji atau mengetes coding, dan black box testing untuk menguji aplikasi yang dibuat berjalan dengan secara fungsionalitas dan sesuai dengan aturan yang telah ditetapkan.
- d. Penelitian keempat, diteliti pada Oktober 2018 Jurnal ini bertujuan membuat sebuah sistem yang bisa mengamankan file terutama file audio dengan algoritma kriptografi OTP dan juga algoritma ElGamal. Algoritma OTP ini aman untuk mengamankan data kita, tapi kelemahan dari algoritma otp ini adalah rentan akan bocornya informasi kunci yang dibuat, sehingga digunakanlah algoritma elgamal untuk mencegah kebocoran kunci. Hasil dari penelitian ini adalah besar ukuran file audio mempengaruhi kecepatan proses enkripsi data tersebut.
- e. Penelitian kelima diteliti Pada tahun April 2018 tujuan dari jurnal adalah membuat suatu aplikasi keamanan data yang fungsinya dapat melakukan pengamanan data menggunakan algoritma RSA. Algoritma RSA dapat

diimplementasikan dalam bahasa pemrograman sehingga file WAV dapat diolah dan di amankan datanya. Walaupun hasil ukuran file WAV setelah di enkripsi menjadi lebih besar tergantung dari besar kunci yang digunakan informasi yang ada dapat disamarkan dengan baik. Algoritma RSA merupakan algoritma kriptografi yang algoritmanya menggunakan kunci public, algoritma ini masih aman digunakan untuk kemanan data, karena panjang kunci mempengaruhi keamanan data kita.[3]

- f. Penelitian keenam dengan Judul “Penerapan algoritma RSA pada system kriptografi file audio MP3” di tulis oleh Ngakan Nyoman Diarse, Kristoforus Jawa Bendi, pada tahun Desember 2016. Jurnal ini bertujuan membuat suatu aplikasi yang akan digunakan menjaga kerahasiaan suatu data. Yaitu dengan proses enkripsi dan deskripsi, proses ini bertujuan untuk mengamankan file kita agar tidak bisa dilihat oleh orang yang tidak berhak, sehingga file yang kita miliki tetap aman. Keamanan file ini bisa dilakukan dibeberapa perangkat multimedia, seperti audio, video, foto. Juga bisa untuk dokumen pribadi kita, jurnal, ataupun yang lainnya.
- g. Penelitian ketujuh diteliti pada tahun 2018, oleh Abdul Rahman. Tujuan dari penelitian di jurnal tersebut adalah mengamankan file yang ada di memory card terutama memory card pada handphone dengan menggunakan metode kriptografi asimetris Elgamal.
- h. Penelitian ke-8, diteliti pada tahun 2016, oleh Sekaesih dan Sri

wahyuni. Tujuan dari jurnal tersebut adalah membuat suatu perangkat lunak yang dapat mengamankan file citra, file citra disini meliputi, foto, audio, teks, dan video. Dalam jurnal ini metode yang digunakan adalah menggunakan algoritma kriptografi RSA (Rivest Shamir Adleman)

- i. Penelitian ke-9, diteliti pada tahun 2016, oleh Ngakan Nyoman Diarse, dan Kristoforus Jawa Bendi. Pada penelitian ini penulis menggunakan metode RSA, dan tujuan dibuatnya penelitian tersebut adalah untuk mengamankan file audio, yang apabila file audio tersebut diputar atau dijalankan tetapi suara yang dihasilkan tidak jelas atau tidak terdengar, maka dibuatlah aplikasi yang bisa mendeskripsikan file tersebut ke bentuk semula.
- j. Penelitian ke-10, diteliti oleh Indra Gunawan, Sumarno dan Satria tambunan. Pada penelitian ini penulis membuat aplikasi pengamanan file yang salah satunya adalah file video. Kenapa penulis menggunakan metode RSA ini ?, karena pada algoritma RSA menggunakan 2 kunci, yaitu kunci public dan kunci privat.

B. Teori Dasar.

Teori dasar merupakan pembahasan dasar yang ada dalam penelitian ini, sebelum kita melakukan penelitian, kita harus mengetahui beberapa teori terlebih dahulu, ada beberapa teori dalam penelitian ini, adapun teorinya adalah :

a. Kriptografi

Kriptografi merupakan persamaan dari kata "enkripsi" yaitu penyandian dari kalimat-kalimat yang dapat dibaca menjadi kalimat yang tidak masuk akal. Kriptografi ada 2, yaitu kriptografi

asimetris dan simetris. Kriptografi modern sangat didasari pada teori matematis dan aplikasi komputer.

Kriptografi itu susah, karena untuk mengenkripsikan file kita, kita harus mengetahui rumus-rumus terlebih dahulu. Oleh karena itu kriptografi sangat aman Teknik kriptografi ini sangat sulit diimplementasikan, karena menggunakan penyandian angka-angka sehingga orang lain tidak bisa mengkases.

b. RSA (Rivest Shamir Adleman)

RSA dibidang kriptografi merupakan algoritma kriptografi asimetris yang pengaplikasiannya menggunakan public key dan privat key. RSA masih digunakan secara luas oleh peneliti-peneliti lainnya, dan dipercaya dalam mengamankan dengan menggunakan kunci. Algoritma RSA ditemukan pada tahun 1977 oleh 3 orang : Ron Rivest, Adi Shamir, dan Len Adleman. Algoritma RSA menggunakan bilangan prima untuk mencari pembangkit kunci, dan dipilih secara acak

Algoritma RSA memiliki 3 sistem yaitu, pembangkit kunci, algoritma enkripsi, dan algoritma deskripsi.[4]

Algoritma RSA memiliki besaran, adapun besaran-besaran pada algoritma RSA adalah sebagai berikut :

- a. p dan q merupakan bilangan prima atau bilangan asli yang lebih besar dari 1 bersifat dirahasia
- b. Nilai $n = p * q$ bersifat tidak dirahasia (tidak menjadi rahasia)
- c. Nilai $(n) = (p - 1) * (q - 1)$ adalah bersifat dirahasia
- d. e (enkripsi) bersifat tidak dirahasia
- e. d (deskripsi) bersifat dirahasia
- f. m (kata asli) bersifat dirahasia
- g. c (chiper) bersifat tidak dirahasia

c. ElGamal

Algoritma ElGamal merupakan algoritma kriptografi asimetris yang artinya algoritma ini memiliki key private dan juga key public. Algoritma Elgamal merupakan algoritma kunci public yang tingkat keamanannya berdasarkan permasalahan logaritma diskrit. Algoritma Elgamal dipublikasikan pada tahun 1985 oleh ilmuwan Mesir yaitu Taher ElGamal. Algoritma RSA ini biasanya digunakan untuk project digital, atau pengolahan citra, baik foto, audio, dan video, namun kemudian setelah dimodifikasi algoritma Elgamal digunakan untuk enkripsi dan dekripsi [5]

3. Metode Penelitian

Pada penelitian ini untuk proses penyusunan laporan sampai pembuatan aplikasi dibutuhkan data-data yang menunjang proses penelitian terutama data yang berhubungan dengan teknik kriptografi dengan algoritma RSA dan ElGamal. Untuk mengumpulkan data yang berkaitan dengan penelitian ini, digunakan beberapa metode yaitu:

1). Metode Observasi

Pada pembuatan aplikasi kriptografi ini metode observasi diterapkan pada pembuatan laporan dan program, misalnya dengan meneliti file audio dengan format mp3 dan wav digunakan pada proses kriptografi dengan algoritma RSA dan ElGamal.

2). Metode studi kepustakaan (*Literature Study*)

Merupakan metode dengan menggunakan referensi-referensi yang ada hubungannya dengan masalah yang dijadikan objek penelitian.

3.1. Tahapan membuat pembangkit kunci RSA (Rivest Shamir Adleman)

Pada penelitian ini, kami akan menjelaskan studi kasus untuk membuat key pada algoritma RSA, memilih secara acak

bilangan prima untuk p dan q dan nantinya akan menghasilkan 2 kunci yaitu (e, n) dan (d, n) . Prosesnya adalah Proses 1, untuk membuat pembangkitan kunci yaitu memilih secara random 2 bilangan prima yang akan dijadikan untuk kunci. Bilangan yang dipilih adalah $p = 17$, $q = 19$

Proses 2, adalah mencari nilai n , dengan memasukkan rumus $n = p * q$, dan hasilnya :
 $n = 17 * 19 = 323$

Proses 3, adalah mencari nilai (n) , dengan rumus $n = (p - 1) * (q - 1)$. hasilnya adalah $n = (17 - 1) * (19 - 1)$
 $n = 16 * 18 = 288$

Proses 4, adalah menentukan nilai e , dan nilai e harus relatif prima terhadap n atau $\gcd(e, n) = 1$. Diantara nilai $1 - (n)$. Memilih nilai $e = 59$.
 Jadi $\gcd(59, 288) = 1$

Proses 5, adalah menghitung nilai d , dengan persamaan $d = e^{-1} \pmod{n}$. Proses perhitungan $1 - (n)$ nilai $d = 83$

Plaintext

Plaintext merupakan teks asli dari kalimat yang akan kita enkripsikan, sebelum mengenkripsikan suatu file kita harus mempunyai plaintextnya terlebih dahulu, plaintext yang kami gunakan adalah "7e 7e 82" dalam format wav.

3.2. Proses Enkripsi RSA

Enkripsi adalah mencari nilai ciphertext nya, dari teks asli yang sudah kita cari tadi. Dari proses pencarian kunci dan juga plaintext diatas, maka kunci yang digunakan adalah $n = 323$, $e = 59$. Dengan rumus $c = p^e \pmod{n}$.

$$C = p^e \bmod n$$

$$c1 = 126^{59} \bmod 323 = 65$$

$$c2 = 126^{59} \bmod 323 = 65$$

$$c3 = 130^{59} \bmod 323 = 80$$

Hasil yang diperoleh dari proses enkripsi tadi adalah 65 65 dan 80

3.3. Proses Deskripsi RSA

Setelah mencari ciphertext kemudian kita mendeskripsikannya lagi menjadi teks asli lagi, biasanya deskripsi ini untuk orang yang telah menerima pesan kita dalam bentuk ciphertext lalu si penerima mendeskripsikan pesan yang sudah diterima. Disini kita memakai kunci privat yang sudah kita cari, yaitu $d=83$, dan $n=323$. Dengan rumus $M = c^d \bmod n$, ciphertext yang digunakan adalah 65 65 80

$$M = c^d \bmod n$$

$$m1 = 65^{83} \bmod 323 = 126$$

$$m2 = 65^{83} \bmod 323 = 126$$

$$m3 = 80^{83} \bmod 323 = 130$$

Dari pencarian diatas maka hasil yang didapat adalah 7e 7e 82, sama seperti plaintext diawal tadi.

4. Hasil

Pembangunan antarmuka pada penelitian ini menggunakan Java Netbeans 8.1. Rancangan aplikasi enkripsi dan deskripsi file audio menggunakan metode RSA dan ElGamal ini, menggunakan flowchart sebagai salah satu cara mempermudah membangun aplikasi,

Gambar1. Diagram alir aplikasi

Gambar 1 menjelaskan bagaimana alur dari aplikasi tersebut berjalan. Pertama kita akan memasuki aplikasi dan akan menampilkan menu, selanjutnya kita akan memilih file mana yang akan di enkripsikan, lalu nanti akan ada button, enkripsi atau deskripsi. Jika kita pilih enkripsi, maka file yang awal tadi akan di enkripsi dan hasilnya akan keluar di kolom hasil. Jika kita pilih deskripsi maka file kita tadi akan dideskripsi dan hasilnya akan keluar di kolom hasil. dan proses pun selesai.

Gambar2. Antarmuka menggunakan Netbeans

Gambar 2 menjelaskan tampilan awal dari aplikasi RSA yang kami buat, ada Button Cari untuk mencari file yang akan kita enkripsikan. Lalu ada Button Enkripsi, dan ada Button Deskripsi.

Gambar3. Proses Pencarian File

Gambar 3 menjelaskan, ketika kita mengklik Button Cari, maka akan menuju ke dokumen atau file-file yang kita cari, seperti gambar di atas.

Gambar4. Hasil dari proses pencarian

Gambar 4 menjelaskan hasil dari file yang kita cari tadi, dan akan muncul di textpanel kita. Seperti digambar

Gambar5. Proses Enkripsi

Gambar 5 menjelaskan hasil dari audio yang kita enkripsikan tadi, maka muncul hasilnya seperti digambar.

Gambar6. Hasil Deskripsi

Gambar 6 menjelaskan hasil dari deskripsi, maka jika kita menekan button deskripsi maka hasil nya akan seperti di awal seperti digambar.

5. Kesimpulan

Berdasarkan penelitian yang kami lakukan, kesimpulan yang kami dapat adalah :

1. Teknik yang kami pakai dalam mengamankan file adalah menggunakan teknik algoritma RSA dan Elgamal, dimana plaintext akan diproses dengan RSA dan hasil dari ciphertext akan dideskripsikan menggunakan Elgamal.
2. Perancangan aplikasi yang kami gunakan adalah menggunakan Flowchart 2007, dan implementasinya menggunakan Java Netbeans 8.1

Daftar Pustaka

- [1] N. Indahwati, "Penerapan Algoritma Kriptografi Asimetris Elgamal dengan Modifikasi Pembangkit Kunci terhadap Enkripsi dan Deskripsi Gambar Warna," *Journal Of Informatics and Computer Science*, p. 97, 2019.
- [2] R. N. Fuad, "Aplikasi Keamanan File Audio WAV(Wavefrom) dengan Terapan Algoritma RSA," *Jumal Nasional Informatika dan Teknologi Jaringan*, p. 113, 2017.
- [3] H. Santoso, "Perancangan Aplikasi Keamanan File Audio menggunakan metode RSA," *Jumal Ilmu Komputer dan Informatika*, p. 47, 2018.
- [4] H. Santoso dan M.Fakhrizal, "Perancangan Aplikasi Keamanan File Audio Format WAV(WaveForm) Menggunakan Algoritma RSA," *Jurnal Ilmu Komputer dan Informatika*, p. 48, 2018.
- [5] D. Hamanongan, "Implementasi Kriptografi Hibird dengan Algoritma ElGamal dan Algoritma One-Time Pad dalam Pengamanan File Audio Berbasis Dekstop," *Repositori Institusi USU, Sumatra Utara*, 2018.
- [6] H. Santoso dan M. Fakhrizal, "PERANCANGAN APLIKASI KEAMANAN FILE AUDIO FORMAT WAV (WAVEFROM) MENGGUNAKAN ALGORITMA RSA," *Jumal Ilmu Komputer dan Informatika*, p. 48, 2018.