

**PERANCANGAN APLIKASI KRIPTOGRAFI RC4 DAN DSA SEBAGAI  
MEDIA BELAJAR KRIPTOGRAFI BERBASIS MOBILE**

**SKRIPSI**



disusun oleh

**Abdul Rachim**

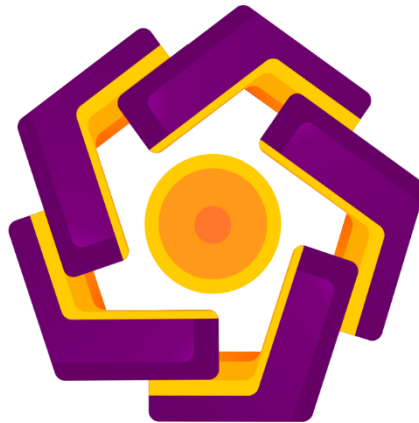
**11.11.5364**

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

**PERANCANGAN APLIKASI KRIPTOGRAFI RC4 DAN DSA SEBAGAI  
MEDIA BELAJAR KRIPTOGRAFI BERBASIS MOBILE**

**SKRIPSI**

untuk memenuhi sebagian persyaratan  
mencapai gelar Sarjana  
pada Program Studi Teknik Informatika



disusun oleh  
**Abdul Rachim**  
**11.11.5364**

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

**PERSETUJUAN**

**SKRIPSI**

**PERANCANGAN APLIKASI KRIPTOGRAFI RC4 DAN DSA SEBAGAI  
MEDIA BELAJAR KRIPTOGRAFI BERBASIS MOBILE**

yang dipersiapkan dan disusun oleh

**Abdul Rachim**

**11.11.5364**

telah disetujui oleh Dosen Pembimbing Sripsi  
pada tanggal 13 Maret 2015

Dosen Pembimbing,

  
**Dony Arivus, M.Kom**  
**NIK. 190302128**

**PENGESAHAN**  
**SKRIPSI**  
**PERANCANGAN APLIKASI KRIPTOGRAFI RC4 DAN DSA SEBAGAI**  
**MEDIA BELAJAR KRIPTOGRAFI BERBASIS MOBILE**

yang dipersiapkan dan disusun oleh

**Abdul Rachim**

**11.11.5364**

telah dipertahankan di depan Dewan Penguji  
pada tanggal 23 September 2016

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

**Anggit Dwi Hartanto, M.Kom**  
NIK. 190302163

**Dony Ariyus, M.Kom**  
NIK. 190302128

**Windha Mega Pradnya D, M.Kom**  
NIK. 190302185



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
tanggal 24 Oktober 2016



**KETUA STMIK AMIKOM YOGYAKARTA**

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

## PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya 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 pembuatan 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 September 2016



Abdul Rachim  
NIM. 11.11.5364

## MOTTO

Mulailah sesuatu dengan membaca “Bismillahirrahmanirrahim” dan akhiri dengan “Alhamdulillahirobbil ‘alamin” agar sesuatu yang kita kerjakan diridhoi Allah

SWT

Bersyukurlah atas apa yang kamu miliki saat ini, karena masih banyak orang disekeliling kamu yang masih kurang beruntung

"Kerjakan kebaikan meskipun kamu anggap itu kecil, sebab engkau tidak tahu kebaikan mana yang memasukanmu ke surga"

Hasan Al-Bashri

"Bahagia adalah ketika kita lebih sering tersenyum, lebih berani bermimpi, lebih mudah tertawa, dan lebih banyak bersyukur"

Merry Riana

“Barang siapa bersungguh-sungguh, sesungguhnya kesungguhannya itu adalah untuk dirinya sendiri”

Al-Ankabut, ayat 6

## PERSEMBAHAN

Syukur Alhamdulillah atas kehadiran Allah SWT yang telah memberikan rahmat dan karunia-Nya sehingga karya ini dapat terselesaikan dengan baik dan lancar tanpa ada hambatan yang berarti.

Karya kecil ini kupersembahkan untuk:

1. Bapak dan Ibu tercinta, sebagai bentuk bakti kecilku, meski tidak sedikitpun bisa membalas segala pengorbanan dan kasih sayang yang telah kalian berikan.
2. Bapak Dony Ariyus, M.Kom selaku dosen pembimbing yang telah banyak memotivasi.
3. Teman-teman kost minomartani yang telah banyak memberikan dukungan dan motivasi nya.
4. Teman - temanku kelas 11-S1TI-11 yang selalu memberikan semangat.
5. Semua pihak yang telah memberikan dukungan secara langsung maupun tidak langsung dan almamater tercinta.

## KATA PENGANTAR

Puji dan syukur penulis persembahkan untuk Allah SWT yang telah memberikan rahmat, hidayah dan kekuatan sehingga penulis dapat menyelesaikan skripsi ini sesuai dengan waktu yang diinginkan penulis. Tidak lupa sholawat serta salam penulis haturkan pada junjungan umat yaitu Nabi Muhammad SAW, yang telah menyebarkan agama Islam sehingga penulis dan seluruh umat Islam dapat merasakan indahnya Islam.

Skripsi ini disusun sebagai salah satu syarat kelulusan bagi setiap mahasiswa STMIK AMIKOM Yogyakarta. Selain itu juga merupakan suatu bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang program Strata-1 dan untuk memperoleh gelar Sarjana Komputer.

Dengan selesainya skripsi ini, maka penulis tidak lupa mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. M. Suyanto, M.M selaku Ketua STMIK AMIKOM Yogyakarta.
2. Bapak Sudarmawan, MT selaku ketua jurusan Teknik Informasi STMIK AMIKOM Yogyakarta.
3. Bapak Dony Ariyus, M.Kom selaku dosen pembimbing yang telah sabar membimbing dan banyak memberikan pengarahan bagi penulis dalam pembuatan skripsi ini.
4. Kedua Orang Tua saya yang telah memberikan doa serta dukungan yang begitu luar biasa untuk saya.



5. Bapak dan Ibu Dosen STMIK AMIKOM Yogyakarta yang telah banyak memberikan ilmunya selama penulis kuliah.
6. Teman-teman saya selama mengikuti perkuliahan.
7. Semua pihak yang telah membantu baik dukungan moril maupun materiil, pikiran, dan tenaga dalam penyelesaian skripsi ini.

Penulis tentunya menyadari bahwa pembuatan skripsi ini masih banyak sekali kekurangan-kekurangan dan kelemahan-kelemahannya. Oleh karena itu penulis berharap kepada semua pihak agar dapat menyampaikan kritik dan saran yang membangun untuk menambah kesempurnaan skripsi ini. Namun penulis tetap berharap skripsi ini akan bermanfaat bagi semua pihak yang membacanya.

Yogyakarta, 19 September 2016

Penulis

## DAFTAR ISI

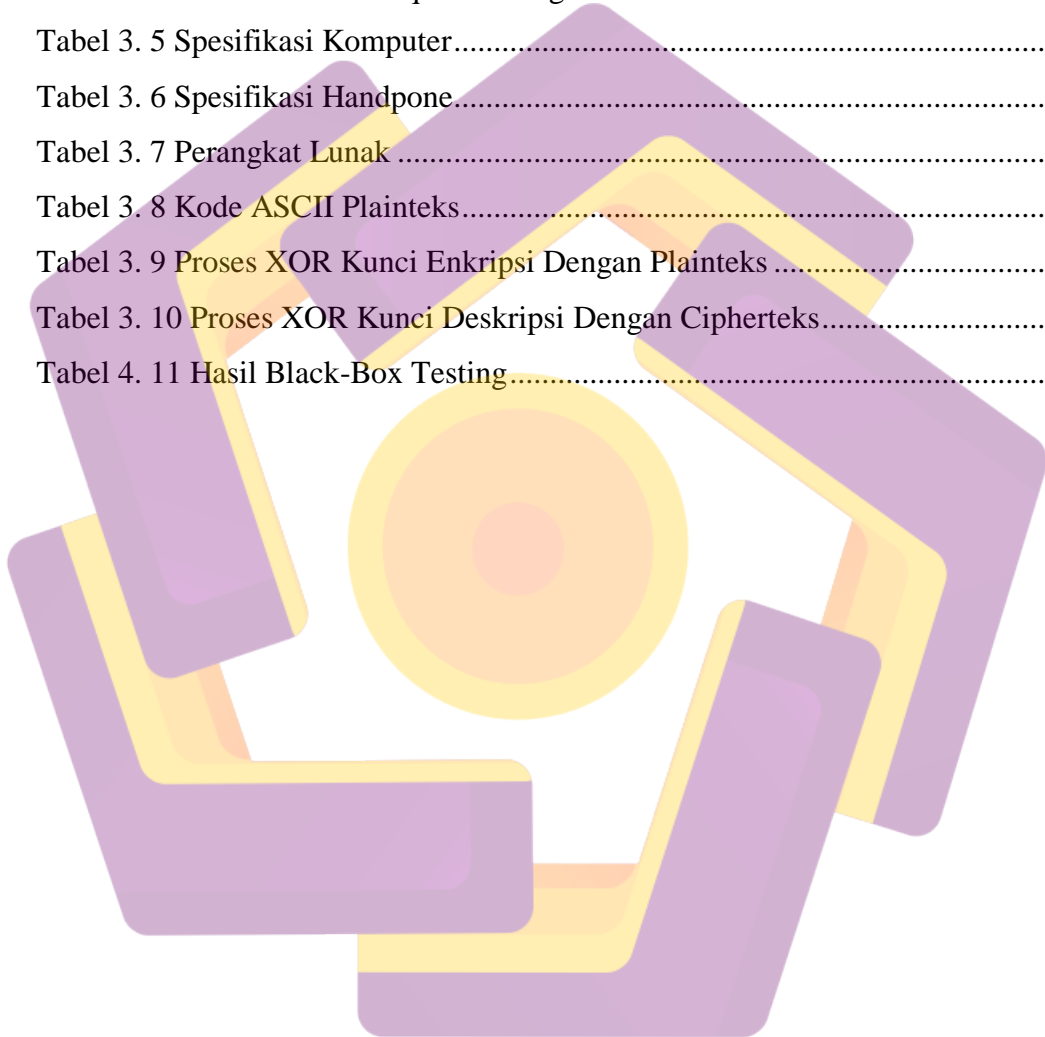
JUDUL .....	i
PERSETUJUAN .....	ii
PENGESAHAN .....	iii
PERNYATAAN .....	iv
MOTTO .....	v
PERSEMBAHAN .....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI .....	ix
DAFTAR TABEL .....	xii
DAFTAR GAMBAR .....	xiii
INTISARI .....	xv
ABSTRACT .....	xvi
<b>BAB I PENDAHULUAN</b> .....	<b>1</b>
1.1 Latar Belakang Masalah .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah .....	2
1.4 Tujuan Penelitian .....	2
1.5 Manfaat Penelitian .....	3
1.6 Metodologi Penelitian .....	3
1.7 Sistematika Penulisan .....	5
<b>BAB II LANDASAN TEORI</b> .....	<b>6</b>
2.1 Landasan Teori .....	6
2.2 Aplikasi Mobile .....	7
2.3 Media Pembelajaran .....	8
2.3.1 Pengertian 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 DSA .....	15
2.7	UML (Unified Modeling Language).....	18
2.7.1	Usecase Diagram.....	19
2.7.2	Class Diagram .....	21
2.7.3	Activity Diagram .....	23
2.7.4	Sequence Diagram .....	24
2.8	Android.....	25
2.8.1	Sejarah Android .....	25
2.8.2	Versi-versi Android .....	27
2.8.3	Android SDK .....	28
2.8.4	Android Development Tolls (ADT).....	28
2.9	Eclipse .....	29
<b>BAB III ANALISIS DAN PERANCANGAN SISTEM.....</b>		<b>30</b>
3.1	Gambaran Umum Apikasi.....	30
3.2	Analisis Kebutuhan Sistem .....	30
3.2.1	Analisis Kebutuhan Fungsional .....	30
3.2.2	Analisis Kebutuhan Non Fungsional .....	31
3.2.3	Analisis Kelayakan Sistem .....	33
3.2.4	Analisis Data .....	34
3.3	Perancangan Sistem.....	42
3.3.1	Perancangan UML .....	42
3.4	Rancangan Tampilan.....	50
<b>BAB IV IMPLEMENTASI DAN PEMBAHASAN .....</b>		<b>55</b>
4.1	Implementasi .....	55
4.1.1	Implementasi Pembuatan Program .....	55
4.2	Pembahasan Program .....	56
4.2.1	enDekRC4.java .....	57
4.2.2	Kunci.java .....	60
4.2.3	sidikdigital.java.....	64
4.2.4	verifikasi.java.....	67

4.3	Tampilan Apikasi .....	68
4.3.1	Form Menu Awal .....	68
4.3.2	Form Kriptografi RC4.....	69
4.3.3	Form Kriptografi DSA .....	69
4.3.4	Form Penjelasan Kriptografi RC4 .....	70
4.3.5	Form Contoh Kriptografi RC4 .....	70
4.3.6	Form Petunjuk Kriptografi RC4 .....	71
4.3.7	Form Enkripsi dan Dekripsi Kriptografi RC4 .....	71
4.3.8	Form Penjelasan Kriptografi DSA .....	72
4.3.9	Form Contoh Kriptografi DSA .....	72
4.3.10	Form Petunjuk Kriptografi DSA .....	73
4.3.11	Form Buat Kunci Kriptografi DSA .....	73
4.3.12	Form Sidik Digital Kriptografi DSA .....	74
4.3.13	Form Verifikasi Kriptografi DSA .....	74
4.4	Uji Coba Program.....	75
4.5	Instalasai Program dan Pembuatan APK .....	75
4.5.1	Menjalankan Program .....	76
4.5.2	Pemilihan Device Untuk Instalasi.....	76
4.5.3	Lokasi File APK .....	77
BAB V PENUTUP .....		78
5.1	Kesimpulan.....	78
5.2	Saran.....	79
DAFTAR PUSTAKA .....		80

## DAFTAR TABEL

Tabel 2. 1 Simbol-simbol Use-case Diagram .....	20
Tabel 2. 2 Simbol-simbol Class Diagram .....	22
Tabel 2. 3 Simbol-simbol Activity Diagram.....	23
Tabel 2. 4 Simbol-simbol Sequence Diagram .....	25
Tabel 3. 5 Spesifikasi Komputer.....	32
Tabel 3. 6 Spesifikasi Handpone.....	32
Tabel 3. 7 Perangkat Lunak .....	33
Tabel 3. 8 Kode ASCII Plainteks.....	39
Tabel 3. 9 Proses XOR Kunci Enkripsi Dengan Plainteks .....	40
Tabel 3. 10 Proses XOR Kunci Deskripsi Dengan Cipherteks.....	40
Tabel 4. 11 Hasil Black-Box Testing.....	75



## DAFTAR GAMBAR

Gambar 2. 1 Kriptografi Simetri .....	12
Gambar 2. 2 Kriptografi Asimetri.....	13
Gambar 2. 3 Proses Tanda Tangan Digital .....	16
Gambar 2. 4 Tanda Tangan Digital.....	16
Gambar 2. 5 Fungsi Tanda Tangan Digital dengan Fungsi Hash .....	17
Gambar 3. 6 Use Case Diagram.....	43
Gambar 3. 7 Activity Diagram Menu Enkripsi Dan Deskripsi Kriptografi RC4 ..	43
Gambar 3. 8 Activity Diagram Menu Perhitungan Manual Kriptografi RC4 .....	44
Gambar 3. 9 Activity Diagram Menu Penjelasan Kriptografi RC4.....	44
Gambar 3. 10 Activity Diagram Menu Petunjuk Kriptografi RC4.....	44
Gambar 3. 11 Activity Diagram Menu Pembuatan Kunci Kriptografi RC4 .....	45
Gambar 3. 12 Activity Diagram Menu Verifikasi Kriptografi DSA .....	45
Gambar 3. 13 Activity Diagram Menu Perhitungan Manual Kriptografi DSA.....	46
Gambar 3. 14 Activity Diagram Menu Penjelasan Kriptografi DSA .....	46
Gambar 3. 15 Activity Diagram Menu Petunjuk Kriptografi DSA .....	46
Gambar 3. 16 Class Diagram .....	47
Gambar 3. 17 Sequence Diagram Menu Penjelasan RC4.....	48
Gambar 3. 18 Sequence Diagram Menu Contoh Perhitungan Manual RC4 .....	48
Gambar 3. 19 Sequence Diagram Menu Petunjuk Kriptografi RC4.....	48
Gambar 3. 20 Sequence Diagram Menu Enkripsi dan Dekripsi Kriptografi RC4.	49
Gambar 3. 21 Sequence Diagram Menu Penjelasan Kriptografi DSA .....	49
Gambar 3. 22 Sequence Diagram Menu Contoh Perhitungan Manual Kriptografi DSA.....	49
Gambar 3. 23 Sequence Diagram Menu Petunjuk Kriptografi DSA.....	50
Gambar 3. 24 Sequence Diagram Menu Verifikasi Kriptografi DSA .....	50
Gambar 3. 25 Rancang Menu Awal.....	50
Gambar 3. 26 Rancang Menu RC4 .....	51
Gambar 3. 27 Rancang Menu DSA .....	51
Gambar 3. 28 Rancang Menu Penjelasan Kriptografi RC4 .....	51

Gambar 3. 29 Rancang Menu Contoh Perhitungan Manual Kriptografi RC4.....	52
Gambar 3. 30 Rancang Menu Petunjuk Kriptografi RC4.....	52
Gambar 3. 31 Rancang Menu Enkripsi dan Dekripsi Kriptografi RC4.....	52
Gambar 2. 32 Rancang Menu Penjelasan Kriptografi DSA .....	53
Gambar 3. 33 Rancang Menu Contoh Perhitungan Manual Kirptografi DSA.....	53
Gambar 3. 34 Rancang Menu Petunjuk Kriptografi DSA .....	53
Gambar 3. 35 Rancang Menu Pembuatan Kunci Kriptografi DSA.....	54
Gambar 3. 36 Rancang Menu Sidik Digital Kriptografi DSA.....	54
Gambar 3. 37 Rancang Menu Verifikasi Kriptografi DSA .....	54
Gambar 2. 38 New Android Aplikasi .....	56
Gambar 2. 39 Halaman Kerja Eclipse.....	56
Gambar 4. 40 Tampilan Form Menu Awal.....	68
Gambar 4. 41 Tampilan Form Kriptografi RC4 .....	69
Gambar 4. 42 Tampilan Form Kriptografi DSA.....	69
Gambar 4. 43 Tampilan Form Penjelasan RC4 .....	70
Gambar 4. 44 Tampilan Form Contoh Kriptografi RC4.....	70
Gambar 4. 45 Tampilan Form Petunjuk Kriptografi RC4 .....	71
Gambar 4. 46 Tampilan Form Enkripsi dan Dekripsi Kriptografi RC4 .....	71
Gambar 4. 47 Tampilan Form Penjelasan Kriptografi DSA.....	72
Gambar 4. 48 Tampilan Form Contoh Kriptografi DSA .....	72
Gambar 4. 49 Tampilan Form Petunjuk Kriptografi DSA .....	73
Gambar 4. 50 Tampilan Form Buat Kunci Kriptografi DSA .....	73
Gambar 4. 51 Tampilan Form Sidik Digital Kriptografi DSA .....	74
Gambar 4. 52 Tampilan Form Verifikasi Kriptografi DSA.....	74
Gambar 4. 53 Menjalankan Program .....	76
Gambar 4. 54 Pemilihan Device .....	76
Gambar 4. 55 Lokasi File APK.....	77

## INTISARI

Kriptografi adalah ilmu yang digunakan untuk menjaga kerahasiaan sebuah data. Dalam perkembangannya kriptografi terdapat banyak algoritma, diantaranya adalah algoritma RC4 dan DSA. 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 DSA.

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 DSA 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 DSA 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, DSA, Enkripsi dan Dekripsi, Verifikasi Pesan.



## **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 DSA 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 DSA 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 DSA 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 DSA 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, DSA, Encryption and Decryption, Message Verification.*