

**PERANCANGAN APLIKASI KRIPTOGRAFI RC4 DAN RSA SEBAGAI
MEDIA BELAJAR KRIPTOGRAFI BERBASIS ANDROID**

SKRIPSI



disusun oleh

Muhammad Qoyim Yusuf

11.11.5406

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016**

**PERANCANGAN APLIKASI KRIPTOGRAFI RC4 DAN RSA SEBAGAI
MEDIA BELAJAR KRIPTOGRAFI BERBASIS ANDROID**

SKRIPSI

untuk memenuhi sebagai persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



disusun oleh

Muhammad Qoyim Yusuf

11.11.5406

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016**

PERSETUJUAN

SKRIPSI

**PERANCANGAN APLIKASI KRIPTOGRAFI RC4 DAN RSA SEBAGAI
MEDIA BELAJAR KRIPTOGRAFI BERBASIS ANDROID**

yang dipersiapkan dan disusun oleh

Muhammad Qoyim Yusuf

11.11.5406

yang disetujui oleh Dosen Pembimbing Skripsi
pada Tanggal 1 Desember 2015

Dosen Pembimbing,



Bayu Setiaji, M. Kom

NIK. 190302216

PENGESAHAN

SKRIPSI

**PERANCANGAN APLIKASI KRIPTOGRAFI RC4 DAN RSA SEBAGAI
MEDIA BELAJAR KRIPTOGRAFI BERBASIS ANDROID**

yang disusun oleh

Muhammad Qoyim Yusuf

11.11.5406

telah dipertahankan di depan Dewan Penguji
pada tanggal 11 Mei 2016

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Yuli Astuti, M.Kom
NIK. 190302146



Ahlihi Masruro, M.Kom
NIK. 190302148



Bayu Setiaji, M. Kom
NIK. 190302216



Skripsi ini telah diterima sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 20 Mei 2016

KETUA SEMIK AMKOM YOGYAKARTA



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

PERNYATAAN

Saya yang bertandatangan di bawah 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, 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 tanggung jawab saya pribadi

Yogyakarta, 16 Mei 2016



Muhammad Qoyim Yusuf
NIM 11.11.5406

MOTTO

- ✓ Mulailah sesuatu dengan membaca "Bismillahirrahmanirrahim" dan diakhiri dengan "Alhamdulillahirobbil 'alamin" agar sesuatu yang kita kerjakan di ridhoi Allah SWT.
- ✓ Selama tekat yang kuat terbungkus semangat, maka akan mampu menerjang badai sekalipun (Diah Ayu Widyawati)
- ✓ Kerjakan apa yang bisa dikerjakan, jangan menunda-nunda hingga waktu hampir habis.
- ✓ Tiada kata udzur dalam berjuang, (KH. Abd. Wahab Hasbulloh)
- ✓ Jangan lihat masa lampau dengan penyesalan, jangan pula lihat masa depan dengan ketakutan, tapi lihatlah sekitar anda dengan penuh kesadaran.
- ✓ Siapa yang melanggar peraturan dianggap sebagai sampah. Namun, siapa yang meninggalkan teman lebih buruk dari sampah. (Uchiha Obito)
- ✓ Kecanduan game lebih baik dari pada kecanduan minum-minuman keras dan narkoba.

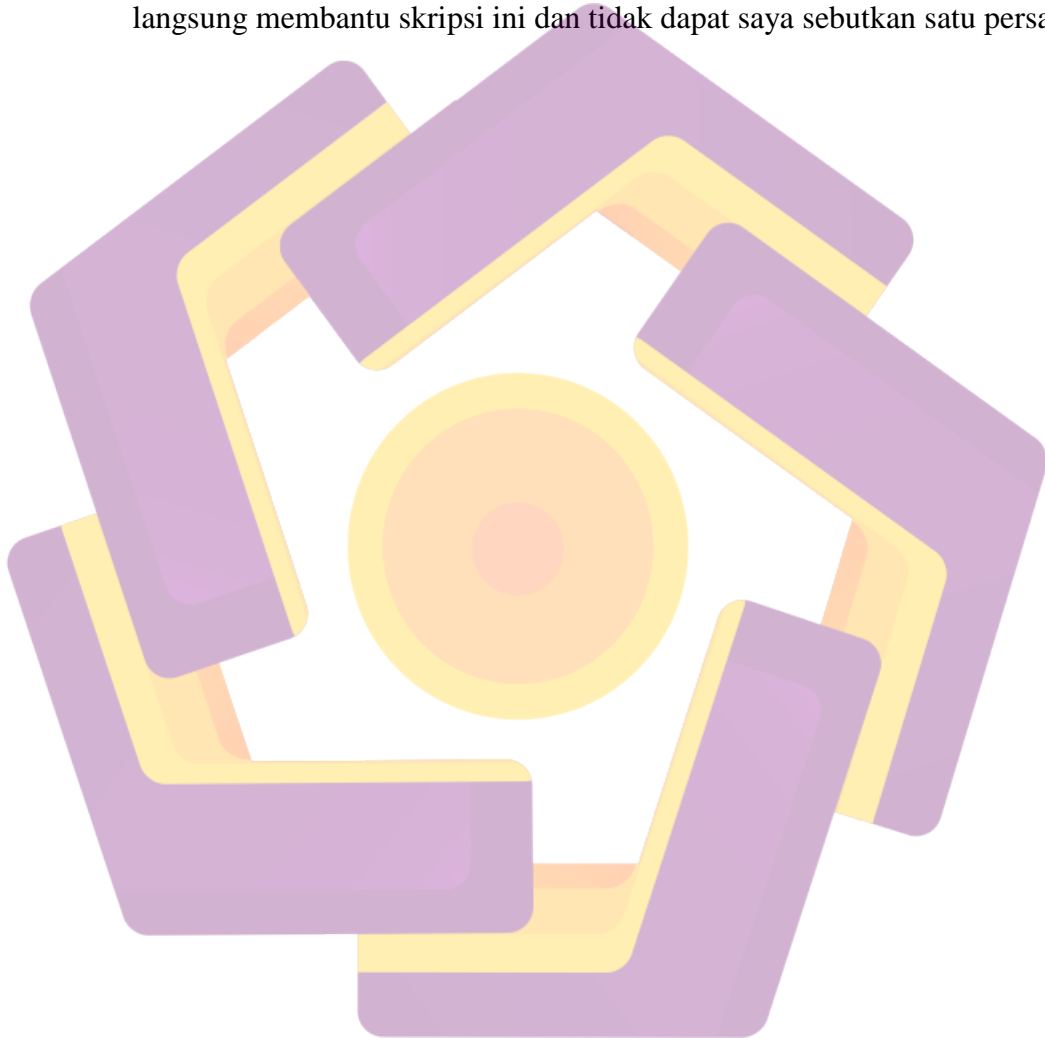
PERSEMBAHAN

Puji syukur senantiasa terucap kehadirat Alloh SWT, yang telah melimpahkan nikmat yang luar biasa kepada setiap hamba-Nya. Shalawat serta salam selalu tercurah kepada Nabi Muhammad SAW.

Skripsi ini saya persembahkan kepada pihak-pihak yang telah memberikan dukungan. Skripsi ini di dedikasikan untuk :

1. Kedua Orang Tua, Mas, Mbak dan anak-anaknya, semua keluarga besar baik dari bapak maupun ibu, yang telah memberikan dukungan baik moril maupun materiil. Untuk doa dan perhatian serta kesabarannya membimbing dan mengajarkan segala hal.
2. Bapak Bayu Setiaji, M.Kom sebagai dosen pembimbing yang memberikan arahan dan bimbingannya selama pengerjaan skripsi ini.
3. Mas Kokok, S.Kom dan mas Yusron, S.Kom yang membagikan *Source Code* yang sangat membantu dalam penyelesaian skripsi ini.
4. Dosen - dosen STMIK AMIKOM Yogyakarta yang telah mengampu selama perkuliahan.
5. Kekasihku (Diah Ayu W) yang telah memberikan dukungan sepenuh hati, doa, nasihat dan motivasi selama pembuatan skripsi ini.
6. Teman - teman 11-S1TI-11, yang telah menemaniku selama kuliah di STMIK AMIKOM Yogyakarta
7. Teman – Teman Farming Wafa, Abdul, Angga & Istri, Adin, Ruli, Elik, S.Kom, Nisa, Pak Huda, S.kom, Irma, Upik, Wanti, Fajrul, terima kasih telah mensupport, menghibur dan menemani selama ini.

8. Teman - teman Dota 2 Rochman, S.kom, Bang Bur, S.kom, M.Eng, Dwi, S.kom, Riko, Syn`z, dkk terima kasih telah mendukung, menghibur dan menemani saat party.
9. Terima kasih pula kepada pihak-pihak yang entah di mana yang secara tidak langsung membantu skripsi ini dan tidak dapat saya sebutkan satu persatu.



KATA PENGANTAR

Assalamu'alaikum Warahmatullah Wabarakatuh

Alhamdulillah, Puji syukur kehadiran Allah *Subhanahu wa ta'ala* yang telah melimpahkan rahmat, taufik, hidayah dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan skripsi ini yang diberi judul ” **PERANCANGAN APLIKASI KRIPTOGRAFI RC4 DAN RSA SEBAGAI MEDIA BELAJAR KRIPTOGRAFI BERBASIS ANDROID.**”

Penyusunan laporan ini dimaksudkan sebagai syarat untuk memperoleh derajat Sarjana S1 pada Jurusan Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer ”AMIKOM” Yogyakarta.

Proses penyusunan hingga selesainya skripsi ini tidak terlepas dari bantuan dan bimbingan dari berbagai pihak secara langsung maupun tidak langsung telah memberikan motivasi kepada penulis. Maka dari itu, sebagai rasa hormat penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Orang tua dan keluarga besar atas doa dan dukungannya selama ini.
2. Bapak Prof. Dr. H. M. Suyanto, MM sebagai Ketua Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
3. Bapak Sudarmawan, MT selaku Ketua Jurusan Teknik Informatika STMIK Amikom Yogyakarta.
4. Bapak Bayu Setiaji, M.Kom selaku dosen pembimbing yang telah memberika masukan, arahan, dan motivasi kepada penulis.
5. Segenap staff dan dosen STMIK Amikom Yogyakarta yang telah sharing dan memberikan ilmunya selama kuliah.

6. Semua pihak yang telah membantu kelancaran penyusunan skripsi yang tidak dapat penulis tulis satu per satu.

Penulis menyadari masih ada kekurangan dari penyusunan laporan skripsi ini. Kritik dan saran yang bersifat membangun selalu penulis harapkan demi kemajuan dan arah lebih baik di masa yang akan datang sehingga dapat bermanfaat bagi penulis serta pihak-pihak yang membutuhkan.

Akhirnya dengan doa kepada Allah *Subhanahu Wa Ta'ala* semoga laporan skripsi ini bermanfaat bagi semua pihak.

Wassalamu'alaikum Warahmatullah Wabarakatuh.

Yogyakarta, 11 Mei 2016

Penyusun

DAFTAR ISI

JUDUL.....	i
PERSETUJUAN	ii
PENGESAHAN	iii
PERNYATAAN	iv
MOTTO	v
PERSEMBAHAN.....	vi
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
INTISARI	xvi
ABSTRACT.....	xvii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Metode Penelitian.....	3
1.7 Sistematika Penulisan.....	4
BAB II LANDASAN TEORI.....	6
2.1 Tinjauan Pustaka	6
2.2 Aplikasi Mobile.....	7
2.3 Media Pembelajaran	8
2.3.1 Penertian Media Pembelajaran.....	8
2.3.2 Klasifikasi Media Pembelajaran	8
2.4 Kriptografi	9
2.4.1 Definisi Kriptografi.....	10

2.4.2	Komponen Kriptografi.....	10
2.4.3	Jenis Kriptografi.....	11
2.5	Algoritma RC4.....	13
2.6	Algoritma RSA.....	15
2.7	UML (<i>Unified Modeling Language</i>).....	18
2.7.1	<i>Use Case Diagram</i>	18
2.7.2	<i>Class Diagram</i>	20
2.7.3	<i>Activity Diagram</i>	21
2.7.4	<i>Sequence Diagram</i>	22
2.8	Android.....	23
2.8.1	Sejarah Android.....	23
2.8.2	Versi-versi Android.....	25
2.8.3	Android SDK.....	26
2.8.4	<i>Android Development Tolls (ADT)</i>	26
2.9	Eclipse.....	26
BAB III ANALISIS DAN PERANCANGAN SISTEM.....		28
3.1	Gambaran Umum Aplikasi.....	28
3.2	Analisis kebutuhan Sistem.....	28
3.2.1	Analisis Kebutuhan Fungsional.....	28
3.2.2	Analisis Kebutuhan Non Fungsional.....	29
3.2.3	Analisis Kelayakan Sistem.....	31
3.2.4	Analisis Data.....	32
3.3	Perancangan Sistem.....	39
3.3.1	Perancangan UML.....	39
3.4	Rancangan Tampilan.....	50
BAB IV IMPLENTASI DAN PEMBAHASAN.....		56
4.1	Implementasi.....	56
4.1.1	Implementasi Pembuatan Program.....	56
4.2	Pembahasan Program.....	58
4.2.1	EnkDekRC4.java.....	58
4.2.2	BuatKunci.java.....	61

4.2.3	EnkDekRSA.java	63
4.3	Tampilan Aplikasi	65
4.3.1	Form Menu Awal	66
4.3.2	Form Kriptografi RC4.....	66
4.3.3	Form Kriptografi RSA	67
4.3.4	Form Enkripsi dan Dekripsi RC4	67
4.3.5	Form Contoh Kriptografi RC4.....	68
4.3.6	Form Penjelasan Kriptografi RC4.....	68
4.3.7	Form Petunjuk Kriptografi RC4	69
4.3.8	Form Buat Kunci Kriptografi RSA	69
4.3.9	Form Enkripsi dan Dekripsi Kriptografi RSA	70
4.3.10	Form Contoh Kriptografi RSA	70
4.3.11	Form Penjelasan Kriptografi RSA	71
4.3.12	Form Petunjuk Kriptografi RSA	71
4.4	Uji Coba Program.....	72
4.5	Instalasi Program dan pembuatan APK	72
4.5.1	Menjalankan Program	73
4.5.2	Pemilihan Device untuk instalasi	73
4.5.3	Lokasi file APK	74
4.6	<i>Publish Playstore</i>	75
BAB V PENUTUP		76
5.1	Kesimpulan.....	76
5.2	Saran.....	77
DAFTAR PUSTAKA		xviii
LAMPIRAN		

DAFTAR TABEL

Tabel 2.1 Ilustrasi dari Algoritma RSA	17
Tabel 2.2 Simbol-simbol Use-case Diagram	19
Tabel 2.3 Simbol-simbol Class Diagram	20
Tabel 2.4 Simbol-simbol Activity Diagram.....	22
Tabel 2.5 Simbol-simbol Sequence Diagram	23
Tabel 3.6 Spesifikasi Komputer.....	29
Tabel 3.7 Spesifikasi Handpone.....	30
Tabel 3.8 Perangkat Lunak	30
Tabel 3.9 Kode ASCII Plainteks.....	37
Tabel 3.10 Proses XOR Kunci Enkripsi Dengan Plainteks	37
Tabel 3.11 Proses XOR Kunci Dekripsi Dengan Cipherteks	37
Tabel 4.12 Hasil Black-box Testing	72

DAFTAR GAMBAR

Gambar 2.1 Kriptografi Simetris	12
Gambar 2.2 Kriptografi Asimetris	13
Gambar 2.3 Proses Enkripsi dan Dekripsi RSA	16
Gambar 3.4 <i>Use Case Diagram</i>	40
Gambar 3.5 Activity Diagram Menu Enkripsi dan Dekripsi Kriptografi RC4.....	41
Gambar 3.6 Activity Diagram Menu Perhitungsn Manual Kriptografi RC4.....	41
Gambar 3.7 Activity Diagram Menu Penjelasan Kriptografi RC4.....	42
Gambar 3.8 Activity Diagram Menu Pentunjuk Kriptografi RC4.....	42
Gambar 3.9 Activity Diagram Menu Pembuatan Kunci Kriptografi RSA	43
Gambar 3.10 Activity Diagram Menu Enkripsi dan Dekripsi Kriptografi RSA....	43
Gambar 3.11 Activity Diagram Menu Perhitungan Manual Kriptografi RSA	44
Gambar 3.12 Activity Diagram Menu Penjelasan Kriptografi RSA	44
Gambar 3.13 Activity Diagram Menu Petunjuk Kriptografi RSA	45
Gambar 3.14 Class Diagram	46
Gambar 3.15 Sequence Diagram Menu Enkripsi dan Dekripsi Kriptografi RC4.	47
Gambar 3.16 Sequence Diagram Menu Contoh Perhitungan Manual Kriptografi RC4	47
Gambar 3.17 Sequence Diagram Menu Penjelasan Kriptografi RC4.....	47
Gambar 3.18 Sequence Diagram Menu Petunjuk Kriptografi RC4.....	48
Gambar 3.19 Sequence Diagram Menu Enkripsi dan Dekripsi Kriptografi RSA	48
Gambar 3.20 Sequence Diagram Menu Buat Kunci RSA	48
Gambar 3.21 Sequence Diagram Menu Contoh Perhitungan Manual Kriptografi RSA.....	49
Gambar 3.22 Sequence Diagram Menu Penjelasan Kriptografi RSA	49
Gambar 3.23 Sequence Diagram Menu Petujuk Kriptografi RSA	49
Gambar 3.24 Rancang Menu Awal.....	50
Gambar 3.25 Rancang Menu RC4	50
Gambar 3.26 Rancang Menu RSA.....	51
Gambar 3.27 Rancang Menu Enkripsi dan Dekripsi Kriptografi RC4	51

Gambar 3.28 Rancang Menu Contoh Perhitungan Manual Kriptografi RC4.....	52
Gambar 3.29 Rancang Menu Penjelasan Kriptografi RC4.....	52
Gambar 3.30 Rancang Menu Petunjuk Kriptografi RC4.....	53
Gambar 3.31 Rancang Menu Pembuatan Kunci Kriptografi RSA	53
Gambar 3.32 Rancang Menu Enkripsi dan Dekripsi kriptografi RSA	54
Gambar 3.33 Rancang Menu Contoh Perhitungan Manual Kriptografi RSA	54
Gambar 3.34 Rancang Menu Penjelasan Kriptografi RSA	55
Gambar 3.35 Rancang Menu Petunjuk Kriptografi RSA	55
Gambar 4.36 New Android Application.....	57
Gambar 4.37 Halaman Kerja Eclipse.....	58
Gambar 4.38 Tampilan Form Menu Awal.....	66
Gambar 4.39 Tampilan Form Kriptografi RC4	66
Gambar 4.40 Tampilan Form Kriptografi RSA.....	67
Gambar 4.41 Tampilan Form Enkripsi dan Dekripsi RC4	67
Gambar 4.42 Tampilan Form Contoh Kriptografi RC4.....	68
Gambar 4.43 Tampilan Form Penjelasan Kriptografi RC4	68
Gambar 4.44 Tampilan Form Petunjuk Kriptografi RC4	69
Gambar 4.45 Tampilan Form Buat Kunci Kriptografi RSA.....	69
Gambar 4.46 Tampilan Form Enkripsi dan Dekripsi Kriptografi RSA.....	70
Gambar 4.47 Tampilan Form Contoh Kriptografi RSA	70
Gambar 4.48 Tampilan Form Penjelasan Kriptografi RSA.....	71
Gambar 4.49 Tampilan Form Petunjuk Kriptografi RSA.....	71
Gambar 4.50 Menjalankan Program	73
Gambar 4.51 Pemulihan Device	74
Gambar 4.52 Lokasi File APK.....	74
Gambar 4.53 Kriptografi RC4 dan RSA di <i>playstore</i>	75

INTISARI

Kriptografi adalah ilmu yang digunakan untuk menjaga kerahasiaan sebuah data. Dalam perkembangannya kriptografi terdapat banyak algoritma, diantaranya adalah algoritma RC4 dan RSA. Dalam setiap algoritma mempunyai metode yang berbeda dalam tingkat kerumitan dan proses perhitungannya, maka demikian masih banyak orang yang masih sulit memahami tentang kriptografi RC4 dan RSA.

Pada skripsi ini diharapkan akan memudahkan untuk mempelajari kriptografi yang dibuat dalam bentuk aplikasi. Dalam aplikasi ini ada 2 jenis kriptografi yaitu dengan metode RC4 untuk jenis kriptografi simetri dan metode RSA untuk metode ansimetri yang masing-masing terdapat contoh perhitungan manual dalam proses enkripsi maupun dekripsi secara sederhana , sehingga memudahkan dalam memahami dalam belajar dan juga terdapat informasi yang berhubungan dengan kriptografi RC4 dan RSA yang akan mempermudah penggunaan aplikasi ini.

Dalam perancangan ini aplikasi menggunakan bahasa pemrograman java dengan software eclipse. Aplikasi dibuat dalam bentuk mobile sehingga padat sewaktu-waktu dapat dipelajari dengan mudah.

Kata kunci : Kriptografi, Algoritma, RC4, RSA, Enkripsi dan Dekripsi.

ABSTRACT

Cryptography is the science that is used to maintain the confidentiality of a data. In its development, there are many cryptographic algorithms, such as RC4 and RSA algorithms. In each of these algorithms has different methods and levels of complexity in the calculation process, then so many people are still hard to understand about RC4 and RSA cryptography.

In this thesis, is expected to be easier to learn cryptography made in the application form. In this application there are two types of cryptography is the cryptographic method for this type of symmetry RC4 and RSA method for ansimetri methods, each of which are examples of manual calculations in the encryption and decryption process is simple, making it easier to understand the study and also information relating to RC4 and RSA cryptography that will facilitate the use of this application.

In this design applications using the Java programming language software eclipse. Made in the form of mobile applications so dense at times can be learned easily.

Keywords: *Cryptography, algorithms, RC4, RSA, Encryption and Decryption.*

