Exact Papers in Compilation
Vol. 2, No. 2, Mei 2020 Hal. 255- 258
e-ISSN: 2656-0550

IMPLEMENTASI ALGORITMA RIJNDAEL PADA ENKRIPSI DOKUMEN ELEKTRONIK UNTUK KEAMANAN INFORMASI

Agus Sifaunajah
Program Studi Sistem Informasi
Universitas KH. A. Wahab Hasbullah.
Email: agus.syifa85@gmail.com

ABSTRACT
Cryptography is one of the fields of science in information security. One of the cryptographic algorithms is the Rinjdael algorithm. Security is still not a priority in an information system. The problem that often arises in government data is data leakage. Rinjdael algorithm is implemented to encrypt and decrypt data. The system design uses the waterfall method so that each part can be done optimally. In the trial, the results of the data decryption level that have been done by the encryption process are 100%..

***Keywords**: Rinjdael Algorithm, Cryptography, Data Security*

ABSTRAK
Kriptografi menjadi salah satu bidang ilmu dalam keamanan informasi. Salah satu algoritma kriptografi adalah algoritma rinjdael. Keamanan masih belum menjadi prioritas dalam sebuah sistem informasi. Permasalahan yang sering timbul dalam data pemerintahan adalah kebocoran data. Algoritma rinjdael diimplementasikan untuk melakukan enkripsi dan dekripsi data. Perancangan sistem menggunakan metode waterfall agar setiap bagian dapat dikerjakan secara maksimal. Dalam ujicoba didapatkan hasil tingkat dekripsi data yang sudah dilakukan proses enkripsi sebanyak 100 %..
***Kata Kunci**: Algoritma Rinjdael, Kriptografi, Keamanan Data*

PENDAHULUAN

Perkembangan teknologi komputer dan teknologi telekomunikasi pada saat ini telah mengubah cara masyarakat dalam berkomunikasi sehingga kasus penyadapan terhadap pejabat pemerintah menjadi hal yang cukup berbahaya. Penyadapan data merupakan hal yang paling ditakuti oleh pengguna jaringan komunikasi. (Wibowo, 2004)

Masalah keamanan merupakan salah satu aspek terpenting dari suatu sistem informasi. Masalah keamanan sering kali kurang mendapat perhatian dari para perancang dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan setelah tampilan, atau bahkan di urutan terakhir dalam daftar hal- hal yang dianggap penting. Apabila mengganggu performansi dari sistem, seringkali masalah keamanan tidak begitu dipedulikan bahkan ditiadakan.

Dengan adanya kemungkinan penyadapan data, maka aspek keamanan dalam pertukaran informasi menjadi sangat penting karena suatu komunikasi data jarak jauh belum tentu memiliki jalur transmisi yang aman dari penyadapan. Terdapat data-data yang tidak terlalu penting, sehingga apabila publik mengetahui data tersebut, pemilik data tidak terlalu dirugikan. Tetapi apabila Pemilik data adalah pihak militer atau pemerintah, keamanan dalam pertukaran informasi menjadi sangat penting karena data yang mereka kirim kebanyakan adalah data-data rahasia yang tidak boleh diketahui oleh publik.

Cryptography adalah salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu informasi. *Cryptography* merupakan kajian ilmu dan seni untuk menjaga suatu pesan atau data informasi agar data tersebut aman.

Cryptography mendukung kebutuhan dari dua aspek keamanan informasi, yaitu *Confidentiality, Authentication, Integrity, Nonrepudation,* dan *Secrecy*. *Cryptography* sudah digunakan oleh bangsa Mesir sejak 4000 tahun yang lalu oleh raja-raja Mesir pada saat perang untuk mengirimkan pesan rahasia kepada panglima perangnya melalui kurir- kurinya (Ariyus, 2006). *AES* (*Advanced Encryption Standard*) digunakan sebagai standar algoritma *cryptography* yang terbaru. AES menggantikan DES (*Data Encryption Standard*) yang pada tahun 2002 sudah berakhir masa penggunaannya. DES juga dianggap tidak mampu lagi untuk menjawab tantangan perkembangan teknologi komunikasi yang sangat cepat. Dalam penelitian yang dilakukan oleh rinaldi Munir tahun 2004, algoritma *Rijndael* dalam di aplikasikan pada tipe data string, dan stream.(Daemen and Rijmen, 1998). AES / *Rijndael* sendiri adalah algoritma *cryptography* simetris dengan menggunakan algoritma *Rijndael*, yang dapat mengenkripsi dan mendekripsi *block* data sepanjang 128 *bit* dengan panjang kunci 128 *bit* , 192 *bit* , atau 256 *bit*. (Kurniawan, 2004).

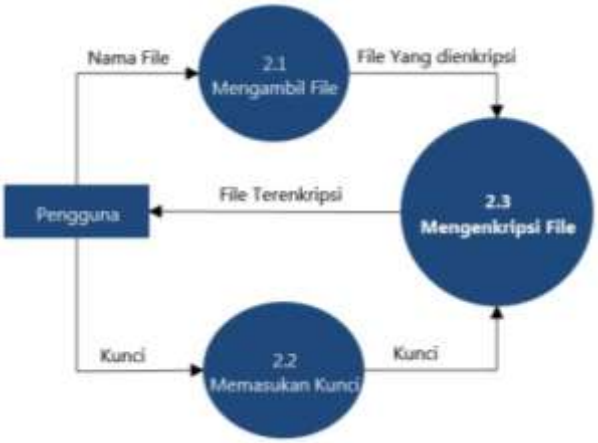
METODE

Metode pengembangan sistem yang digunakan pada penelitian ini menggunakan *waterfall.* Ruang lingkup sebatas pembuktian *enkripsi* data pada sebuah aplikasi. Adapun arsitektur dan proses yang terjadi pada sistem enkripsi data yang akan dibangun ini.

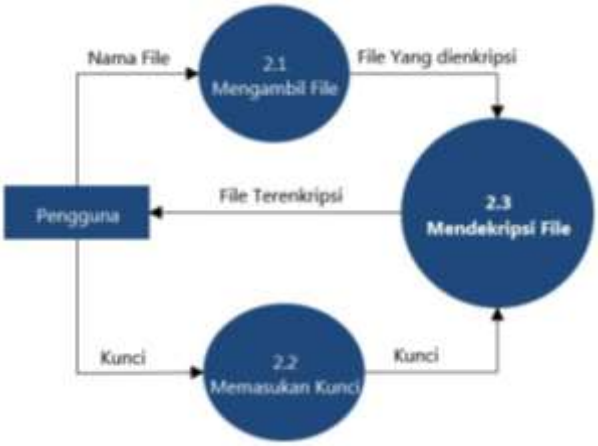
File yang akan diinputkan dalam sistem ini adalah *.excel *.text *.docx *. sistem dapat mengenkrip *file* yang inputkan tersebut. Proses pembentukan enkripsi *file*, secara garis besar akan dijelaskan sebagai berikut:

Langkah-langkah proses enkripsi *file* dengan *string password* sebagai berikut :

1. Masukkan *file* yang akan di enkripsi atau dekripsi. Dalam sistem ini *.excel *.text *.docx *file dapat diinputkan.
2. Pilih metode *hash* untuk mengacak password. fungsi *hash* yang digunakan dalam sistem ini ada delapan yaitu : *HAVAL, MD4, MD5, RIPEMD-128, RIPEMD-160, SHA256, SHA512* dan *TIGER*. Dimana tiap metode mempunyai algoritma dan panjang data yang berbeda.
3. Masukkan *password*, dan konfirmasi *password*. *password* yang dimasukkan sesuai dengan keinginan *user*.
4. Tentukan direktori tempat menyimpan *file* hasil enkripsi atau dekripsi.
5. Tipe *file* hasil enkripsi atau dekripsi dapat disimpan sesuai keinginan *user*. Misalnya, disimpan dalam tipe *.encrypt*. *File* hasil tidak boleh sama dengan *file input*.

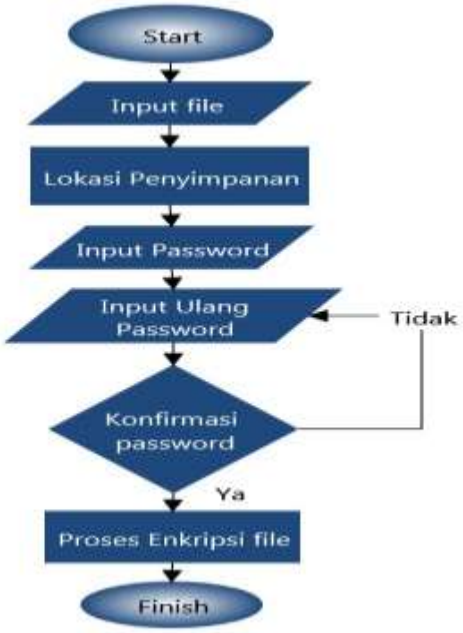


Gambar 1. *Data Flow Diagram* Proses *Enkripsi*



Gambar 2. Data Flow Diagram Dekripsi

Sedangkan mekanisme yang berjalan dalam sistem digambarkan dalam flowchart berikut ini :



Tabel 1. Data Hasil Pengamatan Proses Enkripsi Dan Dekripsi

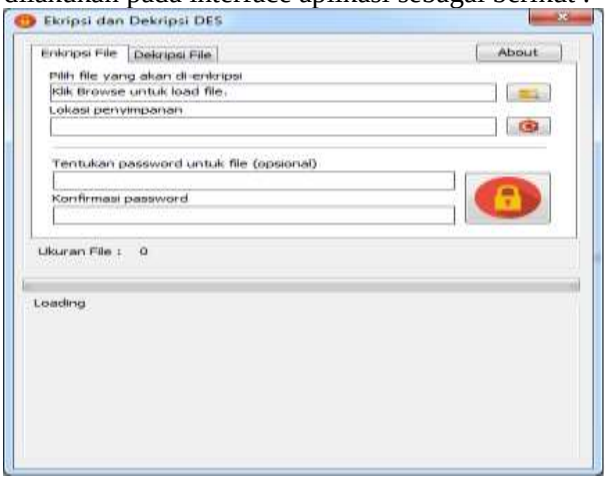
Nama file	**Size File Asli**	**Size file Hasil Enkripsi**	**Lama Proses**	**Size File Hasil Deskripsi Dekripsi**
SPK MI Al Falah.Doc	400,896 bytes	400,912 bytes	20 detik	400, bytes
Emis MI Al Falah,xls	28.343.296 bytes	28.343.312 bytes	7 detik	28.343.296 bytes
Testing.txt	147 bytes	160 bytes	5 detik	147 Bytes

Gambar 3. Flowchart Proses Enkripsi dan Dekripsi

HASIL DAN PEMBAHASAN

Hasil

Dalam proses enkripsi dan dekripsi data dapat dilakukan pada interface aplikasi sebagai berikut :



Gambar 4. Form Enkripsi Dan Dekripsi

Proses enkripsi dan dekripsi file didesain semudah mungkin. Proses enkripsi dapat dijelaskan sebagai proses menyembunyikan data agar tidak dapat dipahami oleh setiap orang. Sedangkan dekripsi adalah proses mengembalikan data yang disembunyikan dari proses enkripsi.

Adapun proses enkripsi yang berjalan sebagai berikut, user melakukan input file yang akan dienkripsi,kemudian user memilih direktori penyimpanan file yang akan dienkripsi dilanjutkan user memasukan kunci enkripsi.
Sedangkan proses dekripsi dapat dipahami sebagai berikut, user melakukan input file yang sudah didekripsi, kemudian user memilih direktori penyimpanan file yang akan didekripsi dilanjutkan user memasukan kunci enkripsi dan sistem akan mencocokan password untuk didekripsi.

Berikut ini contoh tampilan file sebelum dilakukan proses enkripsi :

Gambar 5. Contoh File sebelum proses enkripsi

Setelah dilakukan proses enkripsi akan menghasilkan informasi yang berbeda sebagai berikut :

Gambar 6. Contoh File setelah proses enkripsi

Setelah dilakukan beberapa kali uji coba dalam proses enkripsi dan dekripsi didapatkan data sebagai berikut ini :

SIMPULAN DAN SARAN

Adapun simpulan yang didapat selama penelitian ini dapat diajabrkan sebagai berikut ini :

1. *File* Yang dihasilkan oleh proses enkripsi rata-rata hampir sama dengan *file* asli (99%), dan *file* yang dihasilkan proses dekripsi pasti sama (100%) dengan *file* asli sebelum proses enkripsi.
2. Lama proses yang *dibutuhkan* oleh sistem sangat tergantung dari spesifikasi *hardware* yang digunakan, dan kinerja sistem *processor*.
3. Tipe *File* yang dihasilkan oleh proses enkripsi dapat menjadi tipe apa pun saja.
4. Proses dekripsi nama *file* yang dihasilkan dapat ditulis sesuai keinginan *user*,
5. Agar dapat dibaca saat proses dekripsi tipe *file* harus sama dengan *file* asli sebelum proses enkripsi.

Adapun saran yang dapat kami berikan dalam penelitian ini diantaranya adalah :

1. *File* hasil enkripsi dapat di *hide lock* dari sistem operasi, agar keamanannya lebih kuat.
2. *Proses* yang dilakukan dapat dikembangkan terhadap direktori / *folder*, dan *drive*.

DAFTAR RUJUKAN

Ariyus, Doni. 2006. *Kriptografi Keamanan Data dan Konunikasi.* Yogyakarta : Graha Ilmu.

Daemen and Rijmen. 1998. AES submission document on Rijndael.

Federal Information Processing Standards (FIPS) Publication 197. 2001.

Announcing the Advanced Encryption Standards (AES) RIJNDAEL.

Joan Daemen, Vincent Rijmen. 1999, AES Proposal : Rijndael, Document Version 2. NIST.

Kurniawan Yusuf, Ir.MT. 2004. Kriptografi Keamanan Internet dan Jaringan.
Bandung: Informatika.

Munir, Rinaldi. 2006. Kumpulan Bahan Kuliah Keamanan Sistem Informasi (IF5054). Bandung : DEPARTEMEN TEKNIK ELEKTRO ITB.

Wibowo , Wihartantyo Ari. 2004. ADVANCED ENCRYPTION STANDARD, ALGORITMA *RIJNDAEL.* Bandung : DEPARTEMEN TEKNIK ELEKTRO ITB