APLIKASI ENKRIPSI DAN DEKRIPSI EMAIL MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD BERBASIS WEB

SKRIPSI

disusun oleh

Muhammad Muslih Waskito

16.21.0949

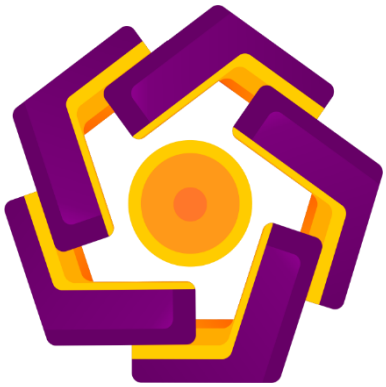
PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2017

APLIKASI ENKRIPSI DAN DEKRIPSI EMAIL MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD BERBASIS WEB

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Muhammad Muslih Waskito

16.21.0949

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2017

PERSETUJUAN

SKRIPSI

APLIKASI ENKRIPSI DAN DEKRIPSI EMAIL MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD BERBASIS WEB

yang dipersiapkan dan disusun oleh

Muhammad Muslih Waskito

16.21.0949

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 5 Mei 2017

Dosen Pembimbing

Andi Sunyoto, M.Kom

NIK. 190302052

PENGESAHAN

SKRIPSI
APLIKASI ENKRIPSI DAN DEKRIPSI EMAIL MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD BERBASIS WEB

yang dipersiapkan dan disusun oleh

Muhammad Muslih Waskito

16.21.0949

telah dipertahankan didepan Dewan Penguji

pada tanggal 18 Agustus 2017

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Dony Ariyus, M.Kom. **NIK. 190302128**	
Dina Maulina, M.Kom, **NIK. 190302250**	
Andi Sunyoto, M.Kom. **NIK. 190302052**	

Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar Sarjana Komputer

Tanggal 26 September 2017

DEKAN FAKULTAS ILMU KOMPUTER

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

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi yang sudah dibuat merupakan karya penulis 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 penulis 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 penulis secara pribadi.

Yogyakarta, 10 September 2017

Muhammad Muslih Waskito
16.21.0949

MOTTO

"Beriktiar dan bertawakal-lah kepada Allah maka jalanmu akan dimudahkan"

"Saling membantu satu sama lain dan berprasangka baik akan membuat hati menjadi bersih dari penyakit hati"

"Tidak ada yang tidak mungkin didunia ini kecuali atas izin Allah"

PERSEMBAHAN

Puji syukur saya panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat dan karunia-Nya, sehingga skripsi ini bisa selesai tepat waktu. Shalawat serta salam semoga tercurah kepada nabi agung Muhammad SAW beserta keluarga dan sahabat-sahabatnya. Skripsi ini saya persembahkan kepada :

1. Kedua orang tua saya dan kakak saya yang selalu mendukung, memberi semangat, motivasi serta do'a yang tanpa henti kepada saya.
2. Kepada Bapak Andi Sunyoto, M.kom dosen pembimbinng terbaik dalam membimbing saya. Hanya bisa berdoa semoga bapak diberikan kemudahan dalam hidup oleh Allah SWT.
3. Spesial juga untuk Endyah Wulandari yang selalu sabar dan menyemangati saya disaat saya mengalami kekurangan motivasi dalam pengerjaan skripsi ini.
4. Sahabat dan temen-temen seperjuangan Dani, Sigit, Iqbal, Wawan, Nila, Luvi, Rita, Arlinda, Joko, Bang Andi, Arum, Retno, Leo, Mas Ridwan, Qori Alya, Alan dan semuanya Kalian luar biasa.
5. Keluarga Besar 16-S1TI Transfer, Sukses buat kalian semua.
6. Untuk rekan-rekan cafe imers (Wicak, mbak Emi, mbak Nisa, mbak Alila, mas Roni dan pak Cahyo).
7. Semua pihak yang tidak dapat penulis sebutkan satu persatu yang telah membantu baik dukungan moril maupun materil, pikiran, dan tenaga dalam penyelesaian Skripsi ini.

Yogyakarta, 10 September 2017

Muhammad Muslih Waskito
16.21.0949

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Alhamdulillah, dengan mengucap syukur kepada Allah SWT, atas limpahan rahmat, nikmat dan karunia-Nya serta arahan dan bimbingan dari berbagai pihak akhirnya peneliti dapat menyelesaikan penyusunan skripsi yang berjudul "**APLIKASI ENKRIPSI DAN DEKRIPSI EMAIL MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD BERBASIS WEB**". Skripsi ini disusun sebagai salah satu persyaratan untuk menyelesaikan pendidikan pada Strata 1 dan untuk memperoleh gelar Sarjana Komputer di Universitas AMIKOM Yogyakarta.

Dalam penyusunan skripsi ini, peneliti telah menerima banyak bantuan, bimbingan serta dukungan yang sangat bermanfaat dari berbagai pihak. Oleh karena itu penulis mengucapkan terimakasih kepada:

1. Bapak Prof. Dr. M. Suyanto, MM selaku Rektor Universitas AMIKOM Yogyakarta.
2. Ibu Krisnawati, S.Si, M.T selaku Ketua Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
3. Bapak Sudarmawan, S.T, M.T selaku ketua Program Studi Informatika Universitas AMIKOM Yogyakarta.
4. Bapak Andi Sunyoto, M.Kom selaku Dosen Pembimbing, penulis berterima kasih atas bimbingan dan arahan kepada penulis dalam pembuatan skripsi.
5. Bapak dan Ibu Dosen Universitas AMIKOM Yogyakarta yang telah banyak memberikan ilmunya selama duduk di bangku perkuliahan.
6. Bapak, Ibu, Kakak dan Adik peneliti yang telah memberikan dukungan dan do'a kepada peneliti.
7. Teman-teman yang memberikan dukungan, do'a serta bantuan dalam mengerjakan skripsi.

Pada akhir kata, peneliti menyadari bahwa dalam penulisan skripsi ini masih jauh dari kesempurnaan. Karena itu, peneliti berharap kepada semua pihak agar dapat menyampaikan saran dan kritik yang bersifat membangun untuk kesempurnaan skripsi ini serta semoga skripsi ini bermanfaat bagi semua pihak yang membacanya.

Wassalamu'alaikum Wr. Wb.

Yogyakarta,10 September 2017

Muhammad Muslih Waskito

16.21.0949

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Kriptografi adalah bidang ilmu untuk menjaga keamanan pesan (message). Kriptografi telah banyak diimplementasikan di banyak hal seperti Smart card, Anjungan Tunai Mandiri (ATM), Pay TV, Mobile Phone, dan Komputer adalah beberapa contoh produk teknologi yang menggunakan kriptografi untuk keamanannya. Cara kerjanya adalah dengan mengubah pesan asli yang dapat imengerti/dibaca manusia (plainteks) ke bentuk lain yang tidak dapat dimengerti/dibaca oleh manusia (cipherteks). Proses transformasi plainteks menjadi chiperteks diistilahkan dengan enkripsi. Sedang proses pengembalian pesan chiperteks menjadi plainteks diistilahkan dengan dekripsi.

Ada banyak algoritma kriptografi, dalam penelitian ini aplikasi kriotografi yang dikembangkan untuk enkripsi dan dekripsi email menggunakan algoritma simetri AES (Advanced Encryption Standard) dengan mengunakan bahasa pemrograman PHP, HTML dan CSS. Advanced Encryption Standard (AES) merupakan standar enkripsi dengan kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat. Standar ini terdiri atas 3 blok cipher, yaitu AES-128, AES-192 and AES-256.

Aplikasi ini dibuat dengan menggunakan program sublime text untuk pebuatan interface dan sistem aplikasinya, XAMPP sebagai virtualserver dan MySql sebagai penyimpan data (database). Dalam pengujiannya, Aplikasi Enkripsi dan Dekripsi Email ini mampu melindungi data yang dikirim oleh pengguna melalui pesan email.

Kata Kunci : *Plainteks*, *Cipherteks*, Kriptografi , *Advanced Encryption Standard* (AES) , *sublimetext*, MySql, XAMPP

ABSTRACT

Abstract – Cryptography is the field of science to maintain the security of messages (message). Cryptography has been widely implemented in many ways such as Smart cards, Automated Teller Machines (ATMs), Pay TV, Mobile Phones, and Computers are some examples of technology products that use cryptography for security. The way it works is by changing the original message that a human can understand / read (plaintext) into another form that can not be understood / read by humans (cipherteks). The process of plaintext transformation into chiperteks is termed encryption. While the process of returning a text message into text is plaintext termed with decryption.

There are many cryptographic algorithms, in this research cryographic application developed for encryption and email decryption using AES (Advanced Encryption Standard) symmetry algorithm using PHP, HTML and CSS programming languages. Advanced Encryption Standard (AES) is a key-symmetric encryption standard adopted by the United States government. This standard consists of 3 blocks of ciphers, namely AES-128, AES-192 and AES-256.

This application is created by using sublime text program to pebuatan interface and application system, XAMPP as virtualserver and MySql as data storage (database). In testing, the Email Encryption and Decryption application is able to protect data sent by users via email messages.

Keywords: Plaintext, Ciphertext, Cryptography, Advanced Encryption Standard (AES), sublimetext, MySql, XAMPP