PERANCANGAN DAN PEMBUATAN APLIKASI DESKTOP KRIPTOGRAFI MENGGUNAKAN METODE AES DENGAN PROSES ENKRIPSI DAN DEKRIPSI BERBASIS JAVA

SKRIPSI

disusun oleh

Glen Hasller Sajori

12.11.6205

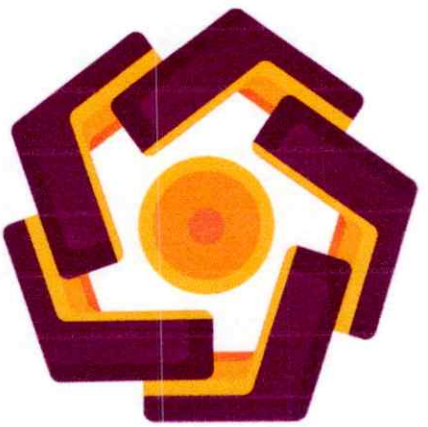
PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2019

PERANCANGAN DAN PEMBUATAN APLIKASI DESKTOP KRIPTOGRAFI MENGGUNAKAN METODE AES DENGAN PROSES ENKRIPSI DAN DEKRIPSI BERBASIS JAVA

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Glen Hasller Sajori

12.11.6205

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019

PERSETUJUAN

SKRIPSI

PERANCANGAN DAN PEMBUATAN APLIKASI DESKTOP KRIPTOGRAFI MENGGUNAKAN METODE AES DENGAN PROSES ENKRIPSI DAN DEKRIPSI BERBASIS JAVA

yang dipersiapkan dan disusun oleh

Glen Hasller Sajori

12.11.6205

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 12 Februari 2019

Dosen Pembimbing,

Ahlihi Masruro, M.Kom.
NIK. 190302148

PENGESAHAN

SKRIPSI

PERANCANGAN DAN PEMBUATAN APLIKASI DESKTOP KRIPTOGRAFI MENGGUNAKAN METODE AES DENGAN PROSES ENKRIPSI DAN DEKRIPSI BERBASIS JAVA

yang dipersiapkan dan disusun oleh

Glen Hasller Sajori

12.11.6205

telah dipertahankan di depan Dewan Penguji
pada tanggal 15 Maret 2019

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Ahlihi Masruro, M.Kom. **NIK. 190302148**	
Ali Mustopa, M.Kom. **NIK. 190302192**	
Dina Maulina, M.Kom. **NIK. 190302250**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Maret 2019

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si , M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 20 Maret 2019

Glen Hasller Sajori

NIM 12.11.6205

MOTTO

- ✓ Sukses bukanlah akhir, kegagalan tidaklah fatal, ini adalah keberanian penting untuk melanjutkannya. (*Winston Churchill*)
- ✓ Pendidikan merupakan senjata yang paling mematikan di dunia, karena dengan pendidikan mampu mengubah dunia. *(Nelson Mandela)*
- ✓ *Don't judge a book by its cover.*
- ✓ *Play hard, work harder, pray hardest.*

PERSEMBAHAN

Segala puji dan syukur atas kehadirat Tuhan Yang Maha Esa berkat hikmat dan karunia-Nya penulis dapat menyelesaikan skripsi ini sebagai salah satu persyaratan untuk mencapai gelar Sarjana Komputer. Skripsi ini penulis persembahkan kepada :

1. Kedua orangtua, serta seluruh keluarga besar yang senantiasa memberikan semangat, doa, serta motivasi tanpa henti.
2. Bapak Ahlihi Masruro, M.Kom selaku dosen pembimbing yang selalu mengarahkan dan memberikan masukan dalam proses penyusunan skripsi.
3. Keluarga besar 12-S1TI-07, terima kasih atas segala bentuk dukungan, dan terima kasih atas kebersamaan kalian hingga saat ini.

KATA PENGANTAR

Segala puji dan syukur bagi Tuhan Yang Maha Esa yang senantiasa telah melimpahkan hikmat, karunia dan petunjuk-Nya, sehingga penulis dapat menyelesaikan skripsi ini.

Skripsi ini disusun sebagai syarat untuk menyelesaikan studi di UNIVERSITAS AMIKOM Yogyakarta dengan skripsi yang berjudul "PERANCANGAN DAN PEMBUATAN APLIKASI DESKTOP KRIPTOGRAFI MENGGUNAKAN METODE AES DENGAN PROSES ENKRIPSI DAN DEKRIPSI BERBASIS JAVA". Aplikasi ini dibuat dengan maksud dan tujuan untuk mengamankan data atau file pengguna.

Skripsi ini dapat terselesaikan dengan baik tentunya dengan adanya dukungan, serta motivasi dari berbagai pihak, sehingga penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Bapak Prof. Dr. M. Suyanto, M.M selaku Ketua UNIVERSITAS AMIKOM Yogyakarta.
2. Bapak Sudarmawan, M.T selaku Ketua Program Studi S1 Informatika UNIVERSITAS AMIKOM Yogyakarta.
3. Bapak Ahlihi Masruro, M.Kom selaku dosen pembimbing yang telah membimbing dan memberikan pengarahan bagi penulis dalam penyusunan skripsi.
4. Kedua orangtua yang selalu memberikan dorongan positif, motivasi serta mendoakan penulis.
5. Bapak dan Ibu Dosen UNIVERSITAS AMIKOM Yogyakarta yang telah memberikan ilmu-ilmu yang bermanfaat sebagai bekal untuk penulis kedepannya.
6. Keluarga besar dan teman-teman 12-S1TI-07.

Penulis menyadari sepenuhnya bahwa dalam penyusunan skripsi ini masih banyak kekurangan. Oleh karena itu, penulis berharap kepada semua pihak agar dapat menyampaikan saran, masukan, dan koreksi yang sifatnya membangun ke arah yang lebih baik. Penulis juga memohon maaf apabila didalam skripsi yang dibuat, masih terdapat kekeliruan yang tidak semestinya. Akhir kata, semoga skripsi ini dapat bermanfaat bagi penulis dan juga bagi pembaca.

Yogyakarta, 20 Maret 2019

Penulis

Glen Hasller Sajori

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Kemajuan teknologi telah berkembang pesat, khususnya pada pertukaran informasi yang semakin global. Kemampuan untuk mengakses serta bertukar data sudah sangat cepat. Hal ini juga mempengaruhi dunia kriminalitas, seseorang atau kelompok tertentu secara sengaja mengambil dan menyebarluaskan ataupun menggunakan sebuah informasi penting tanpa tanggung jawab. Dengan demikian perlunya sebuah pengamanan untuk menjaga kerahasiaan suatu data, yang dikenal dengan kriptografi.

Kriptografi sangat dibutuhkan dalam pengamanan data dan informasi. Dengan adanya kriptografi, data atau informasi yang ada di komputer pengguna dapat terhindar dari pembajakan, penghapusan, dan penyubtitusian yang dilakukan oleh pengguna lain yang tidak berhak atas akses data tersebut. Dalam hal ini, digunakan suatu metode yaitu autentikasi yang berkaitan dengan identifikasi atau pengenalan kesatuan sistem maupun informasi itu sendiri.

Hasil dari penelitian ini adalah mengamankan data-data pengguna. Dengan menggunakan metode AES dengan melakukan proses enkripsi dan dekripsi, dimana data-data yang dimasukkan pengguna dienkripsi, sehingga pengguna lain yang ingin mengakses data tersebut perlu memasukkan kunci yang dibutuhkan untuk mendekripsi data yang sudah dienkripsi, agar dapat diakses. Sehingga data dan informasi dari pengguna yang bersangkutan tidak bocor atau terbongkar, dengan kata lain data-data tersebut aman.

Kata Kunci: Kriptografi, Keamanan, AES, Informasi, Enkripsi, Dekripsi.

ABSTRACT

Technological advances have developed rapidly, especially in information that is increasingly global. Data exchanging the ability to access has also been very fast. This also affects the world of crime, certain people or groups deliberately take and disseminate or use important information without responsibility. Thus the need for security to request the confidentiality of data, known as cryptography.

Cryptography is needed in securing data and information. With the existence of cryptography, data or information that is on the user's computer can avoid piracy, deletion, and subtitution done by other users who are not entitled to access the data. In this case, a method is used, namely related authentication or system participation as well as the information itself.

The results of this study are to secure user's data. By using the AES method by doing the encryption and decryption process, where the data entered by the user is encrypted, so other users who want to access this data need to enter the password needed to decrypt the encrypted data, so that it can be accessed. The data needed and information from the requested user does not leak or be uncovered, in other words the data is safe.

Keywords: *Cryptography, Security, AES, Information, Encryption, Decryption.*