APLIKASI PENGAMANAN DOKUMEN DENGAN MENGGUNAKAN TEKNIK KRIPTOGRAFI ALGORITMA AES-RINJDAEL

Oleh

ARI

1011500176

PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

ATMA LUHUR

PANGKALPINANG

2013

APLIKASI PENGAMANAN DOKUMEN DENGAN MENGGUNAKAN TEKNIK KRIPTOGRAFI ALGORITMA AES-RINJDAEL

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh

ARI

1011500176

PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

ATMA LUHUR

PANGKALPINANG

2013


STMIK
ATMA LUHUR
PANGKAL PINANG

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini :

NIM : 1011500176

Nama : Ari

Judul Skripsi : APLIKASI PENGAMANAN DOKUMEN DENGAN MENGGUNAKAN TEKNIK KRIPTOGRAFI ALGORITMA AES-RINJDAEL

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan di dalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Pangkalpinang, 21 September 2013

(Ari)

LEMBAR PENGESAHAN SKRIPSI

APLIKASI PENGAMANAN DOKUMEN DENGAN MENGGUNAKAN TEKNIK KRIPTOGRAFI ALGORITMA AES-RINJDAEL

Yang dipersiapkan dan disusun oleh

Ari

1011500176

Telah dipertahankan di depan Dewan Penguji

Pada Tanggal 21 September 2013

Susunan Dewan Penguji

Anggota	**Dosen Pembimbing**
Tri Ari Cahyono, M.Kom	**Bambang Adiwinoto, M.Kom**
NIDN. 0613018201	**NIDN. 0216107102**
Ketua	**Kaprodi Teknik Informatika**
Ellya Helmud, M.Kom	**Sujono, M.Kom**
NIDN. 0201027901	**NIDN. 0211037702**

Skripsi ini telah diterima dan sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 21 September 2013

KETUA STMIK ATMA LUHUR PANGKALPINANG

Dr. Moedjiono, M.Sc


STMIK
ATMA LUHUR
PANGKAL PINANG

ABSTRAKSI

Seiring dengan perkembangan zaman, kebutuhan manusia yang semakin meningkat termasuk kebutuhan akan informasi. Oleh sebab itu, pengiriman dan penyimpanan data melalui media elektronik memerlukan suatu proses yang mampu menjamin keamanan dan keutuhan dari data tersebut. Untuk menjamin keamanan dan keutuhan dari suatu data, dibutuhkan suatu proses penyandian. Enkripsi dilakukan ketika data akan dikirim. Proses ini akan mengubah suatu data asal menjadi data rahasia yang tidak dapat dibaca. Sementara itu, proses dekripsi dilakukan oleh penerima data yang dikirim tersebut. Data rahasia yang diterima akan diubah kembali menjadi data asal. Dengan cara penyandian tadi, data asli tidak akan terbaca oleh pihak yang tidak berkepentingan, melainkan hanya oleh penerima yang memiliki kunci dekripsi. Didorong oleh kegunaan yang penting tadi, teknik (algoritma) penyandian telah berkembang sejak zaman dahulu kala. Mulai dari era sebelum masehi, hingga sekarang algoritma penyandian ini selalu berkembang. Pertimbangan bahwa sebuah standard algoritma yang baru sangatlah diperlukan untuk tetap menjaga kerahasiaan suatu data. Dalam hal ini, kunci yang lebih panjang juga merupakan keharusan.

Saat ini, AES digunakan sebagai standar algoritma kriptografi yang terbaru. Algoritma sebelumnya dianggap tidak mampu lagi untuk menjawab tantangan perkembangan teknologi komunikasi yang sangat cepat. AES sendiri adalah algoritma kriptografi dengan menggunakan algoritma Rijndael yang dapat mengenkripsi dan mendekripsi blok data sepanjang 128 bit dengan panjang kunci 128 bit, 192 bit, atau 256 bit.


STMIK
ATMA LUHUR
PANGKAL PINANG

KATA PENGANTAR

Dengan segala puji dan syukur penulis panjatkan ke hadirat Allah SWT yang telah melimpahkan segala rahmat serta karuniaNya, sehingga penulis dapat menyelesaikan laporan skripsi ini yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada jurusan Teknik Informatika STMIK ATMA LUHUR Pangkalpinang.

Dalam penyusunan laporan skripsi ini tentu saja banyak sekali hambatan yang membuat penulis kesulitan. Tapi berkat bimbingan, do'a, serta motivasi dari berbagai pihak, sehingga penulis dapat menyelesaikan laporan skripsi ini tepat pada waktunya. Untuk itu, dengan segala kerendahan hati, penulis ingin mengucapkan rasa terima kasih yang sebesar-besarnya kepada :

1. Allah SWT yang telah senantiasa memberikan segalanya kepada penulis hingga saat ini.
2. Kedua orang tua yang selalu memberikan semangat berupa moril dan materil kepada penulis di saat susah maupun senang.
3. Istri tercinta serta malaikat kecil kami yang selalu memberikan senyuman setiap saat.
4. Bapak Dr. Moedjiono, M.Sc, selaku ketua STMIK Atma Luhur Pangkalpinang.
5. Bapak Bambang Adiwinoto, M.Kom, selaku dosen pembimbing yang telah banyak sekali membantu dalam memberikan pengarahan kepada penulis dalam menyelesaikan laporan skripsi ini.
6. Kepada kakak dan adik-adik yang telah senantiasa memberikan dukungan kepada penulis.
7. Teman-teman seperjuangan selama masa perkuliahan di STMIK Atma Luhur Pangkalpinag yang tidak dapat saya sebutkan satu persatu "terima kasih semuanya".

8. Semua dosen di STMIK Atma Luhur Pangkalpinang yang telah setia membagikan ilmunya kepada penulis selama masa perkuliahan.
9. Untuk semua pihak yang turut membantu dalam memberikan do'a, semangat, serta dukungan moril meskipun kalian tidak ditulis, penulis tetap berterima kasih dan mengingat kalian semua.

Penulis menyadari bahwa laporan skripsi ini masih jauh dari kesempurnaan. Maka dari itu, penulis sangat mengharapkan kritik serta saran yang sifatnya membangun dari semua kalangan agar bisa meningkatkan ilmu pengetahuan penulis untuk masa yang akan datang.

Akhir kata penulis kembalikan segala-galanya kepada Allah SWT, jika terdapat kekurangan itu datangnya dari penulis pribadi, dan apabila ada kebenaran di dalamnya, semuanya datang dari Allah SWT. Semoga laporan skripsi ini dapat bermanfaat bagi mahasiswa/mahasiswi STMIK Atma Luhur Pangkalpinang khususnya serta para pembaca pada umumnya. Semoga Allah SWT selalu memberikan rahmat, hidayah, berkah dan cintaNya kepada kita semua dan memasukkan kita kedalam golongan orang-orang yang selalu bersyukur "Amin".

Pangkalpinang, September 2013

Penulis


STMIK
ATMA LUHUR
PANGKAL PINANG

DAFTAR ISI

Halaman

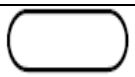
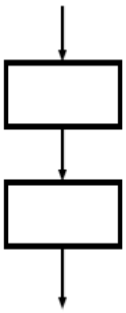
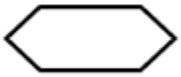
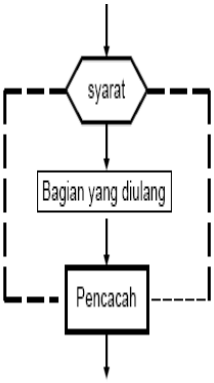
DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR SIMBOL

Keterangan	Lambang	Keterangan	Lambang
mulai/selesai		sequence	
aliran data		process	
input/output			
proses			
percabangan(decision)			
pemberian nilai awal suatu variabel (preparation)			
memanggil prosedur/ fungsi call		perulangan	
connector(pada halaman yang sama)			
connector(pada halaman yang berbeda)			