PENERAPAN ALGORITMA AES DENGAN KUNCI ELGAMAL PADA PENGAMANAN CITRA MEDIS

SKRIPSI

Disusun oleh:

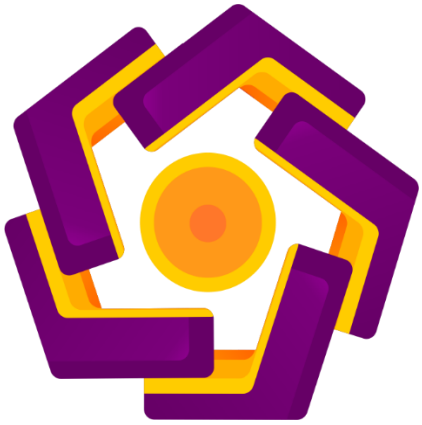
Muhammad Wildan Aizzaddin
17.83.0047

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

PENERAPAN ALGORITMA AES DENGAN KUNCI ELGAMAL PADA PENGAMANAN CITRA MEDIS

SKRIPSI

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer
Pada Jenjang Program Sarjana – Program Studi Teknik Komputer



Disusun oleh:

Muhammad Wildan Aizzaddin
17.83.0047

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

HALAMAN PERSETUJUAN

SKRIPSI

PENERAPAN ALGORITMA AES DENGAN KUNCI ELGAMAL PADA PENGAMANAN CITRA MEDIS

yang dipersiapkan dan disusun oleh

Muhammad Wildan Aizzaddin

17.83.0047

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 28 Agustus 2021

Dosen Pembimbing,

Dony Ariyus, M.Kom
NIK. 190302128

HALAMAN PENGESAHAN

SKRIPSI

PENERAPAN ALGORITMA AES DENGAN KUNCI ELGAMAL PADA PENGAMANAN CITRA MEDIS

yang dipersiapkan dan disusun oleh

Muhammad Wildan Aizzaddin

17.83.0047

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 September 2021

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Lilis Dwi Farida, S.Kom, M.Eng **NIK. 190302288**	_____
Rumini, M.Kom **NIK. 190302246**	_____
Dony Ariyus, M.Kom **NIK. 190302128**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 September 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Muhammad Wildan Aizzaddin
NIM : 17.83.0047

Menyatakan bahwa Skripsi dengan judul berikut:

Penerapan Algoritma AES dengan Kunci Elgamal pada Pengamanan Citra Medis

Dosen Pembimbing : Dony Ariyus, M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 21 September 2021

Yang Menyatakan,

Muhammad Wildan Aizzaddin

HALAMAN MOTTO

“Jangan menyerah sebelum kamu benar-benar berusaha”

HALAMAN PERSEMBAHAN

Skripsi ini saya persembahkan untuk :

Kedua orang tua saya, tanpa mereka saya bukan apa-apa

Ketiga adik saya yang selalu memberikan semangat dan dukungan

Dosen-dosen saya yang tidak pernah lelah membimbing

Seluruh teman-teman saya yang menjadi rekan saya dalam belajar

Semoga Allah balas kebaikan kalian dengan kebaikan yang berlipat ganda.

KATA PENGANTAR

Segala puji bagi Allah *Subhanahuwata'ala* atas limpahan nikmat, rahmat, hidayah dan karuniaNya, sehingga penulis dapat menyelesaikan skripsi dengan judul "Penerapan Algoritma AES dengan Kunci ElGamal pada Pengamanan Citra Medis". Penulis menyadari tanpa bantuan dan bimbingan dari berbagai pihak, skripsi ini tidak mungkin terselesaikan. Oleh karena itu penulis menyampaikan terima kasih kepada :

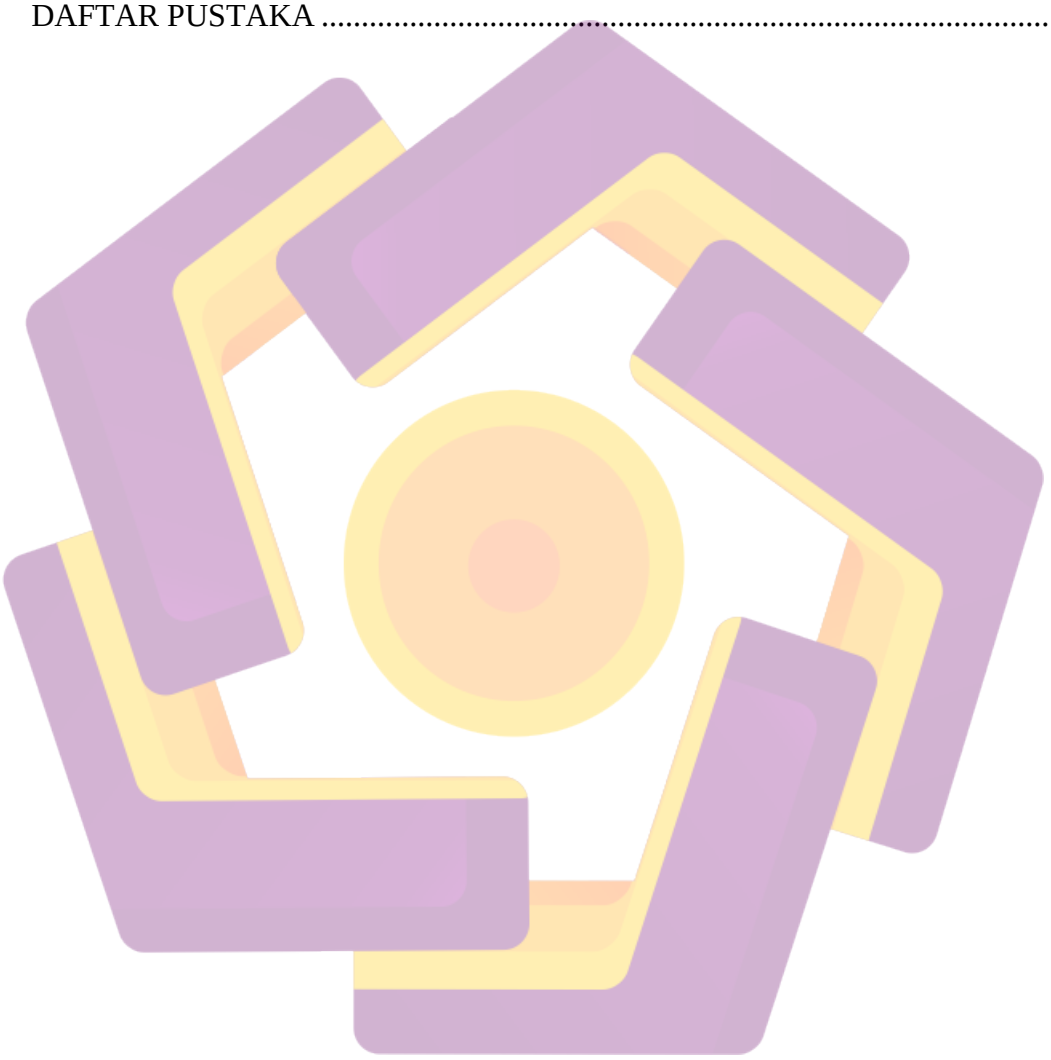
1. Allah *Subhanahuwata'ala,* tanpa karunia dan pertolonganNya, penulis tidak mungkin bisa menyelesaikan skripsi ini.
2. Prof. Dr. M. Suyanto, M.M., selaku Rektor Universitas AMIKOM Yogyakarta.
3. Bapak Dony Ariyus, M.Kom., selaku Kaprodi S1 Teknik Komputer Universitas AMIKOM Yogyakarta dan Dosen Pembimbing yang bersedia memberikan arahan dan bimbingan dalam menyelesaikan skripsi ini.
4. Segenap Dosen, Staff, dan Karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu kepada penulis di bangku kuliah dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya Skripsi ini.
5. Kedua orang tua, adik-adik dan keluarga yang selalu mendoakan, memberikan semangat dan memberikan dukungan kepada penulis.
6. Teman-teman dan seluruh pihak yang telah mendukung penulis dalam menyusun skripsi ini yang tidak dapat penulis sebutkan satu persatu.

Penulis berharap, semoga skripsi ini bisa bermanfaat bagi berbagai pihak. Dalam penulisan skripsi ini penulis menyadari masih banyak kekurangan karena terbatasnya pengetahuan dan pengalaman penulis. Karena itu, dengan lapang hati penulis mengharapkan kritik dan saran yang membangun guna menyempurnakan skripsi ini.

Yogyakarta, 27 Agustus 2021

Penulis

DAFTAR ISI



DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Adanya teknologi internet pada saat ini, membuat kegiatan bertukar informasi menjadi lebih mudah. Jutaan pesan berupa citra dikirimkan melalui internet setiap harinya. Sebuah citra dapat mengandung informasi yang sensitif. Citra medis yang mengandung data pasien merupakan salah satunya. Jika data pasien jatuh kepada pihak yang tidak bertanggung jawab, tentu merupakan hal yang fatal. Sayangnya pada saat ini, pengiriman dan penyimpanan file citra medis masih belum cukup aman. Berdasarkan penelitian yang dikeluarkan oleh *CybelAngle*, jutaan file citra medis pada saat ini dapat diakses secara bebas pada ribuan server yang tidak terlindungi. Untuk mengatasi permasalahan tersebut, salah satu cara yang dapat dilakukan adalah dengan menggunakan teknik kriptografi.

Penelitian ini dilakukan dengan mengembangkan aplikasi pengamanan file citra medis berbasis desktop dengan mengkombinasikan algoritma *Advanced Encryption Standard* (AES) dengan algoritma ElGamal. Algoritma AES akan digunakan pada pengamanan file citra medis sedangkan algoritma ElGamal akan digunakan pada pengamanan kunci AES. Metode penelitian yang digunakan pada penelitian ini adalah metode eksperimen dimana dilakukan pengumpulan data dengan mencatat hasil dari setiap pengujian.

Berdasarkan pengujian yang dilakukan, pengamanan file citra medis berhasil dilakukan dengan menggunakan algoritma AES. Proses enkripsi menggunakan algoritma AES akan menghasilkan file citra baru yang tidak dapat dipahami artinya sebelum didekripsi. File citra medis yang dienkripsi dengan algoritma AES juga berhasil didekripsi tanpa merubah isi dari file citra medis. Selain itu, konsep algoritma asimetri pada algoritma ElGamal juga dapat mengamankan kunci AES pada proses pengiriman. Hasil pengujian juga menunjukkan bahwa lama waktu yang dibutuhkan pada proses enkripsi dan dekripsi menggunakan kombinasi algoritma AES dengan algoritma ElGamal berbanding lurus dengan ukuran dari file citra medis yang di proses. Semakin besar ukuran file, maka semakin lama pula waktu yang dibutuhkan.

Kata kunci: Kriptografi, Citra Medis, Enkripsi, Dekripsi, Algoritma AES, Algoritma ElGamal

ABSTRACT

The existence of internet technology currently, makes the activity of exchanging information easier. Millions of messages in the form of images are sent through the internet every day. An image can contain sensitive information. Medical images containing patient data are one of them. If patient data falls to irresponsible parties, it is certainly a fatal thing. Unfortunately, currently sending and storing medical image files is still not secure enough. According to research released by CybelAngle, millions of medical image files are currently freely accessible on thousands of unprotected servers. To overcome these problems, one way that can be done is to use cryptographic techniques.

This research was conducted by developing a desktop-based medical image file security application by combining the Advanced Encryption Standard (AES) algorithm with the ElGamal algorithm. The AES algorithm will be used for securing medical image files while the ElGamal algorithm will be used for securing AES keys. The research method used in this study is an experimental method where data collection is carried out by recording the results of each test.

Based on the tests carried out, the security of medical image files has been successfully carried out using the AES algorithm. The encryption process using the AES algorithm will produce a new image file that cannot be understood before being decrypted. Medical image files encrypted with the AES algorithm were also successfully decrypted without changing the contents of the medical image files. In addition, the concept of the asymmetric algorithm in the ElGamal algorithm can also secure the AES key in the sending process. The test results also show that the length of time required for the encryption and decryption process using a combination of the AES algorithm with the ElGamal algorithm is directly proportional to the size of the medical image file that is processed. The larger the file size, the longer it will take.

Keyword: *Cryptography, Medical Imagery, Encryption, Decryption, AES Algorithm, ElGamal Algorithm*