**KRIPTOGRAFI**

**ABSTRAK**

Perkembangan teknologi terutama pada sistem pengamanan data dalam menjaga keamanan data informasi telah berkembang pesat. Dalam menjaga keamanan data informasi terdapat cabang ilmu dalam pengembangannya seperti kriptografi dan steganografi. Pada penerapannya dilakukan tidak hanya pada satu teknik keamanan saja, melainkan bisa dilakukan dengan kombinasi dalam keamanan data informasi. Penelitian ini bertujuan untuk membuat sebuah sistem keamanan data dengan mengimplementasikan kriptografi pada pesan teks, isi *file* dokumen, dan *file* dokumen dengan melakukan perhitungan algoritma *Advanced Encryption Standard* (AES). AES merupakan algoritma *cryptographic* yang dapat digunakan untuk mengamakan data dimana algoritmanya adalah blok chipertext simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Hasil dari penelitian yaitu pengguna dapat mengenkripsi pesan teks kemudian disimpan menjadi sebuah *file* dokumen dan isi *file* dokumen tersebut dienkripsi lagi selanjutnya hasil enkripsi isi *file* dokumen tersebut, *file* dokumennya dienkripsikan dan selanjutnya dikompresi dan disembunyikan pada sebuah *file* citra (gambar) agar keamanan data informasi tersebut dapat terjaga keamanannya karena telah dilakukan pengamanan dan penyandian yang berlapislapis.

**Kata kunci** : Kriptografi, *Advanced Encryption Standard* (AES), Pesan Teks, Isi *File* Dokumen, Steganografi

**PENDAHULUAN**

Teknologi komputer sangat dibutuhkan oleh kehidupan manusia terutama personal maupun kelompok (organisasi). Kelompok (organisasi) tersebut sangat membutuhkan adanya komputerisasi dalam setiap kegiatannya. Dari hal penggunaan komputerisasi tersebut, maka dibuatlah sebuah keamanan bagi seluruh aset-asetnya, terutama informasi-informasi dan data-data penting demi menjaga kerahasiaan informasi data tersebut. Dari keamanan data tersebut menimbulkan tuntutan akan tersedianya suatu sistem pengamanan data yang lebih baik agar dapat mengamankan data dari berbagai ancaman yang mungkin timbul. Ini merupakan latar belakang berkembangnya sistem keamanan data yang berfungsi untuk melindungi data yang ditransmisikan atau dikirimkan melalui suatu jaringan komunikasi.

Ada beberapa cara melakukan pengamanan data ataupun pesan, diantaranya adalah dengan menggunakan teknik penyamaran data yang disebut dengan kriptografi dan teknik penyembunyian data yang disebut dengan steganografi.

Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan. Dalam kriptografi, data atau pesan yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa. Sehingga seandainya data tersebut bisa diperoleh dan dibaca oleh orang lain, maka pihak yang tidak berhak atau berwenang tersebut tidak akan bisa mengerti arti dari data tersebut.

Dalam bidang kriptografi terdapat dua konsep yang sangat penting atau utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Sebuah pesan atau data yang masih asli dan belum mengalami penyandian dikenal dengan istilah plaintext. Kemudian setelah disamarkan dengan suatu cara penyandian, maka plaintext ini disebut sebagai *chipertext*. Proses penyamaran dari *plaintext* ke *ciphertext* disebut enkripsi (*encryption*), dan proses pengembalian dari ciphertext menjadi plaintext kembali disebut dekripsi (*decryption*).

Dalam hal ini file yang dapat di enkripsi adalah file dokumen berupa teks, file citra berupa gambar, serta file audio dan file video dalam format digital. Pada pesan teks, isi file dokumen, atau file dokumen dalam menjaga kerahasiaan informasi datanya memerlukan teknik-teknik enkripsi dan dekripsi yang tidak mudah atau sukar untuk dipecahkan. Proses pengamanan pada pesan teks, isi file dokumen, atau file dokumen dapat dilakukan dengan mengenkripsi pesan teks, isi file dokumen, atau file dokumen tersebut dengan menggunakan metode algoritma tertentu yang dapat membuat data informasi tersebut tidak bisa dibaca atau tidak dapat dimengerti oleh pihak lain. Salah satunya dengan menggunakan metode algoritma AdvancedEncryption Standard (AES). Algoritma AdvancedEncryption Standard (AES) dipilih penulis dalam menjaga keamanan pada sebuah data atau informasi tersebut, dikarenakan AES merupakan cipher yang berorientasi pada bit, sehingga memungkinkan untuk implementasi algoritma yang efisien ke dalam software dan hardware. AES memiliki ketahanan terhadap semua jenis serangan yang diketahui. Disamping itu kesederhanaan rancangan, kekompakan kode yang sederhana dan kecepatan pada berbagai platform dimiliki oleh algoritma AES. AES terbukti kebal menghadapi serangan konvensional (linear dan diferensial attack) yang menggunakan statistik untuk memecahkan sandi, dan dalam setiap proses enkripsi dan dekripsi harus melakukan 10 perputaran atau 10 iterasi (10 Round) dalam melakukan pengamanan maupun untuk membuka pengamanan tersebut.

Dalam hal ini juga ditambahkan sebuah sistem pendukung pada pengamanan data setelah melakukan teknik kriptografi dalam menjaga keamanan data informasi tersebut yaitu dengan teknik penyembunyian data atau disebut steganografi. Steganografi merupakan seni dan ilmu untuk menyembunyikan pesan dalam sebuah media pesan. Kerahasiaan pesan yang ingin disampaikan merupakan faktor utama dalam steganografi. Dengan metode steganografi, pesan yang ingin di sampaikan disembunyikan dalam suatu media umum sehingga diharapkan tidak akan menimbulkan kecurigaan dari pihak lain yang tidak di inginkan untuk mengetahui pesan rahasia tersebut. Salah satu implementasi steganography modern adalah pada media citra digital.

Dalam metode steganografi untuk menyembunyikan suatu pesan ke dalam file digital (file citra, file audio, dan file video). Sebagai contoh yaitu media citra digital sebagai pesan yang akan dikirim terlebih dahulu disisipkan atau disembunyikannya suatu pesan rahasia ke dalam filecitra tersebut. Pada file citra yang telah disisipkan suatu pesan tersebut tidak akan terlihat jelas atau diketahui oleh pihak lain bahwa file citra tersebut terdapat suatu pesan rahasia di dalamnya kecuali pengirim dan penerima yang mengetahui bahwa ada pesan rahasia.

Dalam hal ini penulis menggunakan sistem keamanan pendukung steganografi dengan Teknik simple yaitu menyembunyikan sebuah pesan atau file rahasia yang telah terenkripsi ke dalam file citra (gambar) menggunakan command / DOS. Hal ini bertujuan agar pesan atau file rahasia tersebut tidak dapat diketahui oleh pihak lain.

Berdasarkan uraian di atas, dilakukan penelitian yang lebih mendalam mengenai metode kriptografi Advanced Encryption Standard (AES) dan steganografi dengan mengambil konsep judul yaitu “Implementasi Kriptografi Pengamanan Data pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma *Advanced Encryption Standard*”.

**PEMBAHASAN**

**Kriptografi**

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi. Pesan yang akan dienkripsi disebut sebagai plaintext(teks biasa). Disebut demikian karena informasi ini dengan mudah dapat dibaca dan dipahami oleh siapa saja. Algoritma yang dipakai untuk mengenkripsi  
dan mendekripsi sebuah plaintext melibatkan penggunaan suatu bentuk kunci. Pesan plaintextyang telah dienkripsi (atau dikodekan) dikenal sebagai ciphertext (teks sandi).

Di dalam kriptografi kita akan sering menemukan berbagai istilah atau terminology.

Beberapa istilah yang harus diketahui yaitu :

1. Pesan, Plainteks, dan Cipherteks

Pesan (message) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah (plaintext) atau teks jelas (cleartext).

1. Pengirim dan Penerima

Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (sender) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (receiver) adalah entitas yang menerima pesan.

1. Enkripsi dan dekripsi

Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (encryption) atau enciphering (standard nama menurut ISO 7498-2). Sedangkan proses mengembalikan cipherteks menjadi plainteks semula disebut dekripsi (decryption) atau deciphering (standard nama menurut ISO 7498-2).

1. Cipher dan kunci

Algoritma kriptogarfi disebut juga cipher, yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa cipher memerlukan algoritma yang berbeda untuk enkripsi dan dekripsi. Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen-elemen plainteks dan himpunan yang berisi cipherteks. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara dua himpunan tersebut. Misalkan P menyatakan plainteks dan C menyatakan cipherteks, maka :

E(P) = C 🡪 fungsi enkripsi E memetakan

P ke C

D(C) = P 🡪 fungsi dekripsi D memetakan

C ke P

Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan asal, maka persamaan D(E(P)) = P harus benar.  
Kriptografi mengatasi masalah keamanan data dengan menggunakan kunci, yang dalam hal ini algoritma tidak dirahasiakan lagi, tetapi kunci harus tetap dijaga kerahasiaannya. Kunci (key) adalah parameter yang digunakan untuk transformasi enkripsi dan dekripsi. Kunci biasanya berupa string atau deretan bilangan.

**Sejarah Kriptografi**

Sejarah kriptografi sebagian besar merupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (transposition cipher) dan algoritma substitusi (substitution cipher). Cipher transposisi mengubah susunan huruf-huruf di dalam pesan, sedangkan cipher substitusi mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain.

**Tujuan Kriptografi**

Dari paparan awal dapat dirangkumkan bahwa kriptografi bertujuan untuk member layanan keamanan. Yang dinamakan aspek-aspek keamanan:

1. Kerahasiaan (confidentiality)

Adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.

1. Integritas data (data integrity)

Adalah layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman.

1. Otentikasi (authentication)

Adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihakpihak yang berkomunikasi (user autehentication).

1. Non-repudiation

Adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan.

**Jenis Kriptografi**

Kriptografi sebagai metode enkripsi data terdiri dari tiga jenis. Penggunaannya nanti akan disesuaikan menurut kebutuhan. Berikut penjelasannya:

1. Symmetric key

Jenis kriptografi yang pertama yakni symmetric key. Pada jenis kriptografi symmetric key, pengirim dan penerima informasi hanya menggunakan satu kunci untuk melakukan enkripsi dan dekripsi informasi. AES (Advanced Encryption System) merupakan standar algoritma yang digunakan pada metode ini.

1. Public / Asymmetric key

Asymmetric atau public key cryptography adalah jenis kriptografi yang memanfaatkan dua kunci yang saling berkaitan sebagai public dan private key. Kedua kunci ini dipasangkan sehingga kode enkripsi dan data di dalamnya masih terjaga kerahasiaannya. Metode yang digunakan pada jenis kriptografi ini adalah RSA.

1. Hash function

Jenis kriptografi hash function menggunakan persamaan matematika, sehingga metode ini tidak memerlukan kunci apapun karena telah disesuaikan untuk pengiriman data satu arah. Jenis ini menggunakan sistem merangkum informasi dan mengirimkan penjelasan hasil rangkuman tersebut.

**KESIMPULAN**

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi. Pesan yang akan dienkripsi disebut sebagai plaintext(teks biasa).

**DAFTAR PUSTAKA**

[Mengenal Kriptografi, Pengertian, Jenis dan Algoritmanya (dewaweb.com)](https://www.dewaweb.com/blog/apa-itu-kriptografi/#Apa_Fungsi_Kriptografi)

(Nandar Pabokory et al., 2015)