

**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**

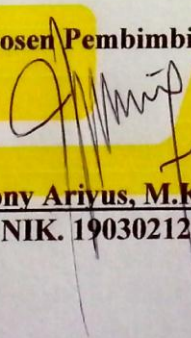
yang dipersiapkan dan disusun oleh

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

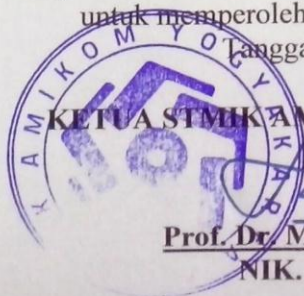
Tanda Tangan

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
pada 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, ... 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 Yogyakarta
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 motivasi 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

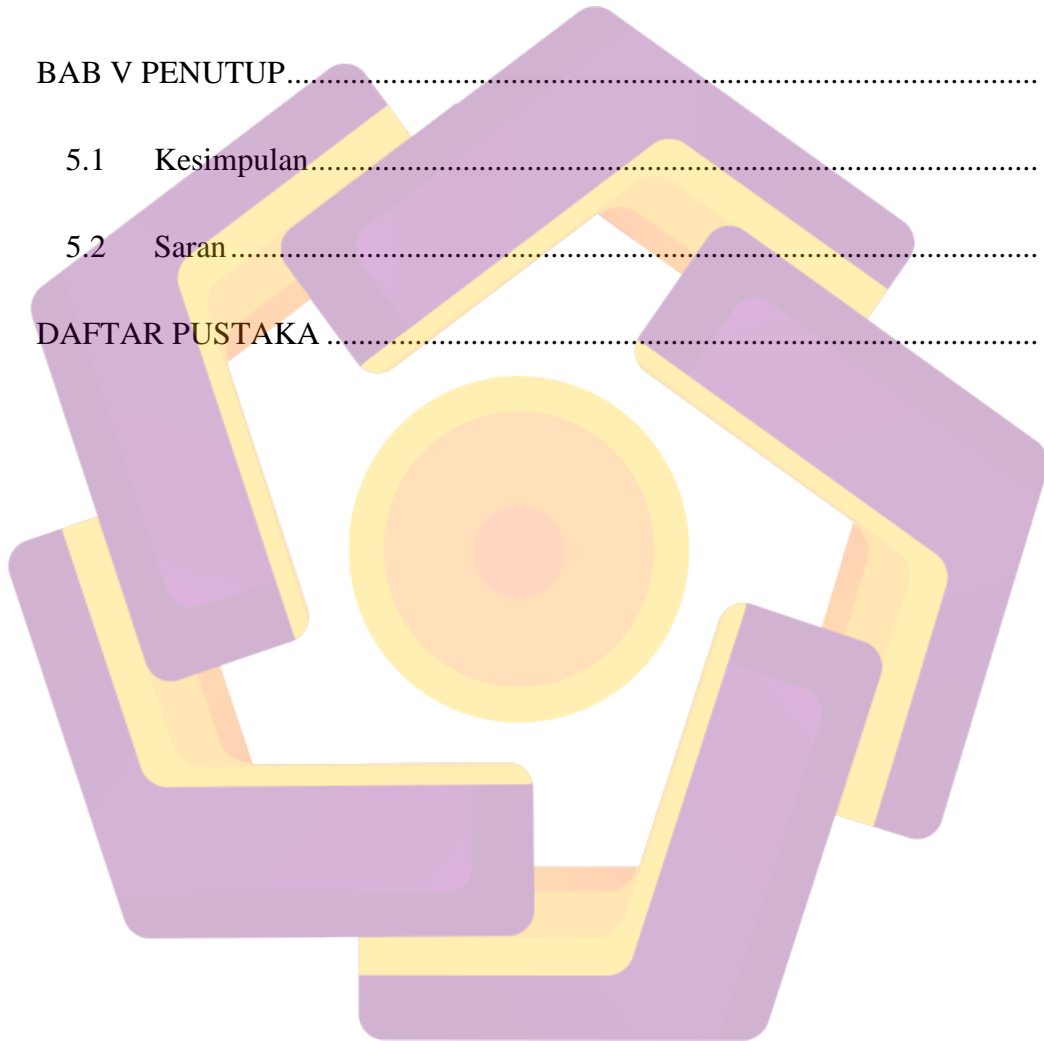
HALAMAN JUDUL.....	i
PERSETUJUAN.....	Error! Bookmark not defined.
PENGESAHAN.....	Error! Bookmark not defined.
PERNYATAAN.....	Error! Bookmark not defined.
MOTTO.....	v
PERSEMBAHAN.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR.....	xiv
INTISARI.....	xvii
ABSTRACT.....	xviii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah.....	3
1.4 Maksud dan Tujuan.....	3
1.5 Metode Penelitian.....	4

1.5.1	Metode Pengumpulan Data	4
1.5.2	Metode Analisis	4
1.5.3	Metode Perancangan	4
1.5.4	Metode Pengembangan	4
1.5.5	Metode Testing.....	5
1.6	Sistematika Penulisan.....	5
BAB II LANDASAN TEORI		7
2.1	Tinjauan Pustaka	7
2.2	Konsep Dasar Aplikasi	9
2.3	Konsep Dasar Sistem File	9
2.3.1	Konsep File	9
2.3.2	Sistem File.....	10
2.4	Konsep Dasar Kriptografi	13
2.4.1	Definisi Kriptografi.....	13
2.4.2	Komponen Kriptografi	13
2.4.3	Algoritma Kriptografi	15
2.5	Twofish.....	17
2.5.1	Unsur Pembangun Algoritma Twofish	17
2.5.2	Algoritma Twofish.....	19
2.5.3	Tujuan Desain Twofish	34

2.6	Android.....	34
2.6.1	Sejarah Android	34
2.6.2	Arsitektur Android	35
2.6.3	Aplikasi Android.....	38
2.7	UML (<i>Unified Modelling Language</i>).....	39
2.7.1	Pengenalan UML	39
2.7.2	Tujuan UML	39
2.7.3	Diagram dalam UML	40
2.8	Interface.....	45
2.9	Pengujian Perangkat Lunak.....	45
2.9.1	Konsep Pengujian Perangkat Lunak	45
2.9.2	Jenis – Jenis Pengujian Perangkat Lunak	46
BAB III ANALISIS DAN PERANCANGAN		48
3.1	GAMBARAN UMUM APLIKASI.....	48
3.2	ANALISIS SISTEM.....	48
3.2.1	Identifikasi Masalah	48
3.2.2	Analisis SWOT	49
3.2.3	Analisis Kebutuhan	50
3.2.4	Kebutuhan Sistem	50
3.2.4	Kebutuhan Sumber Daya Manusia.....	53

3.2.5	Analisis Kelayakan.....	53
3.3	PERANCANGAN SISTEM.....	54
3.3.1	Perancangan Proses Sistem.....	55
3.3.2	Perancangan Proses Enkripsi dan Dekripsi.....	64
3.4	PERANCANGAN INTERFACE.....	68
3.4.1	Rancangan Tampilan Menu.....	69
3.4.2	Rancangan Tampilan File Encryptor.....	69
3.4.3	Rancangan Tampilan Help.....	70
3.4.4	Rancangan Tampilan About.....	71
BAB IV IMPLEMENTASI DAN PEMBAHASAN.....		73
4.1	IMPLEMENTASI.....	73
4.1.1	Pembuatan Aset Aplikasi.....	73
4.1.2	Implementasi Listing Program.....	82
4.2	KOMPILASI PROGRAM (MEMBUAT APK).....	90
4.3	MANUAL INSTALASI.....	93
4.4	UJI COBA APLIKASI.....	97
4.4.1	<i>White Box Testing</i>	97
4.4.2	<i>Black Box Testing</i>	101
4.4.3	<i>Compability Testing</i>	103
4.4.4	Uji Coba Perangkat Lunak.....	104

4.4.5	Uji Coba dengan Menghapus Extensi .enc	113
4.5	PEMBAHASAN	116
4.5.1	Hubungan Lama Proses Encrypt/Decrypt dengan Kapasitas File.	116
4.5.2	Pemeliharaan Sistem	116
BAB V PENUTUP.....		117
5.1	Kesimpulan.....	117
5.2	Saran.....	117
DAFTAR PUSTAKA		118



DAFTAR TABEL

Tabel 2. 1 Tipe – Tipe File.....	11
Tabel 2. 2 Simbol Use Case Diagram	41
Tabel 2. 3 Simbol – Simbol Activity Diagram	43
Tabel 3. 1 Deskripsi Perancangan Class Diagram	63
Tabel 4. 1 Testing Menu Utama.....	101
Tabel 4. 2 Testing Menu Help.....	101
Tabel 4. 3 Testing Menu About	102
Tabel 4. 4 Testing Menu File Encryptor	102
Tabel 4. 5 Hasil Pengujian dengan Penghapusan extensi .enc.....	114
Tabel 4. 6 Uji Coba pada Berbagai Jenis Smartphone.....	104

DAFTAR GAMBAR

Gambar 2. 1 Blok Diagram Twofish.....	21
Gambar 2. 2 Gambar 2.2 Fungsi h	28
Gambar 2. 3 Satu Putaran Fungsi F (kunci 128-bit)	33
Gambar 2. 4 Versi Pengembangan Sistem Operasi Android	35
Gambar 2. 5 Arsitektur android	38
Gambar 3. 1 Use Case Diagram.....	55
Gambar 3. 2 Activity Diagram About.....	57
Gambar 3. 3 Activity Diagram Help	57
Gambar 3. 4 Activity Diagram Enkripsi	58
Gambar 3. 5 Activity Diagram Dekripsi	59
Gambar 3. 6 Sequence Diagram Menu Enkripsi.....	60
Gambar 3. 7 Sequence Diagram Menu Dekripsi	61
Gambar 3. 8 Sequence Diagram Menu Help	61
Gambar 3. 9 Sequence Diagram Menu About	62
Gambar 3. 10 Class Diagram	63
Gambar 3. 11 fungsi h (Schneier 1998:9)	65
Gambar 3. 12 Input Whitening (Schneier 1998:6).....	66
Gambar 3. 13 Fungsi F (Schneier 1998:6).....	67
Gambar 3. 14 Swap blok terakhir dan Output Whitening.....	68
Gambar 3. 15 Tampilan Interface Menu Utama	69
Gambar 3. 16 Tampilan Interface Menu File Encryptor.....	70
Gambar 3. 17 Tampilan Interface Menu Help	71

Gambar 3. 18 Tampilan Interface Menu About	72
Gambar 4. 1 Tampilan Menu utama	73
Gambar 4. 2 Kode xml form menu utama	74
Gambar 4. 3 Form Tampilan Menu Help.....	75
Gambar 4. 4 Kode xml form menu help	76
Gambar 4. 5 String.xml untuk Menu Help.....	77
Gambar 4. 6 Form Tampilan menu File Encryptor.....	77
Gambar 4. 7 Kode xml Form Menu File Encryptor.....	78
Gambar 4. 8 Form Tampilan Menu About.....	80
Gambar 4. 9 Kode xml Form Menu About.....	81
Gambar 4. 10 Class MainActivity.java	82
Gambar 4. 11 Class helpActivity.java.....	83
Gambar 4. 12 Class FileEncActivity.java Bagian 1.....	84
Gambar 4. 13 Class FileEncActivity.java Bagian 2.....	85
Gambar 4. 14 Gambar Class AboutActivity.java	86
Gambar 4. 15 Class CryptActivity.java	87
Gambar 4. 16 TwofishEngine.java Bagian 1	88
Gambar 4. 17 TwofishEngine.java Bagian 2	89
Gambar 4. 18 Membuat Keystore baru	90
Gambar 4. 19 Generate Signed APK	91
Gambar 4. 20 Release APK	91
Gambar 4. 21 Notifikasi Generate APK Telah Selesai	92
Gambar 4. 22 Hasil APK yang Dibuat.....	92

Gambar 4. 23 Set Ulang Nama APK	93
Gambar 4. 24 Tampilan Konfirmasi Install	94
Gambar 4. 25 Tampilan Loading Proses Instalasi	95
Gambar 4. 26 Tampilan Konfirmasi Aplikasi Sukses Diinstall.....	96
Gambar 4. 27 Script Pengujian Panjang Kunci.....	97
Gambar 4. 28 Paddings	98
Gambar 4. 29 Padding Key kurang dari 64 bit.....	99
Gambar 4. 30 Padding Key Lebih dari 256 bit	99
Gambar 4. 31 Script Pengujian Panjang Byte Plaintext.....	100
Gambar 4. 32 Uji Coba Enkripsi ekstensi file.doc	106
Gambar 4. 33 File Hasil Enkripsi ekstensi .docx.....	107
Gambar 4. 34 File Hasil Enkripsi Tidak dapat di Buka	108
Gambar 4. 35 Proses Dekripsi ALL 1.0.docx.enc.....	109
Gambar 4. 36 Proses Enkripsi dan Dekripsi file ekstensi .pdf	110
Gambar 4. 37 Proses Enkripsi dan Dekripsi file ekstensi .jpg.....	110
Gambar 4. 38 Proses Enkripsi dan Dekripsi file ekstensi .png.....	111
Gambar 4. 39 Proses Enkripsi dan Dekripsi file ekstensi .mp3.....	111
Gambar 4. 40 Proses Enkripsi dan Dekripsi file ekstensi .mp4.....	112
Gambar 4. 41 Proses Enkripsi dan Dekripsi file ekstensi .mkv.....	113

INTISARI

Kemajuan teknologi saat ini dengan munculnya *smartphone* sangat menunjang keefektifan dan efisiensi 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 suatu 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