HYBRID CRYPTOSYSTEM UNTUK PENGAMANAN E-DOKUMEN MENGGUNAKAN ALGORITMA RC4, RSA DAN MD5

SKRIPSI

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

disusun oleh

Rano Alyas

11.11.5425

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

2014

PERSETUJUAN

SKRIPSI

HYBRID CRYPTOSYSTEM UNTUK PENGAMANAN E-DOKUMEN MENGGUNAKAN ALGORITMA RC4, RSA DAN MD5

yang dipersiapkan dan disusun oleh

Rano Alyas

11.11.5425

yang disetujui oleh Dosen Pembimbing Skripsi
pada Tanggal 21 Februari 2014

Dosen Pembimbing,

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

PENGESAHAN

SKRIPSI

***HYBRID CRYPTOSYSTEM* UNTUK PENGAMANAN E-DOKUMEN MENGGUNAKAN ALGORITMA RC4, RSA DAN MD5**

yang dipersiapkan dan disusun oleh

Rano Alyas

11.11.5425

telah dipertahankan di depan Dewan Penguji
pada tanggal 20 Agustus 2014

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Hartatik, S.T, M.Cs **NIK. 190000017**	
Bayu Setiaji, M. Kom **NIK. 190302216**	
Ema Utami Dr., S.Si, M. Kom **NIK. 190302037**	

Skripsi ini telah diterima sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 25 Agustus 2014

KETUA STMIK AMIKOM YOGYAKARTA

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

PERNYATAAN

Yang bertandatangan dibawah ini saya :

Nama : Rano Alyas

NIM : 11.11.5425

Jurusan : Teknik Informatika

Selaku mahasiswa STMIK AMIKOM Yogyakarta yang menyusun skripsi ini, saya menyatakan bahwa skripsi ini adalah benar-benar murni hasil karya intelektual saya setelah melakukan pengumpulan data dan mengambil referensi dari berbagai sumber. Dan jika dikemudian hari terjadi pertentangan terhadap skripsi ini, saya siap untuk mempertanggungjawabkannya.

Demikian surat pernyataan keaslian ini saya buat dalam keadaan sadar dan tanpa pengaruh apapun.

Yogyakarta, 21 Februari 2014

Rano Alyas

NIM 11.11.5425

HALAMAN MOTO

- ✓ Mulailah sesuatu dengan membaca "Bismillahirrahmanirrahim" dan diakhiri dengan "Alhamdulillahirobbil 'alamin" agar sesuatu yang kita kerjakan di ridhoi Allah SWT.

- ✓ Jadikan kepandaian sebagai kebahagiaan bersama, sehingga mampu meningkatkan rasa ikhlas tuk bersyukur atas kesuksesan.

- ✓ Bersyukurlah atas apa yang kamu miliki saat ini, karena masih banyak orang disekeliling kamu masih kurang beruntung.

- ✓ *"Life is a struggle, there is no life without a struggle."*

- ✓ *"Life is like a wheel, sometimes you will be on the top, sometimes you will be at the bottom. It is not important when we become on the top or at the bottom. But the most important is syukur when success and shabar when fail."*

- ✓ *just do it, it will go away* (Skripsi – Pendadaran – Yudisium - Wisuda)., *and in the end we will always say* "Cuma kayak gini toh"

HALAMAN PERSEMBAHAN

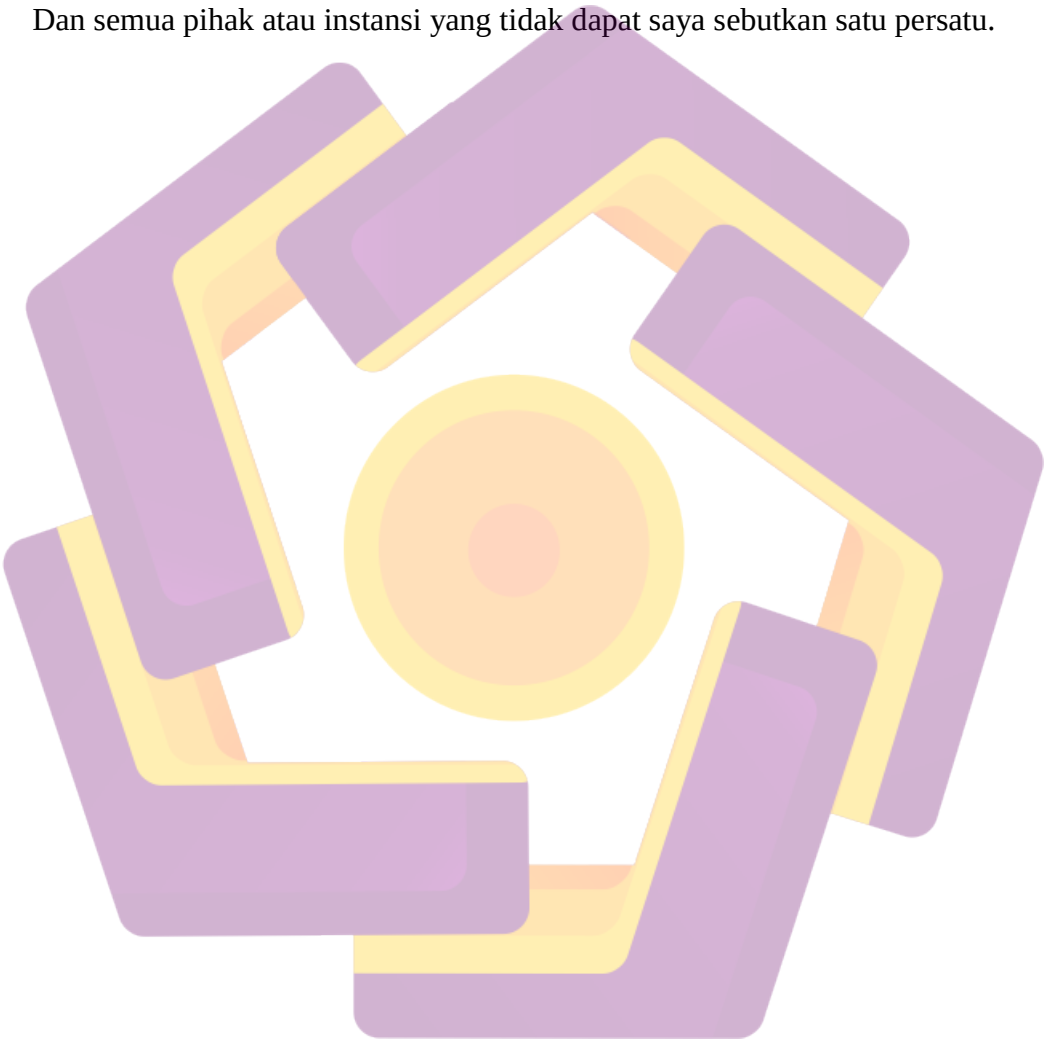
Puji syukur senantiasa terucap kehadirat Alloh SWT, yang telah melimpahkan nikmat yang luar biasa kepada setiap hamba-Nya. Shalawat serta salam selalu tercurah kepada Nabi Muhammad SAW.

Skripsi ini saya persembahkan kepada pihak-pihak yang telah memberikan dukungan. Skripsi ini di dedikasikan untuk :

1. Kedua Orang Tua, yang telah memberikan dukungan baik moril maupun materiil. Untuk doa dan perhatian serta kesabarannya membimbing dan mengajarkan segala hal.
2. Mas dan Mba ku tercinta, pakdhe, budhe, semua keluarga besar baik dari bapak maupun ibu. Terima kasih atas petuah, nasihat, serta doanya.
3. Keponakan ku tersayang, dhe Vera, Danniz, Arqi, dan dhe Njey, terima kasih atas senyuman, candaan, dan tingkah lucu kalian.
4. Teman-teman 11-S1TI-11, yang telah banyak memberikan kenangan di kampus ungu tercinta. Terima kasih atas dukungan, kritik, dan sarannya semoga kita semuanya sukses dunia akhirat.Amin. .
5. Seluruh Keluarga Besar Badan Eksekutif Mahasiswa AMIKOM Kabinet “Normalisasi kontribusi” dan “Sinergis Berkarakter”. Terima kasih atas suasana kekeluargaannya selama ini, dukungan dan doanya.
6. Teman-teman ku, Aris, Prast, Ardun, Iyan, Nana, Ninda, Mas Erwandy, Akhid, Chandra, Devi, Yunis dan Fikri, Wina yang di Bumiayu. Terima kasih tingkah gila dan lucu kalian.semoga kita jadi sahabat sejati.

7. Teman-teman Asisten (HS II, Stuktur Data, Pemrog Lanjut, PBO 2), Kontrakan "Rumah Kece", Fighter School, Public Relations School, Forum Asisten, yang telah men*support* dan memberikan share ilmu serta doanya.

Dan semua pihak atau instansi yang tidak dapat saya sebutkan satu persatu.



KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa yang telah memberikan rahmat dan hidayahnya, sehingga penulisan Skripsi ini dapat penulis selesaikan.

Pembuatan Skripsi ini guna memenuhi persyaratan akademis untuk memperoleh gelar Sarjana Komputer di STMIK AMIKOM Yogyakarta.

Penulis sangat menyadari bahwa dalam penulisan Skripsi ini sangat jauh dari kesempurnaan, karena keterbatasan kemampuan dan pengetahuan yang penulis miliki, dan juga walaupun Skripsi ini sangat sederhana namun tanpa bantuan dari berbagai pihak tentunya penulis akan mengalami kesulitan. Oleh karena itu dalam kesempatan ini, penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. M.Suyanto, Prof., Dr., MM. selaku Ketua STMIK AMIKOM Yogyakarta.
2. Ema Utami, Dr., S.Si., M.Kom. selaku Dosen Pembimbing yang telah meluangkan waktunya untuk membimbing penulis dengan penuh kesabaran.
3. Ibu Hartatik, M.Cs, Bpk.Hastari Utama, S.Kom., M.Cs dan Bapak Emha Taufiq Luthfi, M.Kom. yang juga telah membantu penulis dalam menyelesaikan Skripsi ini.
4. Segenap staf pengajar STMIK AMIKOM Yogyakarta yang telah banyak memberikan ilmunya dan pengalaman selama penulis kuliah.
5. Orang Tua penulis yang telah mendoakan dan memberi dukungannya.

6. Seluruh pihak yang telah membantu penulis dalam menyelesaikan Skripsi ini.

Penulis menyadari bahwa pembuatan Skripsi ini jauh dari sempurna, oleh karena itu saran dan kritik yang bersifat membangun sangat penulis harapkan demi sempurnanya skripsi ini. Namun, penulis tetap berharap skripsi ini akan bermanfaat bagi semua pihak yang membacanya.

Yogyakarta, 21 Februari 2014

Penyusun

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Pertukaran dokumen di dunia maya sudah banyak digunakan dalam transaksi komersial. Oleh karena itu, dokumen merupakan peranan penting yang harus di amankan oleh setiap *user*. Keamanan dari suatu dokumen merupakan hal yang perlu diperhatikan dalam menjaga kerahasiaan informasi, terutama untuk informasi yang isinya hanya boleh diketahui oleh pihak yang berwenang saja. Pengiriman data atau informasi tanpa dilakukan pengamanan akan beresiko terhadap penyadapan dan informasi yang ada di dalamnya dapat mudah diketahui oleh pihak-pihak yang tidak berwenang.

Salah satu cara untuk mengamankan dokumen adalah dengan menggunakan algoritma kriptografi. Prinsip pengamanan dokumen ini adalah bagaimana sistem dapat mengamankan proses penyimpanan dan pengiriman dokumen menggunakan *hybrid cryptosystem*. Pada penelitian ini, penggunaan *hybrid cryptosystem* merupakan gabungan algoritma RC4, RSA dan MD5. Adapun tahapan pengamanan dokumen ini meliputi tiga tahapan yaitu proses pengamanan data, pengamanan kunci, dan pengujian integritas sebuah berkas.

Aplikasi yang dibangun dapat melakukan enkripsi dan dekripsi file / dokumen. Hasil pengujian yang telah dilakukan dapat disimpulkan bahwa aplikasi telah mampu menunjukkan dan melakukan enkripsi dan dekripsi pada dokumen file. Kinerja aplikasi ini dapat disimpulkan bahwa semakin besar ukuran file yang dienkripsi maka semakin lama prosesnya dan semakin tinggi spek komputer yang digunakan maka semakin cepat pula proses enkripsi dan dekripsi yang diproses dalam aplikasi SecureDoc.

Kata Kunci : *Hybrid Cryptosystem*, Kriptografi, RC4, RSA, MD5 dan Dokumen.

ABSTRACT

The exchange of documents in cyberspace already widely used in commercial transactions . Therefore , the document is an important role that must be secured by each user . Security of a document is to be considered in maintaining the confidentiality of information , especially for the contents of information that should only be known by the authorities alone . Delivery of data or information without any security will be at risk to eavesdropping and the information in it can be easily identified by parties who are not authorized .

One way to secure the document is to use a cryptographic algorithm . The principle of security of this document is how the system can secure the storage and delivery of documents using a hybrid cryptosystem . In this research , the use of hybrid cryptosystem is combination the RC4 algorithm , RSA and MD5. The stages of the security document includes three stages: data security processes , security locks , and testing the integrity of a file .

Applications built can perform encryption and decryption of file / document. The results of the testing that has been done can be concluded that the application has been able to show and perform encryption and decryption on a document of file. The performance of these applications can be concluded that the larger the file size the longer the process in encrypted and the higher spec computer used the faster encryption and decryption processes are processed on SecureDoc applications.

Keywords : *Hybrid Cryptosystem , Cryptography , RC4 , RSA , MD5 and Documents.*