# PERANCANGAN DAN IMPLEMENTASIAPLIKASI PENGAMANAN DATA MENGGUNAKAN ALGORITMA RIJNDAEL

**SKRIPSI**


disusun oleh

**Agung Budi Utomo**

**11.11.5205**



**JURUSAN TEKNIK INFORMATIKA**
**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER**
**AMIKOM YOGYAKARTA**
**YOGYAKARTA**
**2015**

# PERANCANGAN DAN IMPLEMENTASIAPLIKASI PENGAMANAN DATA MENGGUNAKAN ALGORITMA RIJNDAEL

**SKRIPSI**

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Sistem Informasi


disusun oleh

**Agung Budi Utomo**

**11.11.5205**



**JURUSAN TEKNIK INFORMATIKA**
**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER**
**AMIKOM YOGYAKARTA**
**YOGYAKARTA**
**2015**

# PERSETUJUAN

## SKRIPSI

## PERANCANGAN DAN IMPLEMENTASI APLIKASI PENGAMANAN DATA MENGGUNAKAN ALGORITMA RIJNDAEL

yang disusun oleh

**Agung Budi Utomo**

**11.11.5205**

telah disetujuai oleh Dosen Pembimbing Skripsi

pada tanggal 5 Agustus 2015

**Dosen Pembimbing,**

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

# PENGESAHAN

## SKRIPSI

## PERANCANGAN DAN IMPLEMENTASI APLIKASI PENGAMANAN DATA MENGGUNAKAN ALGORITMA RIJNDAEL

yang disusun oleh

**Agung Budi Utomo**

**11.11.5205**

telah dipertahankan di depan Dewan Penguji
pada tanggal 2 September 2015

**Susunan Dewan Penguji**

| Nama Penguji | Tanda Tangan |
|---|---|
| **Anggit Dwi Hartanto, M.Kom**<br>**NIK. 190302163** | |
| **Hartatik, S.T., M.Cs**<br>**NIK. 190302232** | |
| **Ema Utami, Dr., S.Si, M.Kom**<br>**NIK. 190302037** | |

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 2 September 2015

**KETUA STMIK AMIKOM YOGYAKARTA**

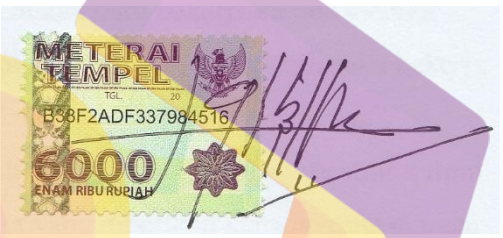
**Prof. Dr. M. Suyanto, M.M.**
**NIK. 190302001**

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya sayasendiri (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, 10 September 2015




Agung Budi Utomo

NIM. 11.11.5205

# MOTTO

"Hidup memang berawal dari sebuah mimpi, tapi mimpi juga tidak akan terwujud jika tidak ada niat yang besar dari kita sendiri."

"Keberhasilan adalah sebuah proses. Niatmu adalah awal keberhasilan. Peluh keringatmu adalah penyedapnya. Tetesan air matamu adalah pewarnanya. Do'amu dan do'a orang-orang isekitarmu adalah bara api yang mematangkannya. Kegagalandi setiap langkahmu adalah pengawetnya. Maka dari itu, bersabarlah! Allah selalu menyertai orang-orang yang penuh kesabaran dalam proses menuju keberhasilan. Sesungguhnya kesabaran akan membuatmu mengerti bagaimana cara mensyukuri arti sebuah keberhasilan."

"Untuk memperoleh suatu kesuksesan, keberanianmu harus lebih besar daripada ketakutanmu. Sehingga berani mengambil kepustusan dan siap menerima konsekuensinya."

"Aku percaya bahwa apapun yang aku terima saat ini adalah yang terbaik dari Allah S.W.T dan aku percaya Dia akan memberikan yang terbaik untukku disaat aku siap dan pantas untuk menerimanya."

"Tidak semua kesuksesan diukur menggunakan kekayaan dan materi, tetapi sukses adalah sebuah pencapaian dari apa yang kita inginkan."

# PERSEMBAHAN

Puji syukur kepada Allah SWT, atas segala nikmat hidup dan kesempatan mengenggam ilmu, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Perancangan Dan Implementasi Aplikasi PengamananData Menggunakan Algoritma Rijndael". Skripsi ini disusun sebagai salah satu persyaratan untuk mencapai derajat Sarjana Komputer jurusanTeknik Informatika. Dalam penelitian dan penyusunan skripsi ini, penulis banyak dibantu, dibimbing, dan didukung oleh berbagai pihak. Oleh karena itu, pada kesempatan ini penulis sangat ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Allah SWT yang selalu melimpahkan rahmat dan karunia-Nya serta memberikan kelancaran dan kemudahan kepada saya sehingga dapat menyelesaikan skripsi dengan baik.Semoga keberhasilan ini menjadi satu langkah awal bagiku untuk meraih cita-cita besarku.
2. Terima kasih kepada orang tua, bapak dan ibu, yang selalu menyelipkan nama anakmu dalam setiap do'a yang dipanjatkan, demi kesuksesan anak-anakmu. Serta dukungan baik secara moral dan material yang sampai terselesaikan skripsi ini.
3. Kepada keluarga besar,saudara, para adik, kakek-nenek, dan lainnya yang selalu mendukung serta tiada henti memberikan semangat.
4. Para dosen yang telah memberikan ilmu kepada saya, sehingga saya dapat menyelesaikan janjang S1 Teknik Informatika.
5. Teman dan sahabat tercinta yang telah mendukung dan menemani saya setiap saat. Terima kasih untuk kalian semua, *wish you all the best*.
6. Untuk yang pernah menemani (Sri Darwatik) ataupun yang belum sempat berjumpa, terimakasih untuk semuanya yang pernah tercurah untukku. Untuk seseorang di relung hati percayalah bahwa hanya ada satu namamu yang selalu kusebut-sebut dalam panjatan do'aku, semoga keyakinan dan takdir ini akan terwujud, insyallah jodohnya kita bertemu atas ridho dan izin Allah S.W.T

# KATA PENGANTAR

Puji syukur kehadirat Allah SWT, atas limpahan Rahmat dan Karunia-Nya, sehingga penulis dapat merampungkan skripsi dengan judul: “Perancangan Dan Implementasi Aplikasi PengamananData Menggunakan Algoritma Rijndael”. Ini untuk memenuhi salah satu syarat menyelesaikan studi serta dalam rangka memperoleh gelar Sarjana Komputer pada Program Studi S1 Teknik Informatika STMIK AMIKOM Yogyakarta.

Penghargaan dan terima kasih yang setulus-tulusnya kepada Ayahanda dan Ibunda yang kusayangi yang telah mencurahkan segenap cinta dan kasih sayang serta perhatian moril maupun materil. Semoga Allah SWT selalu melimpahkan Rahmat, Kesehatan, Karunia dan keberkahan di dunia dan di akhirat atas budi baik yang telah kalian berikan.

Dalam penyusunan dan penulisan skripsi ini tidak terpas dari bantuan, bimbingan, serta dukungan dari berbagai pihak. Oleh karena itu dalam kesempatan ini penulis dengan senang hati menyampaikan terima kasih kepada yang terhormat:

1. Bapak Prof Dr M. Suyanto, MM, selaku ketua STIMK AMIKOM Yogyakarta yang telah mengesahkan secara resmi judul penelitian sebagai bahan penulisan skripsi, sehingga penulisan skripsi dapat berjalan dengan lancar.
2. Bapak Sudarmawan, MT, selaku ketua jurusan S1 Teknik Informatika STMIK AMIKOM Yogyakarta yang telah mengesahkan secara resmi naskah publikasi sehingga pengerjaannya dapat berjalan dengan lancar.
3. Ibu Ema Utami, Dr., S.Si, M.Kom, selaku pembimbing, yang membimbing penulis dalam mengerjakan skripsi, sehingga penulisan skripsi dapat berjalan dengan lancar.
4. Anggit Dwi Hartanto, M.Kom,Hartatik, S.T., M.Cs, Ema Utami, Dr., S.Si, M.Kom, selaku penguji yang telah menguji hasil dari skripsi saya sehingga nantinya dapat dipertanggung jawabkan.

5. Bapak dan Ibu dosen jurusan Teknik Informatika khususnya yang telah mengajar di kelas S1-TI08 yang telah banyak memberikan bekal ilmu pengetahun sehingga penulis dapat menyelesaikan studi dan menyelesaikan penulisan skripsi ini.
6. Rekan-rekan mahasiswajurusan Teknik Informatika angkatan tahun 2011 yang telah banyak memberikan masukan kepada penulis baik selama dalam mengikuti perkuliahan maupun dalam penulisan skripsi ini.
7. Teman-teman satu kelas 11-S1TI-08 yang telah banyak memberikan kenang-kenangan yang sangat mengesankan dan pengalaman baik di kampus maupun di luar kampus bersama kalian.
8. Terkhusus untuk kalian sahabat-sahabat ku kontrakan melati dan teratai, ucapan terimakasih tidak lah cukup untuk membayar semua kenangan, pengalaman serta ilmu yang telah di dapatkan selama bersama kalian. Semoga suatu saat nnanti kita bertemu kembali dengan kesuksesan ditangan kita semua.

Akhirnya, dengan segala kerenadahan hati penulis menyadari masih banyak terdapat kekurangan-kekurangan, sehingga penulis mengharapkan adanya saran dan kritik yang bersifat membangun demi kesempurnaan skripsi ini.

Yogyakarta, 10 September 2015

Penulis

# DAFTAR ISI

## DAFTAR TABEL

## DAFTAR GAMBAR

# DAFTAR ISTILAH

| | | |
|---|---|---|
| Enkripsi | : | Proses penyandian sebuah pesan atau data menggunakan algoritma tertentu sehingga isi dari pesan atau data diubah menjadi sandi yang tidak dapat dipahami oleh pihak yang tidak memiliki wewenang atas isi dari pesan atau data tersebut. |
| Dekripsi | : | Proses pengembalian pesan atau data yang dienkripsi menjadi data asli sehingga isinya dapat dipahami oleh pihak yang berhak. |
| Plaintext | : | Pesan asli yang akan diamankan atau disandikan isinya. |
| Chipertext | : | Hasil dari proses enkripsi dari penyandian pesan asli. |
| Public Key | : | Kunci yang diketahui oleh khlayak banyak (umum) yang berguna untuk menyandikan pesan saja bisa untuk menyandikan dan membuka pesan. |
| Private Key | : | Kunci yang hanya diketahui oleh pihak – pihak tertentu berguna untuk menyandikan atau membuka isi dari suatu pesan. |
| Grayscale | : | Metode penyandian sebuah data yang berupa gambar (citra digital), yang nanti hasil dari penyandiannya berwarna abu-abu. |

# INTISARI

AES ( *Advance Encryption Standard* ) 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.

Keamanan merupakan salahsatu prioritas utama dizaman teknologi yang menuntut akan keutuhan privasi. Faktor keamanan tidak hanya dibutuhkan oleh lembaga militer dan pemerintah, tetapi juga sektor bisnis dan perseoranganyang selalu erat hubunganya dengan pengiriman dan penyimpanan data melalui media elektronik. Dimana hal tersebut memerlukan suatu proses yang mampu menjamin keamanan dan keutuhan isi 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 asli menjadi data rahasia yang tidak dapat dibaca. Sementara itu, proses dekripsi dilakukan untuk mengubah kembali menjadi data asli.

Salah satu solusinya yaitu algoritma Rijndael yang diimplementasikan pada sebuah aplikasi Virtual Basic 6.0, yang tidak hanya untuk mengamankan kata atau kalimat tetapi juga mengamankan data yang berupa gambar digital, audio, dan video.

**Kata kunci:** AES, enkripsi, dekripsi, keamanan data, Rijndael.

## *ABSTRACT*

*AES ( Advance Encryption Standard ) is by using a cryptographic algorithm Rijndael algorithm that can encrypt and decrypt the data blocks along with 128 bit key length of 128 bits, 192 bits or 256 bits*

*Security is one of the main priorities in the technological era that demands wholeness privacy.The safety factor is not only needed by the military and government agencies, but also the business sector and individuals are always close relationship with the delivery and storage of data through the electronic media. Where it requires a process that is able to ensure the security and integrity of the contents of the data.To ensure the security and integrity of the data, we need a process of encoding. Encryption is done when the data is sent. This process will transform an original data into confidential data can not be read . Meanwhile, the decryption process is done to convert it back into the original data.*

*One solution is the Rijndael algorithm that is implemented in a Virtual Basic 6.0 application, which is not only to secure the word or phrase but also securing data in the form of digital images, audio, and video.*



**Keywords:** *AES , data security, encryption , decryption , data, Rijndael.*