PEMBUATAN PERANGKAT LUNAK SEBAGAI MEDIA PEMBELAJARAN KRIPTOGRAFI ALGORITMA VIGENERE CIPHER DAN AES 128bit (*ADVANCED ENCRYPTION STANDARD*)

SKRIPSI

Disusun oleh

Gita Ramadanita Qamaril

11.11.5055

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA

2015

PEMBUATAN PERANGKAT LUNAK SEBAGAI MEDIA PEMBELAJARAN KRIPTOGRAFI ALGORITMA VIGENERE CIPHER DAN AES 128bit (*ADVANCED ENCRYPTION STANDARD*)

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika

Disusun oleh

Gita Ramadanita Qamaril

11.11.5055

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA

2015

PERSETUJUAN

SKRIPSI

PEMBUATAN PERANGKAT LUNAK SEBAGAI MEDIA PEMBELAJARAN KRIPTOGRAFI ALGORTIMA VIGENERE CIPHER DAN AES 128bit (*ADVANCED ENCRYPTION STANDARD*)

yang dipersiapkan dan disusun oleh

Gita Ramadanita Qamaril

11.11.5055

Telah disetujui oleh Dosen Pembimbing Skripsi

Pada tanggal 08 September 2015

Dosen Pembibing

Ema Utami, Dr., S.Si, M.Kom
NIK. 190302037

PENGESAHAN

SKRIPSI

PEMBUATAN PERANGKAT LUNAK SEBAGAI MEDIA PEMBELAJARAN KRIPTOGRAFI ALGORTIMA VIGENERE CIPHER DAN AES 128bit (*ADVANCED ENCRYPTION STANDARD*)

yang disusun oleh

Gita Ramadanita Qamaril
11.11.5055

telah dipertahankan di depan Dewan Penguji
pada tanggal 15 September 2015

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Robert Marco, M.T **NIK. 190302228**	
Barka Satya, M.Kom **NIK. 190302126**	
Ema Utami, Dr., S.Si, M.Kom **NIK. 190302037**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 15 September 2015

KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang bertandatangan di bawah 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 Instansi Pendidikan 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.

Yogyakarta, 15 September 2015

Gita Ramadanita Qamaril

11.11.5055

MOTTO

"Semua ini adalah rentetan dari sebuah proses, jalani semuanya dengan sabar maka kelak kamu akan mendapatkan hasil yang memuaskan"

HALAMAN PERSEMBAHAN

Segala puji hanyalah terucap bagi Allah SWT pencipta alam semesta ini yang telah menganugrahkan sekala nikmat untuk semua umat-NYA , Serta shalawat dan salam selalu tercurah kepada junjungan kita Nabi Muhammad SAW .

Ku persembahkan karya ini untuk kedua orang tua ku tercinta

Ayahanda Amir Gapuri dan Ibunda Rukanah

Terima kasih yang tak terhingga dan segala dukungan serta cinta kasih yang tiada mungkin bisa kubalas hanya dengan selembar kertas yang bertuliskan kata cinta dan persembahan. Semoga ini menjadi langkah awal untuk membuat kalian bahagia. Terima kasih selalu membuat termotivasi dan selalu mendo'akan ku serta menasihati agar menjadi lebih baik.

dan

Keluarga besar ku

"Yang selalu memberi dukungan, semangat serta nasihat-nasihat"

KATA PENGANTAR

Assalamu'alaikum wr.wb.

Puji syukur penulis panjatkan kepada Allah SWT , yang telah melimpahkan segala rahmat, karunia serta hidayah-Nya kepada penulis, dan sholawat serta salam tetap tercurahkan kepada Nabi Muhammad SAW, sehingga penulis dapat menyelesaikan serta menyusun Laporan Skripsi ini sebagai syarat untuk menyelesaikan studi Strata 1 Teknik Informatika STMIK AMIKOM Yogyakarta.

Penulis menyadari bahwa penyusunan skripsi ini tidak akan terselesaikan dengan baik, tanpa bantuan, petunjuk, bimbingan dan saran dari berbagai pihak. Oleh karenanya, pada kesempatan ini dengan kerendahan hati, penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Sang Khalik Allah Subhanahu Wa Ta'ala, yang selalu memberikan petunjuk, pencerahan, kemudahan serta ridho, dan kasih sayang yang tiada terkira kepada setiap hamba-Nya, dan tidak terkecuali kepada penulis.
2. Nabi besar Muhammad Shalallahu Alaihi Wa Sallam.
3. Bapak Prof. Dr. M. Suyanto, M.M. selaku Ketua STMIK AMIKOM Yogyakarta,
4. Bapak Sudarmawan, M.T, selaku Ketua Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta,
5. Ibu Ema Utami, Dr., S.Si, M.Kom, selaku dosen pembimbing yang telah mendukung dan membimbing sampai laporan ini selesai,
6. Kepada seluruh dosen STMIK AMIKOM Yogyakarta, Terima kasih atas ilmu yang diberikan, semoga penulis dapat mengamalkan dan menjadikan sebagai amal jariyah,
7. Ayahanda Amir Gapuri dan Ibunda Rukanah selaku kedua orang tua penulis yang selalu memberikan dukungan dan motivasi selama penulisan laporan ini,
8. Muhammad Rizqiannor yang selalu menemani dan memberi semangat dalam menyelesaikan Skripsi ini,

9. Seluruh teman-teman S1TI-06, terkhusus Lutfi Fauziah, Nurul Hidayah, Elvira Devina N.F, yang selalu memberi masukan dalam penyelesaian Skripsi ini,
10. Teman-teman Asrama Himpunan Mahasiswa dan Pelajar Tabalong Putri "Kambang Tanjung" yang selalu mendukungku dan mendidik ku selama berada di Kota Yogyakarta ini.
11. Semua pihak yang tidak dapat disebutkan satu persatu atas perhatian dan curahan ide sehingga skripsi ini dapat diselesaikan dengan baik.

Menyadari bahwa laporan ini masih jauh dari sempurna maka penulis mengharapkan segala kritik dan saran dari para pembaca agar laporan ini dapat lebih sempurna sehingga dapat menjadi perbaikan untuk penyusunan laporan di masa mendatang. Semoga laporan ini dapat bermanfaat bagi para pembaca pada umumnya dan penulis pada khususnya.

Yogyakarta, 15 September 2015

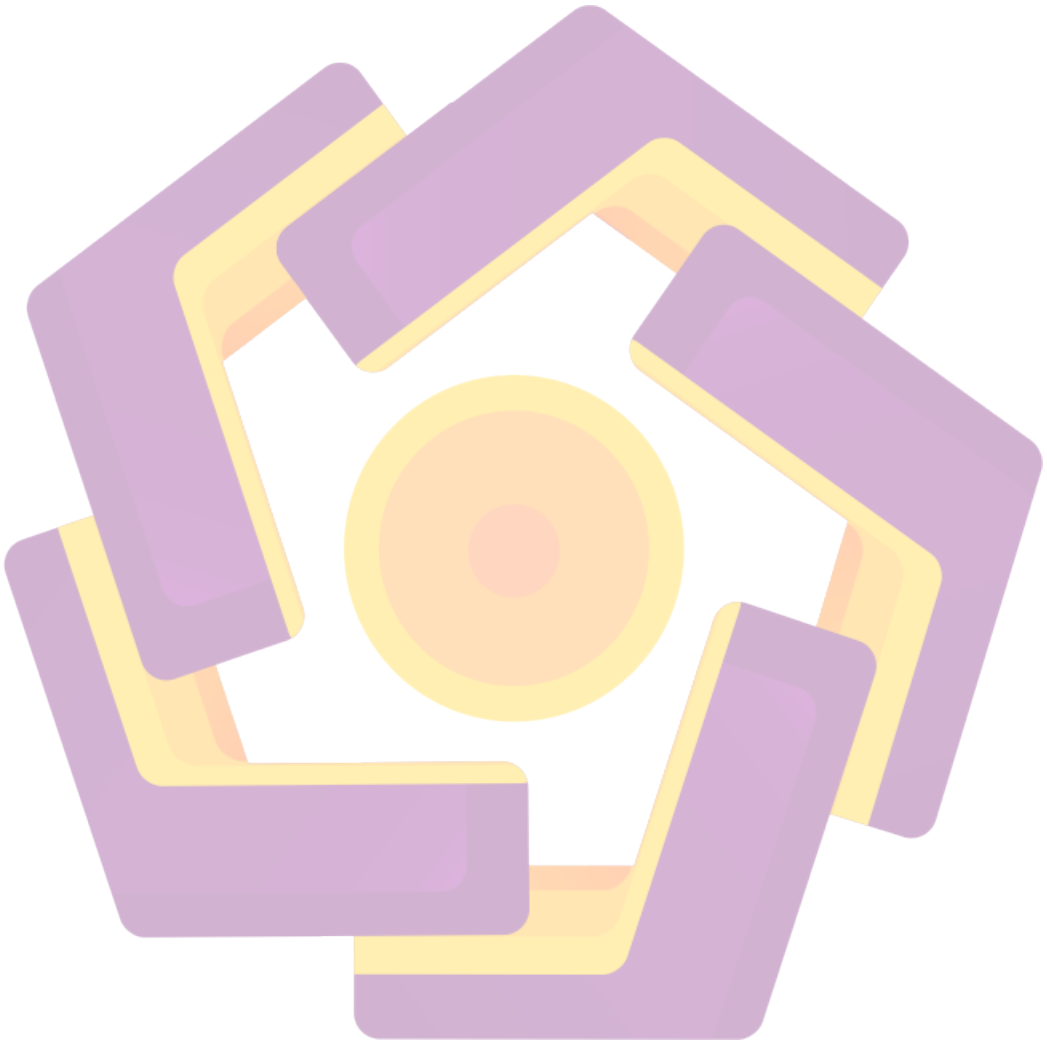
Penulis,

Gita Ramadanita Qamaril

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR



INTISARI

Pengamanan sistem informasi memiliki beberapa dasar-dasar dan teori yang digunakan. Kriptografi, enkripsi dan dekripsi merupakan dasar dari pengamanan sistem informasi. Algoritma Vigenere Cipher dan AES merupakan beberapa algoritma pada kriptografi yang dapat digunakan atau diimplementasikan sebagai pengamanan sistem informasi.

Dikarenakan peranan kriptografi yang penting, oleh karena itu di dalam dunia pendidikan diperlukan suatu aplikasi untuk mempelajari kriptografi secara visual dan interaktif. Di beberapa tempat kuliah dan belajar sering sekali ditemukan pembelajaran kriptografi yang masih menggunakan teori-teori tanpa langsung melihat apa yang terjadi di dalam proses kriptografi tersebut.

Maka dari itu, akan dibuat suatu perangkat lunak pembelajaran kriptografi klasik yang dapat mempermudah dalam mempelajari proses dari beberapa algoritma kriptografi seperti vigenere dan AES, dengan visualisasi dan proses dalam perubahan data.

Kata kunci : Kriptografi, Vigenere, AES, perubahan data.

ABSTRACT

Information system security has some basics and theory are used. Cryptography, encryption and decryption is the Foundation of the security of information systems. Vigenere Cipher Algorithm and AES cryptographic algorithm on some of that can be used or implemented as information systems security.

Due to the role of cryptography are important, therefore in the educated world needed an application to learn Cryptography visually and interactively. In some places lecture and study often found still using cryptographic learning theories without directly see what is going on inside the cryptographic process.

Therefore, it will be created a classic Cryptography learning software that can ease in learning process of several cryptographic algorithms such as AES and vigenere, with visualization and data changes in the process.

***Keywords**: Cryptography, Vigenere, AES, data changes*