PERANCANGAN DAN IMPLEMENTASI APLIKASI KRIPTOSISTEM FILE BERBASIS ANDROID MENGGUNAKAN ALGORITMA TWOFISH

SKRIPSI

disusun oleh

Ita Rahmatiah Mustamin

12.11.6568

PROGRAM SARJANA
PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016

PERSETUJUAN

SKRIPSI

PERANCANGAN DAN IMPLEMENTASI APLIKASI KRIPTOSISTEM FILE BERBASIS ANDROID MENGGUNAKAN ALGORITMA TWOFISH

yang dipersiapkan dan disusun oleh

Ita Rahmatiah Mustamin

12.11.6568

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 6 Oktober 2015

Dosen Pembimbing,

Dony Ariyus, M.Kom

NIK. 190302128

PENGESAHAN

SKRIPSI

PERANCANGAN DAN IMPLEMENTASI APLIKASI KRIPTOSISTEM FILE BERBASIS ANDROID MENGGUNAKAN ALGORITMA TWOFISH

yang dipersiapkan dan disusun oleh

Ita Rahmatiah Mustamin

12.11.6568

telah dipertahankan di depan Dewan Penguji
pada tanggal 23 Juni 2016

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Ahmad Dahlan, M.Kom **NIK. 190302174**	
Erni Seniwati, M.Cs **NIK. 190302231**	
Dony Ariyus, M.Kom **NIK. 190302128**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 1 Juli 2016

KETUA STMIK AMIKOM YOGYAKARTA

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

PERNYATAAN

Saya yang bertandatangan dibawah 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 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.

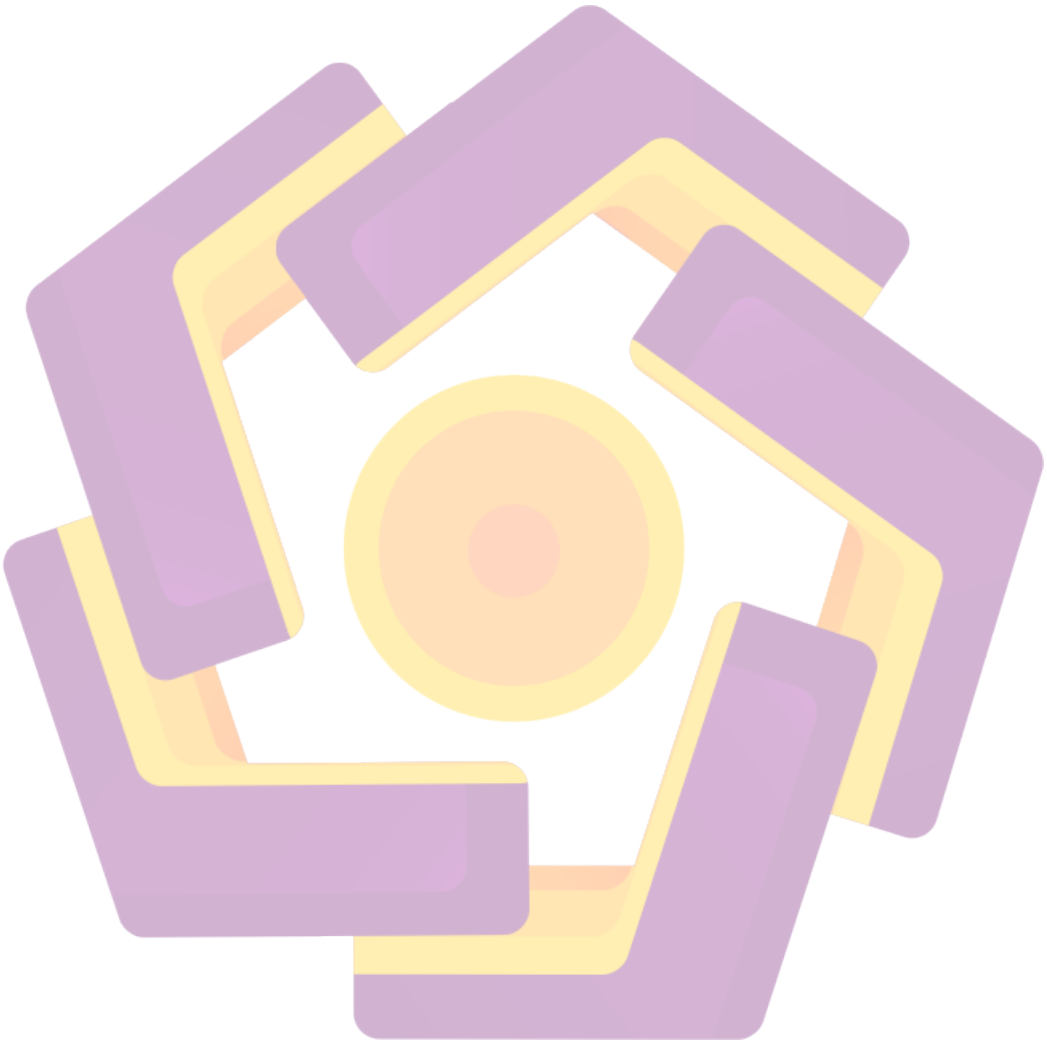
Yogyakarta, 1 Juli 2016

Ita Rahmatiah M

NIM. 12.11.6568

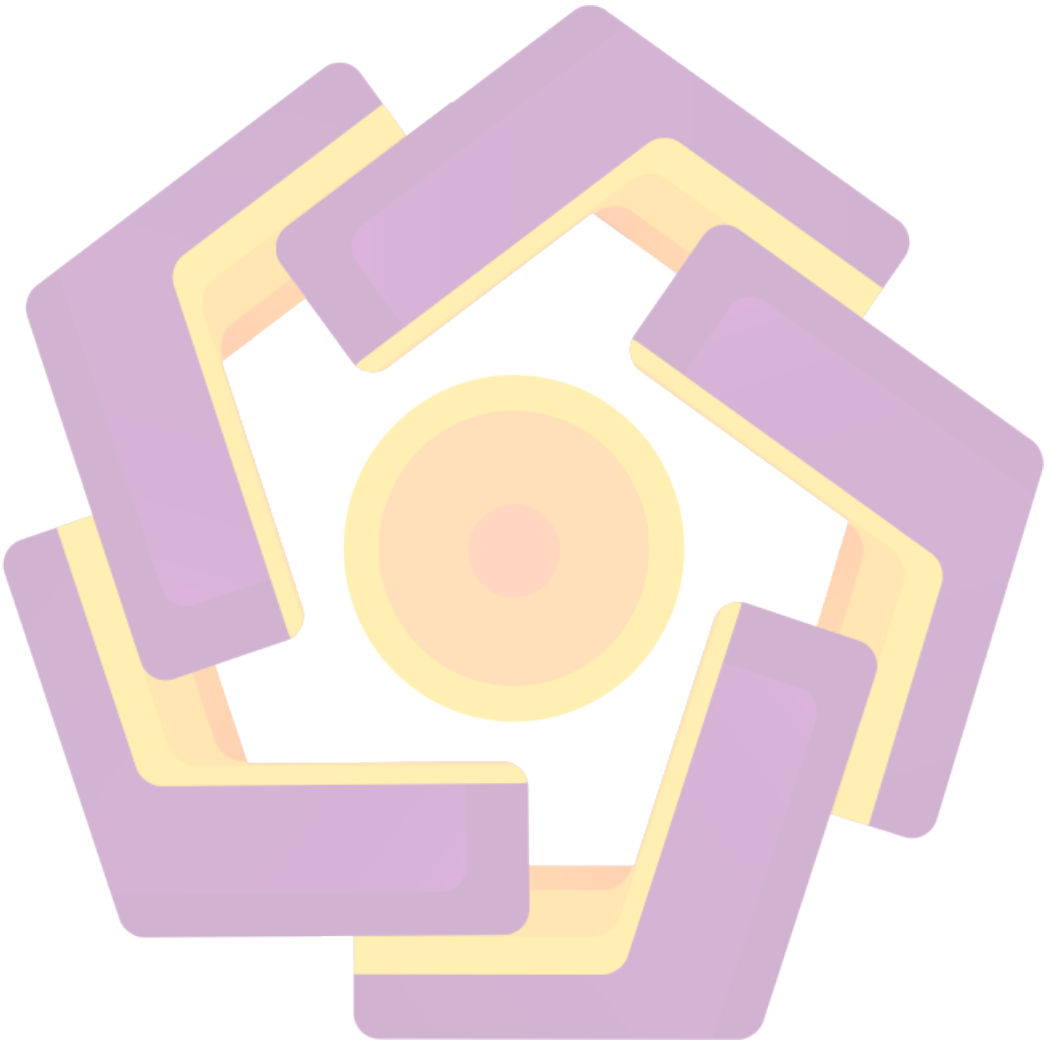
MOTTO

Keberuntungan adalah sesuatu yang terjadi ketika kesempatan bertemu dengan kesiapan, maka jika mau terus beruntung, selalu persiapkan yang terbaik karena kesempatan bisa datang kapan saja. ☺



PERSEMBAHAN

Skripsi ini saya persembahkan untuk kedua orang tuaku, kakak dan adik - adik ku (Syaiful, Yuyun, dan Fatma), para sahabat ku, teman- teman 12-S1TI-12, dan semua orang yang sedang menyusun skripsi tentang kriptografi.



KATA PENGANTAR

Puji Syukur saya panjatkan kehadirat Allah SWT atas segala rahmat dan karunia-Nya serta sholawat dan salam saya curahkan kepada junjungan Nabi Muhammad SAW, sehingga skripsi berjudul "Perancangan dan Implementai Aplikasi Kriptosistem File Menggunakan Algoritma Twofish" ini dapat terselesaikan.

Penyelesaian skripsi ini tidak lepas dari bantuan berbagai pihak, oleh karena itu saya ingin mengucapkan terimakasih kepada :

1. Bapak Prof. Dr. M. Suyanto, MM, selaku ketua STMIK Amikom Yogyakarta
2. Bapak Sudarmawan, MT, sebagai ketua jurusan STMIK Amikom Yohyakarta
3. Bapak Dony Ariyus, M.Kom, selaku dosen pembimbing saya, yang telah membimbing dan memberikan banyak saran sehingga skripsi ini dapat terselesaikan
4. Bapak dan Ibu saya yang selalu mendoakan dan memberikan motifasi kepada saya
5. Kakak dan adik-adik ku (ipul, yuyun, dan fatma), terimakasih atas suport moril dan materilnya.
6. Semua pihak yang telah membantu penulisan dalam menyelesaikan skripsi ini

Saya menyadari bahwa penyusunan skripsi ini jauh dari kata sempurna, oleh karena itu penulis mengharapkan saran maupun kritik yang membangun agar kedepannya menjadi lebih baik lagi. Semoga skripsi ini dapat bermanfaat bagi pembaca pada umumnya dan saya sendiri.

Yogyakarta, 29 Juni 2016

Ita Rahmatiah M

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Kemajuan teknologi saat ini dengan munculnya *smartphone* sangat menunjang keefektifan dan efisensi aktifitas sehari – hari bagi pengguna yang mempunyai mobilitas cukup tinggi. Salah satunya adalah android. Selain kemudahan dan dampak positif yang terjadi ternyata ada ancaman keamanan data yang bersifat rahasia, dan sangat dimungkinkan terjadinya *cyber crime* yang meliputi pencurian penipuan, pemerasan, kompetitif, sampai jatuhnya informasi ke pihak yang tidak berhak.

Cara mencegah permasalahan keamanan tersebut, diperlukan suatu metode keamanan data. Data atau informasi tidak hanya berupa data teks, tetapi juga dapat berupa data citra (image), data suara (audio), dan video. Metode yang sering digunakan adalah kriptografi. Kriptografi adalah salah satu kategori utama terhadap keamanan komputer yang dapat mengubah suatu informasi yang dapat dikenali menjadi informasi yang tidak dapat dimengerti. Teknik kriptosistem digunakan untuk penerapan metode kriptografi, yaitu menggunakan algoritma untuk mengambil kunci yang dapat melakukan *convert* pada *plaintext* menjadi *ciphertext* sehingga data tidak dapat dimengerti. Pemilihan algoritma twofish sebagai pembangun kriptosistem file karena algoritma ini mempunyai parameter – parameter yang sesuai standar AES untuk tingkat keamanan data yang tinggi di bidang kriptografi.

Hasil analisis masalah dan observasi terkait teori kriptografi dan algoritma twofish, dilakukan perancangan sautu aplikasi yang dapat berjalan di *smartphone* android dengan menerapkan metode kriptosystem file. Perancangan aplikasi dilakukan agar dapat menghasilkan aplikasi kriptografi berbasis android. Implementasi dan pengujian menunjukkan hasil bahwa aplikasi yang dibuat dapat berjalan sesuai tujuan dengan salah satu pencapaian yaitu penerapan enkripsi dan dekripsi pada file text (pdf dan doc), image (jpg dan png), audio (mp3), dan video (mp4 dan mkv).

Kata Kunci: smartphone, android, cyber crime, kriptografi, algoritma, kunci, convert, plaintext, ciphertext, enkripsi, dekripsi

ABSTRACT

Nowdays, technology advances by smartphones very support the effectiveness and efficiency daily activities for people who has many mobility. One of them is an android. In addition to ease and the positive impact that occurred but also there was a data security threat confidential impact, and it is possible to occurrence of cyber crime, such as theft, fraud, extortion, competitive, until the fall of information to unauthorized parties.

How to prevent the security issues, we need a method of data security. Data or information not only in text, but also image, voice, and video. The method often used is cryptography. Cryptography is one of the main categories to computer security that can transform an identifiable information into information that can not be understood. Cryptosystem used for the application of cryptographic methods, which uses an algorithm to retrieve the key that can convert the plaintext to ciphertext, so the data can not be understood. Selection algorithm Twofish as builders cryptosystem file because these algorithms have parameters that correspond AES standard for high data security level in cryptography.

The results of the analysis that problem and observations related to the theory of cryptography and Twofish algorithms, to designed an application which can run on android smartphone by applying the method kriptosystem file. Application design is done so that can generate cryptographic applications based on Android. Implementation and testing showed results that the application can be run in accordance with one achievement goal is the implementation of encryption and decryption on a text file (pdf and doc), image (jpg and png), audio (mp3) and video (mp4 and mkv).

Keywords : *smartphones, android, cyber crime, cryptography, algorithms, keys, convert, plaintext, ciphertext, encryption, decryption*