PENGAMANAN FILE SUARA MENGGUNAKAN KRIPTOGRAFI ALGORITMA RIJNDAEL DENGAN PROSES ENKRIPSI DAN DEKRIPSI

Kristin D R Sianipar[1], Septri Wanti Sihaan[2], Marina Siregar[3], Indra Gunawan[4]
Program Studi Teknik Informatika
STIKOM Tunas Bangsa Pematangsiantar
Jl. Jend. Sudirman Blok A, No. 1,2 dan 3, Kota Pematangsiantar, Sumatera Utara
kristinsianipar@gmail.com [1]
septriwanti26@gamil.com [2]
marinasiregar686@gmail.com [3]
indra@amiktunasbangsa.ac.id [4]

Abstrak

Abstrak— Pada era ini, perkembangan dan kemajuan dari teknologi informasi semakin meningkat dengan pesat. Sehingga membuat lebih mengerti dalam bidang teknologi. Dengan semakin majunya teknologi saat ini, kita dapat membuat sebuah program untuk mengamankan file seperti : file gambar, file dokumen, file suara, dan lain-lain. Kita dapat mengamankan file kita dengan menggunakan kriptografi algoritma rijndael. Dengan menggunakan algoritma ini kita dapat mengamankan file menggunakan proses enkripsi dan dekripsi.

Kata Kunci : pengamanan data, kriptografi, algoritma rijndael, enkripsi, dekripsi

1. Pendahuluan

Pada saat ini, semakin banyak cara yang dapat dilakukan untuk mengamankan file-file yang kita miliki. Dalam menjaga keamanan dan kerahasiaan data yang kita miliki, kita dapat mengantisipasi orang-orang yang ingin merusak atau bahkan mencuri data kita.

DOI: https://doi.org/10.29103/techsi.v11i3.1967

Algoritma yang dapat dipakai untuk mengamankan file, seperti file suara yaitu algoritma rijndael.

Hal yang cukup membahayakan dari masalah tersebut salah satunya adalah mengurangi sistem keamanan penyimpanan informasi dalam komputer yang terhubung dengan jaringan ke luar komputer sehingga gangguan-gangguan dari pihak luar dalam proses perpindahan informasi sedikit banyak tidak dapat dielakkan. Dengan tujuan meminimalkan efek gangguan tersebut telah mendorong perkembangan teknologi kriptografi dan steganografi. Kriptografi merupakan studi matematika yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data, keaslian entitas dan keaslian data.[1][2]

Kriptografi menggunakan berbagai macam cara dalam upaya mengamankan suatu data. Pengiriman data dan penyimpanan data melalui media elektronik memerlukan suatu proses yang dapat menjamin keamanan dan keutuhan dari data yang dikirimkan tersebut. Data tersebut harus tetap rahasia pada saat melalui proses pengiriman, dan harus utuh pada saat data tersebut sampai di tujuan. Untuk memenuhi kebutuhan tersebut, dilakukan teknik enkripsi dan dekripsi terhadap data yang akan dikirimkan. Enkripsi dilakukan pada saat pengiriman dengan cara merubah data asli menjadi data rahasia, sedangkan proses dekripsi dilakukan pada saat proses penyampaian pesan ketujuan dengan cara merubah data rahasia tadi kembali ke data asli. Tujuan dari dua proses ini adalah agar pada saat proses pengiriman, data asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Untuk memenuhi kebutuhan akan sistem keamanan yang lebih, maka *National Institute of Standard and Technology (NIST)* pada tahun 1997 mengumumkan bahwa sudah saatnya membuat standar algoritma penyandian baru yang diberi nama *Advanced Encryption Standard (AES)*. Algoritma *AES* ini dibuatdengan tujuan menggantikan algoritma *DES*. Setelah

DOI: https://doi.org/10.29103/techsi.v11i3.1967

melalui beberapa tahap seleksi, algoritma *Rijndael* ditetapkan sebagai algoritma kriptografi *AES* pada tahun 2000. [3]

Dengan adanya kriptografi ini *user* akan lebih mudah dalam mengamankan file mereka seperti file suara dari orang-orang yang tidak berkepentingan dan menjaga keaslian file tersebut.

2. Metode Penelitian

A. Definisi Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan(*Cryptography is theart and science of keeping message secure*) [4]. Teknik enkripsi yang dilakukan adalah dengan menyandikan data sebelumnya yang telah ditambahkan dengan kata sandi sehingga untuk mengakses data tersebut di butuhkan kata sandi untuk mendekripsi kembali data tersebut. Dalam kriptografi, terdapat beberapa istilah yangsering di gunakan yaitu :

- Enkripsi
  Mengubah sebuah informasi kebentuk lain yang tidak dapat di mengerti.
- Dekripsi
  Kebalikan dari enkripsi, dekripsi merupakan proses untuk mengembalikan sebuah informasi yang telah di enkripsi sehingga informasi tersebut dapat di pahami kembali maknanya.
- Kunci
  Sebuah karakter yang di gunakan untuk mengenkripsi dan dekripsi suatu informasi sehingga di butuhkan kunci untuk mengubah informasi yang dapat dipahami menjadi data yang tidak dapat di pahami, begitu juga sebaliknya [5].

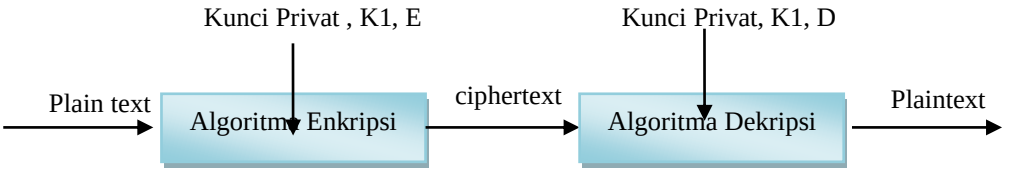
B. Jenis – Jenis Kriptografi

- **Kriptografi Kunci Simetri**

Kunci simetri berarti menggunakan kunci yang sama untuk proses enkripsi maupun dekripsi pada prosesnya pengirim pesan

DOI: https://doi.org/10.29103/techsi.v11i3.1967

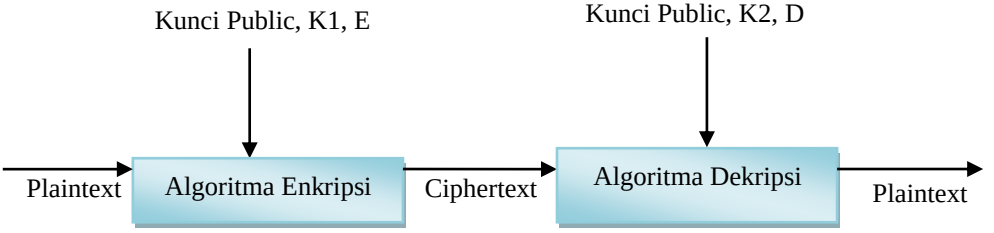
harus berbagi kunci rahasia tersebut. Keamanan sistem kriptografi kunci simetri terletak pada kerahasiaan kuncinya[6].



Gambar 1. Kriptografi Kunci Simetri

- **Kriptografi Kunci Asimetris**

Teknik kriptografi kunci asimetris berarti mengugunakan kunci *public* dan kunci *privat.* pada proses enkripsi, dekripsi dan pembuatan kunci teknik kriptografi asimetris memerlukan komputerasi yang lebih intensif dibandingkan kriptografi simetri, karena enkripsi asimetris menggunakan bilangan–bilangan yang sangat besar. Naskah yang telah dienkripsi menggunakan kunci privat hanya dapat didekripsi menggunakan kunci publik dan naskah yang dapat didekripsi menggunakan kunci publik dapat dipastikan telah dienkripsi menggunakan kunci privat. Sebaliknya, naskah yang telah dienkripsi menggunakan kunci publik hanya dapat didekripsi menggunakan kunci privat.[7]



Gambar 2. Kriptografi Kunci Asimetris

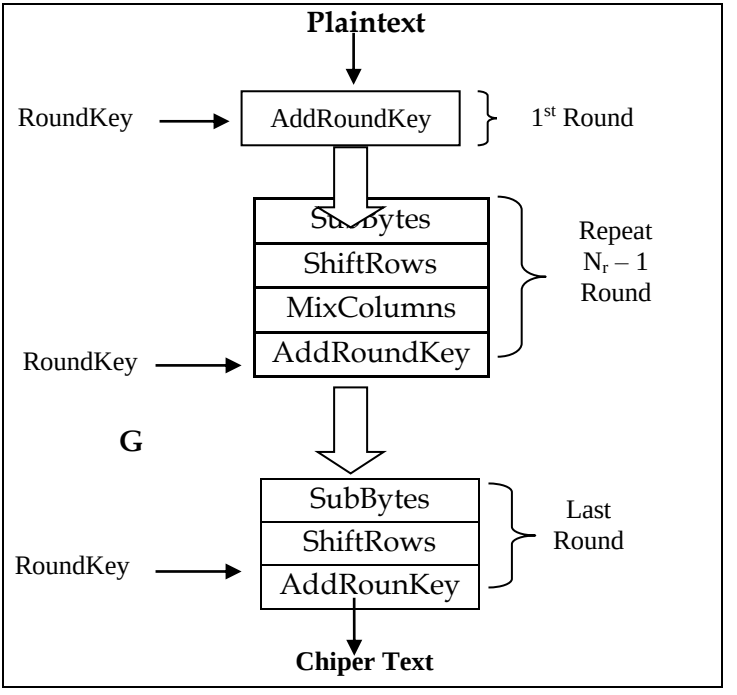
DOI: https://doi.org/10.29103/techsi.v11i3.1967

C. Definisi Algoritma Rinjdael

Algoritma *Rijndael* merupakan algoritma yang ditetapkan oleh NIST sebagai AES pada bulan Oktober 2000. Algoritma *Rijndael* ditemukan oleh Vincent Rijmen dan Joan Daemen dari Belgia. *Rijndael* termasuk dalam algoritma kriptografi yang sifatnya simetris dan *block chiper*. *Rijndael* mendukung panjang kunci 128 bit, 192 bit, dan 256 bit. Panjang kunci dan ukuran blok dapat dipilih secara independen.

Proses enkripsi pada algoritma *Rijndael* terdiri dari 4 jenis transformasi *byte*, yaitu *SubBytes()*, *ShiftRows()*, *MixColumns()*, dan *AddRoundKey()*. Pada awal proses enkripsi, masukan yang telah berbentuk *array state* akan mengalami transformasi *AddRoundKey()*. Setelah itu, *array state* akan mengalami transformasi *SubBytes()*, *ShiftRows()*, *Mixcolumns()*, dan *AddRoundKey()* secara berulang-ulang sebanyak N_r. Proses ini dalam algoritma *Rijndael* disebut sebagai *round function*. *Round* yang terakhir agak berbeda dengan *round-round* sebelumnya di mana pada *round* terakhir, *array state* tidak mengalami transformasi *Mixcolumns()*.

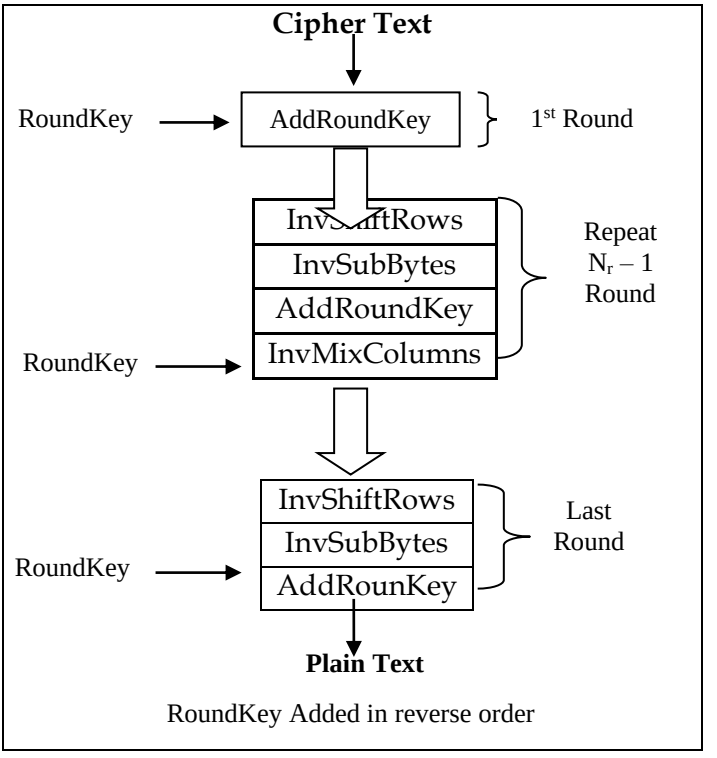
DOI: https://doi.org/10.29103/techsi.v11i3.1967



Gambar 3. Diagram Proses Enkripsi *Rijndael* [8]

Transformasi *cipher* dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan *inverse cipher* adalah *InvShiftRows()*, *InvSubBytes()*, *InvMixColumns()*, dan *AddRoundKey()* [9].

DOI: https://doi.org/10.29103/techsi.v11i3.1967



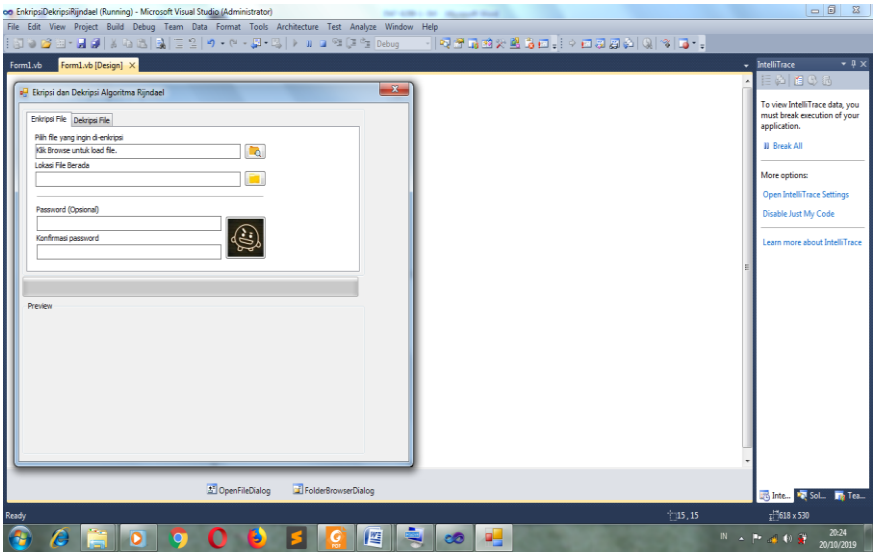
Gambar 4. Diagram Proses Dekripsi *Rijndael* [8]

3. Hasil dan Pembahasan

Pembangunan antarmuka pada tulisan ini menggunakan Microsoft Visual Basic 2010. Pada aplikasi ini dibangun sebuah form yang dimana terdapat proses enkripsi dan dekripsi file. Aplikasi ini memiliki satu form tetapi sudah terdapat enkripsi dan enkripsi. Hal tersebut dapat terjadi karena enkripsi dan dekripsi file dipisahkan dengan komponen yaitu TabControl. Pada aplikasi ini komponen-komponen yang digunakan yaitu GroupBox, TabControl, Label, TextBox, Button, ProgressBar, dan PictureBox. Untuk menguji keberhasilan aplikasi ini, maka dilakukan dengan cara menjalankan aplikasi ini.

a. Tampilan awal dari aplikasi. Pada tampilan awal ini, *user* dapat memilih proses yang diinginkan

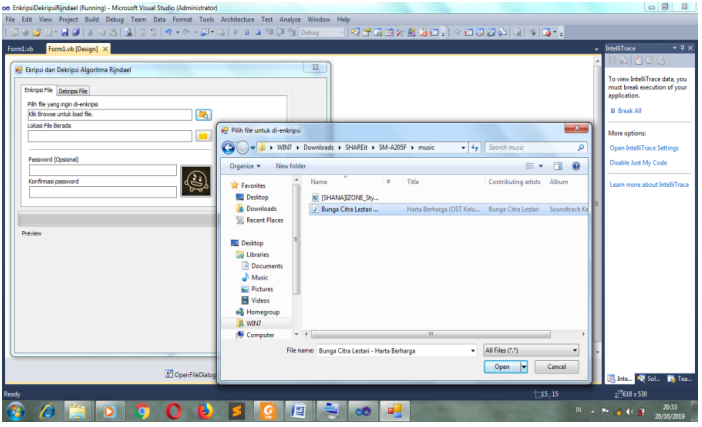
DOI: https://doi.org/10.29103/techsi.v11i3.1967



Gambar 5. Tampilan Awal Aplikasi Enkripsi dan Dekripsi Algoritma Rijndael

b. Proses Enkripsi

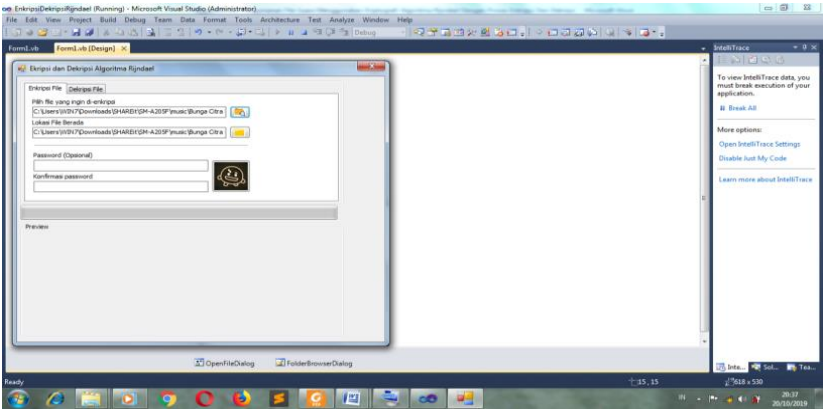
Jika kita ingin melakukan proses enkripsi pada file, maka kita dapat melakukan nya dengan meng-klik button *file search*. Dan akan muncul tampilan seperti ini pada saat kita akan memilih file yang ingin kita enkripsi.



Gambar 6. Tampilan pilih file yang ingin di enkripsi

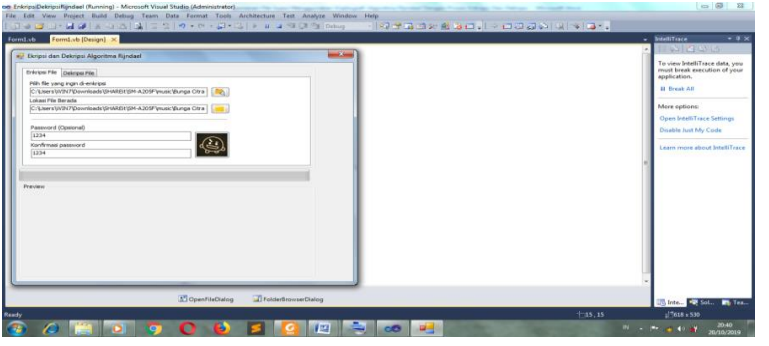
DOI: https://doi.org/10.29103/techsi.v11i3.1967

c. Tampilan Lokasi File Yang Telah Dipilih Untuk Dienkripsi.
Setelah kita klik open pada saat kita memilih file yang ingin di enkripsi, maka akan muncul tampilan seperti berikut ini yang menunjukan lokasi file yang telah dipilih.



Gambar 7. Tampilan Lokasi File Berada

d. Tampilan Isi Password
Setelah mengetahui letak file berada, maka langkah selanjutnya untuk mengisi password yang kita inginkan. Pada tahap ini, kita harus mengingat password yang kita buat, karena pada saat nanti kita akan dekripsi kan file yang telah kita enkripsi, itu akan berguna. Jika kita lupa password yang kita buat, maka file tidak akan bisa dikembalikan seperti file aslinya.

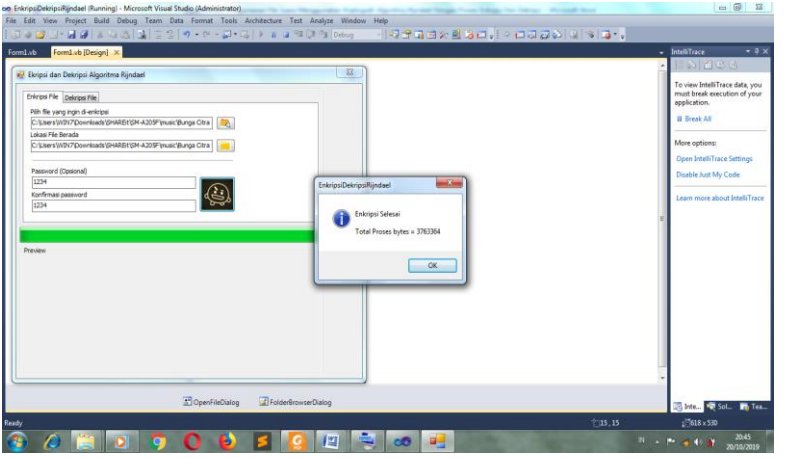


Gambar 8. Tampilan Isi Password

DOI: https://doi.org/10.29103/techsi.v11i3.1967

e. Tampilan Selesai Enkripsi

Sesudah mengisi password, lalu klik button yang disamping isi password, maka akan muncul tampilan seperti dibawah ini.



Gambar 9. Tampilan *Finish* Proses Enkripsi

Pada tahap ini adalah tampilan akhir dari proses enkripsi file yang dilakukan. Jika kita ingin melakukan proses pengembalian file yang telah dienkripsi, dapat dilakukan dengan cara yang sama dan hanya meng-klik pada tabcontrol di samping enkripsi. Kita harus mengingat password yang telah kita buat pada saat proses enkripsi karena pada saat proses dekripsi nantinya, password yang digunakan adalah password yang kita buat di awal.

4. Kesimpulan

Dengan adanya Kriptografi Algoritma Rijndael maka proses enkripsi dan dekripsi pada file suara akan semakin memudahkan *user* untuk menjaga keaslian file yang mereka miliki. Pada aplikasi yang telah dibuat ini kita juga harus mengingat password yang kita buat pada saat proses enkripsi.

DOI: https://doi.org/10.29103/techsi.v11i3.1967

Daftar Pustaka

[1]Biham, E (2004). Journal of Cryptography v 7.

[2]Davies, DW dan Murphy, S (2005). Pairs and Triplets of DES S-Boxes, Journal of Cryptology version 8.

[3]Hansfeld, Nils. The Cryptography Tutorial. http://www. antilles. k12.vi.us/math/ Akses: November 2009.

[4]Schneier, Bruce. (1996). *Applied Cryptography*, *Second Edition : Protocols*, *Algorthms, and Source Code in C*. John Wiley & Sons, Inc.

[5]Alim, Z., & Cancer, Y. (2016). Meningkatkan keamanan data **cloud computing** menggunakan algoritma rijndael. *Jurnal TI , Vol. V No 1*, 2.

[6]Ratih, 2010. Tugas Akhir : Studi dan Perbandingan Penggunaan Kriptografi Kunci Simetri dan Asimetri pada Telepon Selular, *Institute Teknologi Bandung*.

[7]Kromodimoeljo, S., 2009. *Teori & Aplikasi Kriptografi*, Jakarta: SPK IT Consulting.

[8]Stallings, William. (2005). *Cryptography and Network Security Principles and Practices*, *Fourth Edition*. Prentice Hall.

[9]Federal Information Processing Standards Publication 197, (2001). *Announcing the Advanced Encryption Standard (AES)*.

DOI: https://doi.org/10.29103/techsi.v11i3.1967