

BAB I

PENDAHULUAN

1.1. Latar Belakang

Pada saat ini sebuah data atau informasi sudah dianggap sebagai sesuatu yang bersifat berharga dimana tingkat keamanan dan tingkat efisien ruang penyimpanan sangat diperlukan. Dalam ruang lingkup pengamanan data terutama dalam bentuk dokumen dibutuhkan sebuah solusi guna melindungi data pribadi ataupun data suatu organisasi, agar tingkat kerahasiaan data dan privasi setiap individu maupun organisasi dapat terjaga dengan lebih baik, sehingga tidak dapat dilihat ataupun diubah oleh pihak yang tidak bertanggung jawab. Sebagaimana dalam undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik pasal 32 ayat 1, Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik (Indonesia, Undang-Undang, 2008).

Tidak hanya di Indonesia tetapi kasus pencurian terhadap suatu dokumen juga terjadi di belahan dunia lain seperti yang menimpa pabrikan mobil tesla pada tahun 2019. Pada kasus pencurian dokumen milik tesla disinyalir dokumen tersebut berisi tentang kode autonomous. Dari dokumen tersebut sistem yang dikembangkan tesla dalam bidang kendaraan otomatis dapat saja disebarluaskan dan beberapa pihak tentu saja mendapatkan keuntungan.

Oleh karena itu diperlukannya sebuah konsep CIA (*Confidentiality, Integrity dan Availability*) Triad yaitu agar sebuah data dapat terjaga kerahasiannya, integritas dan ketersediannya. Atas dasar tersebut maka data dokumen yang berisi informasi pribadi atau tentang suatu perusahaan tidak dapat diubah oleh pihak lain yang tidak bertanggung jawab. dibutuhkan sebuah langkah pengamanan pada data tersebut.

Salah satu bentuk pengamanan pada file dokumen tersebut dengan teknik kriptografi, dalam penelitian kali ini metode kriptografi yang digunakan

adalah AES (*Advanced Encryption Standard*) dengan kunci yang digunakan sebanyak 256 bit. Dimana metode ini digunakan sebagai metode enkripsi dan dekripsi data dokumen tersebut.

Selain tingkat keamanan yang tinggi pada saat ini kapasitas dari data tersebut cukup diperhitungkan mengingat jumlah data terutama data dokumen pada suatu organisasi ataupun perorangan dapat berjumlah cukup banyak maka dibutuhkan solusi guna meringkas kapasitas data dokumen tersebut menjadi lebih efisien. Salah satu cara untuk meringkas suatu data terutama data dokumen adalah dengan menggunakan metode kompres, dalam penelitian kali ini juga digunakan metode kompres dan dekompres menggunakan metode RLE (*Run Length Encoding*) metode ini dinilai lebih efisien untuk file dokumen dikarenakan metode ini bekerja dengan cara meringkas beberapa karakter berulang menjadi karakter tunggal saja.

Penelitian ini akan menggunakan dua teknik yaitu teknik kriptografi dan teknik kompresi, dimana metode kriptografi untuk enkripsi data dokumen menggunakan metode AES. Kemudian setelah proses enkripsi dikombinasikan dengan metode kompresi yaitu RLE untuk menjaga keamanan dan meringkas data dokumen. Untuk mengembalikan file menjadi file asli juga terdapat proses dekompres dan juga dekripsi pada dokumen tersebut. Kombinasi dari dua metode ini diharapkan mampu memenuhi aspek keamanan dan kerahasiaan serta meringkas data menjadi lebih efisien dalam penyimpanan yang dibutuhkan oleh setiap individu dan juga organisasi.

1.2. Rumusan Masalah

Dari latar belakang yang telah dijelaskan, permasalahan yang akan dibahas sebagai berikut :

1. Apakah kombinasi algoritma enkripsi AES dan algoritma kompresi RLE cocok digunakan untuk file dokumen?
2. Bagaimana kualitas file sesudah dan sebelum melalui proses enkripsi, dekripsi dan kompresi, dekompres dengan sebelum melalui proses tersebut?

1.3. Batasan Masalah

Permasalahan yang dibahas, terdapat batasan pada beberapa pembahasan adalah sebagai berikut :

- a. File dokumen yang digunakan berupa file yang berisi data pribadi dengan format Word (*.docx), Excel (*.xlsx) dan Pdf (*.pdf).
- b. Algoritma AES 256 Bit diterapkan pada proses enkripsi dan dekripsi file dokumen.
- c. Algoritma RLE diterapkan pada proses kompresi dan dekompres file dokumen.

1.4. Tujuan dan Manfaat

Tujuan penelitian ini adalah untuk pengembangan sistem pengamanan yang lebih untuk file dokumen guna kepentingan integritas data bagi individu ataupun suatu organisasi, dengan menggunakan kombinasi algoritma AES sebagai enkripsi-dekripsi dan algoritma RLE sebagai kompresi-dekompresi.

1.5. Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut :

- a. Untuk individu & organisasi
Merupakan sebuah solusi untuk pengaman file dokumen yang lebih efisien dengan menggunakan kombinasi algoritma AES dan algoritma RLE sehingga memenuhi kebutuhan dalam konteks kerahasiaan dan keamanan file dokumen.
- b. Untuk Penulis
Meningkatkan kemampuan dan pengetahuan dengan implementasi dalam bidang kriptografi dan kompresi mengenai algoritma AES dan algoritma RLE.

1.6. Ruang Lingkup

Ruang lingkup penelitian yang dilakukan adalah mengenai kombinasi algoritma AES dalam poses enkripsi-dekripsi dan algoritma RLE dalam proses kompresi-dekompresi dalam proses pengamanan yang lebih efisien untuk file dokumen yang memiliki tipe file docx, xlsx, dan pdf.

1.7. Luaran yang Diharapkan

Luaran yang diharapkan dari penelitian ini adalah mengetahui tingkat keberhasilan pengamanan ntuk file dokumen dengan proses enkripsi-dekripsi menggunakan algoritma AES dan dokombinasikan dengan metode kompresi-dekompresi menggunakan algoritma RLE.

1.8. Sitematika Penulisan

Sistematika penulisan yang digunakan pada penelitian ini diatur dalam susunan yang terbagi menjadi lima bab dan daftar pustaka yang terbagi dalam beberapa sub bab di dalamnya, dengan sistematika penulisan sebagai berikut:

BAB 1 PENDAHULUAN

Berisi tentang Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Ruang Lingkup, Luaran yang Diharapkan, dan Sistematika Penulisan dari penelitian ini.

BAB 2 LANDASAN TEORI

Pada bab ini berisi tentang penyampaian teori mendasar yang digunakan dalam penelitian ini sebagai dasar analisa permasalahan yang diteliti.

BAB 3 METODOLOGI PENELITIAN

Bab ini menjelaskan beberapa metode yang digunakan oleh penulis dan proses serta tahapan dalam melakukan penelitian secara yang dilakukan secara menyeluruh.

BAB 4 HASIL DAN PEMBAHASAN

Dalam bab ini berisi hasil luaran dari sistem yang telah dibuat dan dibahas sesuai penelitian untuk menjawab permasalahan yang ada.

BAB 5 PENUTUP

Pada bab ini berisi kesimpulan dan saran dari hasil dan pembahasan yang di ulas pada bab 4 (empat) dalam proses penelitian ini sebagai suatu refrensi dan acuan untuk penlitian yang dilakukan kedepannya.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN