

**APLIKASI MOBILE KEAMANAN BERBAGI FILE
MENGUNAKAN KOMBINASI ALGORITMA
AES, RSA DAN RC6**

SKRIPSI



disusun oleh

Eric Triawan

12.11.6422

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

**APLIKASI MOBILE KEAMANAN BERBAGI FILE
MENGUNAKAN KOMBINASI ALGORITMA
AES, RSA DAN RC6**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan teknik informatika



disusun oleh

Eric Triawan

12.11.6422

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

PERSETUJUAN

SKRIPSI

**APLIKASI MOBILE KEAMANAN BERBAGI FILE
MENGUNAKAN KOMBINASI ALGORITMA
AES, RSA DAN RC6**

Yang dipersiapkan dan disusun oleh

Eric Triawan

12.11.6422

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 27 Maret 2015

Dosen Pembimbing,



Kusnawi, S.Kom, M.Eng

NIK.190302112

PENGESAHAN
SKRIPSI
APLIKASI MOBILE KEAMANAN BERBAGI FILE
MENGGUNAKAN KOMBINASI ALGORITMA
AES, RSA DAN RC6

Yang disusun oleh

Eric Triawan

12.11.6422

Telah dipertahankan di depan dewan Penguji
Pada tanggal 3 September 2015

Susunan Dewan Penguji

Nama Penguji

Kusnawi, S.Kom, M.Eng

NIK. 190302112

Hastari Utama, M.Cs

NIK. 190302230

Windha Mega Pradnya D, M.Kom

NIK. 190302185

Tanda Tangan

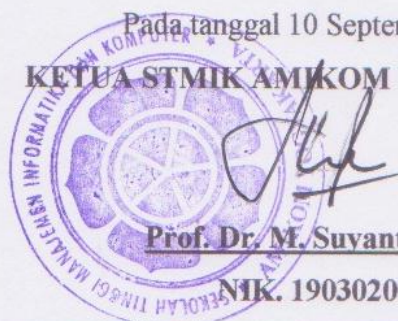


Skripsi ini telah diterima sebagai salah satu persyaratan

Untuk memperoleh gelar Sarjana Komputer

Pada tanggal 10 September 2015

KETUA STM IK AMIKOM YOGYAKARTA



Prof. Dr. M. Suvanto, M.M

NIK. 190302001

PERNYATAAN KEASLIAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa, skripsi ini merupakan hasil karya sendiri, bukan merupakan pengambil alihan tulisan atau karya orang lain untuk memperoleh gelar Akademis di suatu institusi pendidikan tinggi manapn, dan sepanjang pengetahuan saya tidak terdapat karya yang sama dan diterbitkan oleh orang lain, kecuali yang secara tertulis diacu sebagai sumber refrensi dalam naskah ini disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

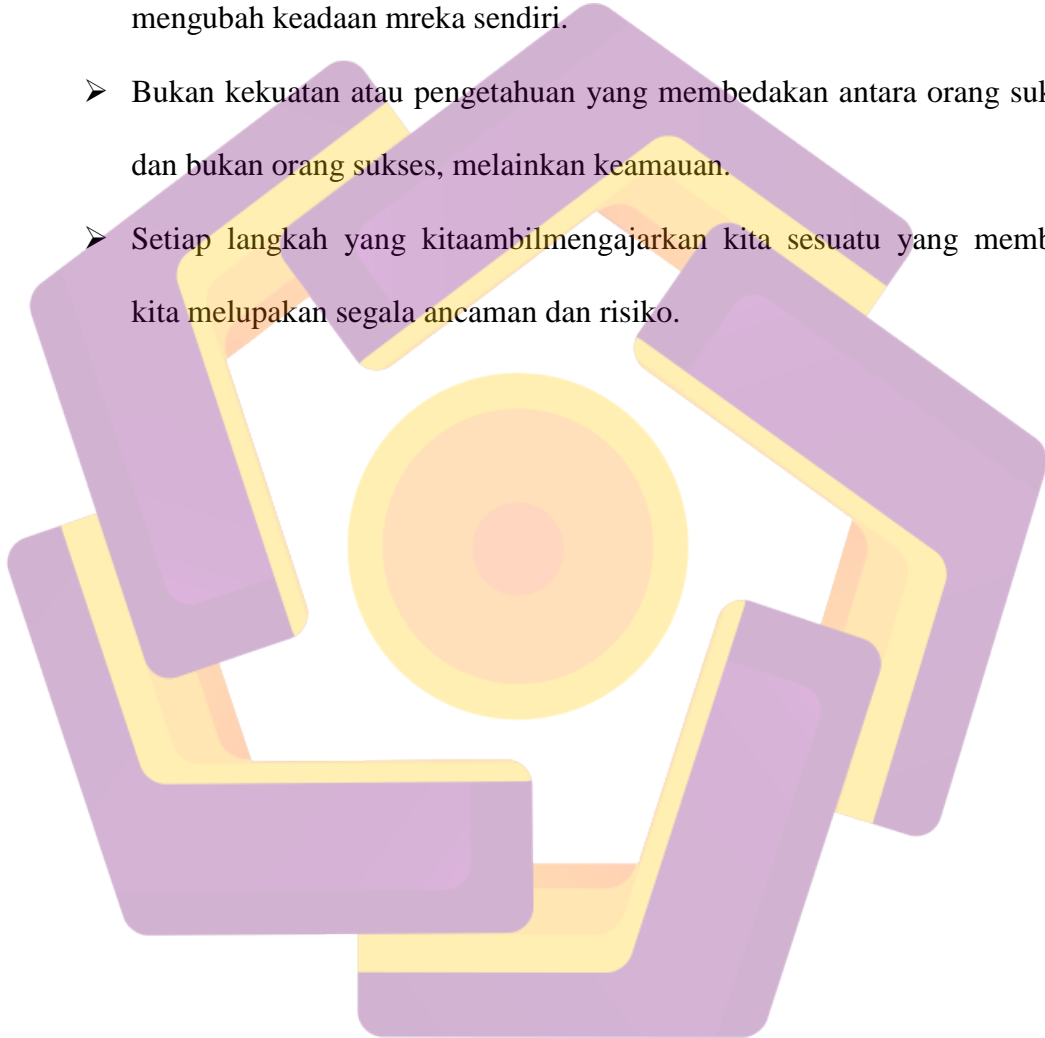
Yogyakarta, 10 September 2015

Eric Triawan

12.11.6422

MOTTO

- Menang bukanlah segalanya. Tetapi, keamuan untuk menang adalah segalanya.
- Allah tidak akan mengubah keadaan suatu kaum sehingga mereka mau mengubah keadaan mreka sendiri.
- Bukan kekuatan atau pengetahuan yang membedakan antara orang sukses dan bukan orang sukses, melainkan keamauan.
- Setiap langkah yang kitaambil mengajarkan kita sesuatu yang membuat kita melupakan segala ancaman dan risiko.



PERSEMBAHAN

Alhamdulillah Puji Syukur ini penulis panjatkan, akhirnya skripsi ini dapat terselsaikan dengan baik. Karya ini merupakan wujud dari kegigihan dalam ikhtiar untuk sebuah makna kesempurnaan dengan tanpa berharap melampaui kemaha sempurna sang maha sempurna. Selaku penulis mempersembahkan skripsi ini kepada :

1. Allah SWT atas ridho-Nya skripsi ini dapat terselesaikan dengan baik, Sujud syukur aku panjatkan kepada-Mu dan jadikanlah hamba-Mu yang pandai bersyukur dan selalu dalam lindungan-Mu.
2. Shalawat serta salam senantiasa tercurah kepada Nabi Muhammad SAW. Sebagai sang pencerah untuk menyempurnakan akhlak manusia di muka bumi ini.
3. Untuk yang tercinta yaitu kedua orangtuaku. Yang selalu memanjatkan doa kepada putra Mu tercinta dalam setiap sujudnya, memberi semangat, mengarahkanku untuk menjadi lebih baik.
4. Keluargaku dan kakak-kakakku yang telah menjadi contoh yang baik, *mensupport*, dan mendo'akan setiap langkahku.
5. Untuk teman-teman seangkatan saat kuliah dan teman-teman kost yang menjadi keluarga keduaku.

KATA PENGANTAR

Bismillahirrohmannirrokhim, puji syukur penulis haturkan kehadiran Allah SWT, atas limpahan rahmat-Nya sehingga penulisan skripsi *Aplikasi Mobile Keamanan Berbagi File Menggunakan Kombinasi Algoritma AES, RSA Dan RC6* dapat terselesaikan.

Penulisan skripsi ini diajukan untuk memenuhi salah satu syarat kelulusan dalam jenjang perkuliahan Strata 1 STMIK AMIKOM Yogyakarta, Penulis menyadari bahwa dalam penulisan laporan skripsi ini tidak lepas dari hambatan dan kesulitan, namun berkat dukungan, dorongan, kerjasama maupun bimbingan dari berbagai pihak. Untuk itu penulis mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, MM, selaku Ketua STMIK “AMIKOM” Yogyakarta.
2. Bapak Kusnawi, S.Kom, M.Eng, selaku Dosen Pembimbing yang telah membantu dalam pembuatan skripsi ini.
3. Segenap Staf Pengajar di STMIK “AMIKOM” Yogyakarta yang telah member ilmu dan pemahaman tentang dunia informatika.
4. Kedua orang tua, serta semua keluarga yang selalu memberikan dukungan dan semangat dalam menjalani kuliah dan menyelesaikan skripsi.
5. Teman – teman serta Sahabat yang telah banyak membantu dalam penyelesaian skripsi ini.

Disadari bahwa dalam penyusunan laporan skripsi ini masih jauh dari sempurna. Oleh karena itu kritik maupun saran yang bersifat membantu atau membangun sangat diharapkan.

Akhir kata, semoga penyusunan skripsi ini ada manfaatnya, khususnya bagi penulisan dan umumnya bagi kita semua dalam rangka menambah wawasan pengetahuan dan pemikiran kita.

Yogyakarta, 10 September 2015

Penulis,

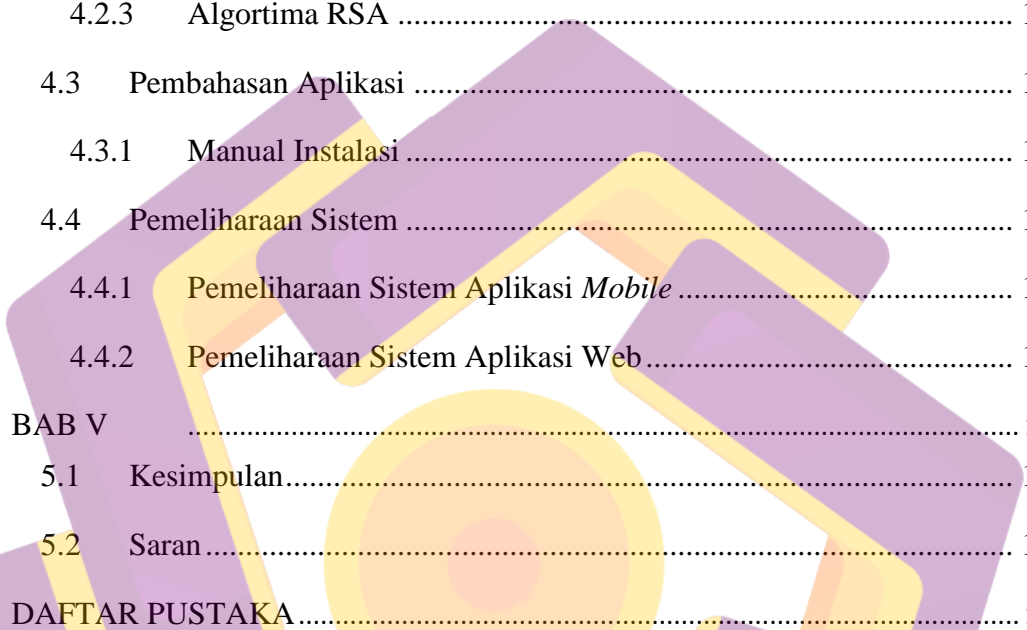
Eric Triawan

DAFTAR ISI

JUDUL	i
PERSETUJUAN	ii
PENGESAHAN	Error! Bookmark not defined.
PERNYATAAN KEASLIAN	iv
MOTTO	v
PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR GAMBAR	xiii
DAFTAR TABEL	xvi
INTISARI	xvii
<i>ABSTRACT</i>	xviii
BAB I	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Maksud dan Tujuan Penelitian	4
1.4.1 Maksud Penelitian	4
1.4.2 Tujuan Penelitian	4
1.5 Metode Penelitian	4
1.5.1 Teknik Pengumpulan Data	4
1.5.2 Metode Analisis	5
1.5.3 Metode Perancangan	5
1.5.4 Metode Pengembangan	6
1.5.5 Metode Pengujian Unit	6
1.5.6 Metode Implementasi	6

1.6	Sistematika Penulisan.....	6
BAB II	9
2.1	Tinjauan Pustaka	9
2.2	Program dan Aplikasi	10
2.2.1	Pengertian Program.....	10
2.2.2	Pengertian Aplikasi	10
2.2.3	Pengertian Aplikasi Mobile.....	11
2.3	Android.....	11
2.3.1	Perkembangan Android API.....	11
2.3.2	Komponen Android.....	12
2.4	Jaringan	13
2.4.1	Jaringan Client Server.....	14
2.4.2	Jaringan Peer to Peer.....	14
2.5	Android Studio IDE (Integrated Development Environment).....	14
2.6	Pengertian Java.....	15
2.6.1	Perkembangan Java API	16
2.6.2	Pemrograman dengan Java.....	17
2.7	Kriptografi.....	17
2.7.1	Sejarah Kriptografi.....	17
2.7.2	Tujuan Kriptografi	19
2.7.3	Algoritma Simetri dan Asimetri.....	20
2.7.4	AES	21
2.7.5	RSA.....	23
2.7.6	RC6.....	26
2.8	Basis Data.....	29

2.8.1	Konsep Basis Data	29
2.8.2	Pemodelan Basis Data.....	30
2.8.3	Definisi SQL	32
2.9	Metodologi Pengembangan Sistem	32
2.10	UML (Unified Modeling Language).....	35
2.11	ERD (Entitiy Relationship Diagram)	39
BAB III	41
3.1	Gambaran Aplikasi.....	41
3.2	Analisis.....	43
3.2.1	Analisis SWOT	43
3.2.2	Analisis Kebutuhan.....	45
3.3	Kelayakan Sistem.....	48
3.3.1	Kelayakan Teknis.....	48
3.3.2	Kelayakan Hukum.....	48
3.4	Perancangan.....	49
3.4.1	Algoritma	49
3.4.2	Perancangan Sistem	58
3.4.3	Activity Diagram.....	59
3.4.4	Class Diagram.....	72
3.4.5	Squence Diagram	74
BAB IV	96
4.1	Implementasi	96
4.1.1	Implemntasi Database	96
4.1.2	Impemntasi Algoritma	98
4.1.3	Implementasi <i>Interface</i>	111



4.1.4	Uji Coba Sitem dan Program	132
4.2	Pembahasan	135
4.2.1	Algortima AES.....	135
4.2.2	Algortima RC6.....	137
4.2.3	Algortima RSA	137
4.3	Pembahasan Aplikasi	137
4.3.1	Manual Instalasi	137
4.4	Pemeliharaan Sistem	140
4.4.1	Pemeliharaan Sistem Aplikasi <i>Mobile</i>	141
4.4.2	Pemeliharaan Sistem Aplikasi Web.....	141
BAB V	143
5.1	Kesimpulan.....	143
5.2	Saran.....	143
DAFTAR PUSTAKA	145

DAFTAR GAMBAR

Gambar 2. 1 SDLC	33
Gambar 3. 1 Diagram Enkripsi AES	51
Gambar 3. 2 Diagram Dekripsi AES	53
Gambar 3. 3 Block Diagram Algoritma Enkripsi Kriptografi RC6	55
Gambar 3. 4 Block Diagram Algoritma Deskripsi Kriptografi RC6.....	58
Gambar 3. 5 Use Case Diagram Sharing Secure	58
Gambar 3. 6 Activity Diagram Sign In	59
Gambar 3. 7 Activity Diagram Sign Up.....	60
Gambar 3. 8 Activity Diagram Share File.....	61
Gambar 3. 9 Activity Diagram Send Private Message.....	62
Gambar 3. 10 Activity Diagram Encrypt Key	63
Gambar 3. 11 Activity Diagram Files Received.....	64
Gambar 3. 12 Activity Diagram Decrypt File	65
Gambar 3. 13 Activity Diagram Decrypt Message	66
Gambar 3. 14 Activity Diagram Decrypt Key.....	67
Gambar 3. 15 Activity Diagram Contact.....	68
Gambar 3. 16 Activity Diagram Add Contact.....	69
Gambar 3. 17 Activity Diagram Account.....	70
Gambar 3. 18 Activity Diagram About	71
Gambar 3. 19 Class Diagram.....	73
Gambar 3. 20 Sequence Diagram Login	74
Gambar 3. 21 Sequence Diagram Sign Up.....	75
Gambar 3. 22 Sequence Diagram Send	76
Gambar 3. 23 Relasi Tabel Database	78
Gambar 3. 24 Gambar Diagram ERD	77
Gambar 3. 25 Tampilan Splash Screen	80
Gambar 3. 26 Tampilan Front Menu	81

Gambar 3. 27 Tampilan Sign In	82
Gambar 3. 28 Tampilan Sign Up.....	83
Gambar 3. 29 Tampilan Encrypt Key.....	84
Gambar 3. 30 Tampilan Private Message.....	85
Gambar 3. 31 Tampilan Share File.....	86
Gambar 3. 32 Tampilan File Received.....	87
Gambar 3. 33 Tampilan Contact.....	88
Gambar 3. 34 Tampilan Tab Decryption.....	89
Gambar 3. 35 Tampilan Tab Encryption.....	90
Gambar 3. 36 Tampilan Decryp File.....	91
Gambar 3. 37 Tampilan Home Website.....	92
Gambar 3. 38 Tampilan Website Panel Login Admin.....	93
Gambar 3. 39 Tampilan Website Panel Home Admin.....	94
Gambar 3. 40 Tampilan Website Member.....	95
Gambar 4. 1 Tabel User.....	96
Gambar 4. 2 Tabel Admin.....	96
Gambar 4. 3 Tabel Contact.....	97
Gambar 4. 4 Tabel Pesan.....	97
Gambar 4. 5 Tabel Upload File.....	97
Gambar 4. 6 Tabel Andoid GCM Device.....	97
Gambar 4. 7 Tampilan Splash Screen.....	112
Gambar 4. 8 Tampilan Fornt Menu.....	113
Gambar 4. 9 Tampilan Form Sign In.....	114
Gambar 4. 10 Tampilan Form Sign Up.....	115
Gambar 4. 11 Tampilan Tab Encryption.....	116
Gambar 4. 12 Tampilan Share File.....	117
Gambar 4. 13 Tampilan Private Message.....	118
Gambar 4. 14 Tampilan Encrypt Key.....	119
Gambar 4. 15 Tampilan Tab Decryption.....	120

Gambar 4. 16 Tampilan File Received.....	121
Gambar 4. 17 Tampilan Decrypt File.....	122
Gambar 4. 18 Tampilan Decrypt Message.....	123
Gambar 4. 19 Tampilan Decrypt Key.....	124
Gambar 4. 20 Tampilan Tab Contact.....	125
Gambar 4. 21 Tampilan Chat Messenger.....	126
Gambar 4. 22 Tampilan Add Contact.....	127
Gambar 4. 23 Tampilan Account.....	128
Gambar 4. 24 Tampilan About.....	129
Gambar 4. 25 Tampilan Website User.....	130
Gambar 4. 26 Tampilan Website Panel Login Admin.....	130
Gambar 4. 27 Tampilan Website Home Panel Admin.....	131
Gambar 4. 28 Tampilan Website Member Panle Admin.....	132
Gambar 4. 29 Log Cat.....	135
Gambar 4. 30 Uji Prosepe Enkripsi dan Dekripsi File.....	136
Gambar 4. 31 Manual Instalsi 1.....	138
Gambar 4. 32 Manual Instalasi 2.....	139
Gambar 4. 33 Manual Instalasi 3.....	140

DAFTAR TABEL

Tabel 2. 1 Parameter AES	22
Tabel 2. 2 Use Case	36
Tabel 3. 1 SWOT.....	45
Tabel 3. 2 Spesifikasi Notebook.....	46
Tabel 3. 3 Spesifikasi Smartphone Android.....	47
Tabel 3. 4 Perangkat Lunak Komputer.....	47
Tabel 3. 5 Perangkat Lunak Smartphone Android.....	48
Tabel 3. 6 Rancang Tabel User	78
Tabel 3. 7 Rancang Tabel Contact	79
Tabel 3. 8 Rancang Tabel Pesan.....	79
Tabel 3. 9 Rancang Tabel Admin.....	79
Tabel 4. 1 Black Box Testing	133
Tabel 4. 2 Uji Instalsi	134
Tabel 4. 3 Uji Enkripsi dan Dekripsi File.....	136

INTISARI

Berbagi file antar *smartphone* sekarang ini masih sebatas pengiriman dan penerimaan file saja, tanpa adanya keamanan yang mumpuni sehingga data yang terkirim tidak akan terjaga kerahasiaannya. Aplikasi *mobile* yang dapat berbagi file dan dapat menjaga kerahasiaan file tersebut sangatlah di butuhkan sekarang ini dikarenakan semakin intensnya penggunaan perangkat *smartphone* daripada komputer *desktop*.

Berbagi file antar perangkat *smartphone* secara umum dilakukan menggunakan media *transfer* bluetooth yang mudah, dengan media bluetooth antar perangkat tinggal mengaktifkan bluetooth masing-masing. Namun hal ini dapat disusupi oleh pihak yang tidak berhak atas akses tersebut dan masuk dalam area konektivitas bluetooth untuk menyadap file hasil transfer antar perangkat tersebut.

Dengan demikian aplikasi *mobile* dengan fungsi pengamanan file sangatlah dibutuhkan untuk menunjang mobilitas pengguna *smartphone*, untuk itu akan di rancang sebuah aplikasi *mobile* yang akan memberikan keamanan pada file yang akan di dibagikan kepada pihak lain antar pengguna *smartphone* agar dapat menjaga kerahasiaan file tersebut.

Kata Kunci : Kriptografi, Keamanan, Berbagi File.

ABSTRACT

Sharing files between smartphones today is still limited to sending and receiving files only, in the absence of qualified security so that data sent will not be kept confidential. Mobile applications that can share files and be able to maintain the confidentiality of the file is needed now because of increasingly intense use of smartphones than desktop computers.

Sharing files between smartphones is generally performed using a simple bluetooth transfer media, with the media between devices bluetooth stay bluetooth activate respectively. But this can be compromised by a person not entitled to such access and bluetooth connectivity into the area to tap the file transfer between devices.

Thus mobile applications with file security functions is needed to support the mobility of users of smartphones, for that will be designed a mobile application that will provide security to the file that will be distributed to other parties among smartphone users in order to maintain the confidentiality of the file.

Keyword: *Cryptography, Security, Sharing File.*

