MEDIA PEMBELAJARAN ALGORITMA KRIPTOGRAFI AES DAN RSA BERBASIS ANDROID

SKRIPSI

disusun oleh

Handy Thadius

12.11.6449

PROGRAM SARJANA PROGRAM STUDI INFORMATIKA FAKULTAS ILMU KOMPUTER UNIVERSITAS AMIKOM YOGYAKARTA YOGYAKARTA

2017

MEDIA PEMBELAJARAN ALGORITMA KRIPTOGRAFI AES DAN RSA BERBASIS ANDROID

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika

disusun oleh

Handy Thadius

12.11.6449

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2017

PERSETUJUAN

SKRIPSI

MEDIA PEMBELAJARAN ALGORITMA KRIPTOGRAFI AES DAN RSA BERBASIS ANDROID

yang dipersiapkan dan disusun oleh

Handy Thadius

12.11.6449

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 10 Maret 2017

Dosen Pembimbing,

Kusrini, S.Kom, M.Kom, Dr.
NIK. 190302106

PENGESAHAN

SKRIPSI

MEDIA PEMBELAJARAN ALGORITMA KRIPTOGRAFI AES DAN RSA BERBASIS ANDROID

yang dipersiapkan dan disusun oleh

Handy Thadius

12.11.6449

telah dipertahankan di depan Dewan Penguji
pada tanggal 20 Maret 2017

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Kusrini, S.Kom, M.Kom, Dr. **NIK. 190302106**	
Ferry Wahyu Wibowo, S.Si., M.Cs **NIK. 190302235**	
Rizqi Sukma Kharisma, M.Kom **NIK. 190302215**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 20 Maret 2017

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, Tugas Akhir ini merupakan karya saya (ASLI), dan isi dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya 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.

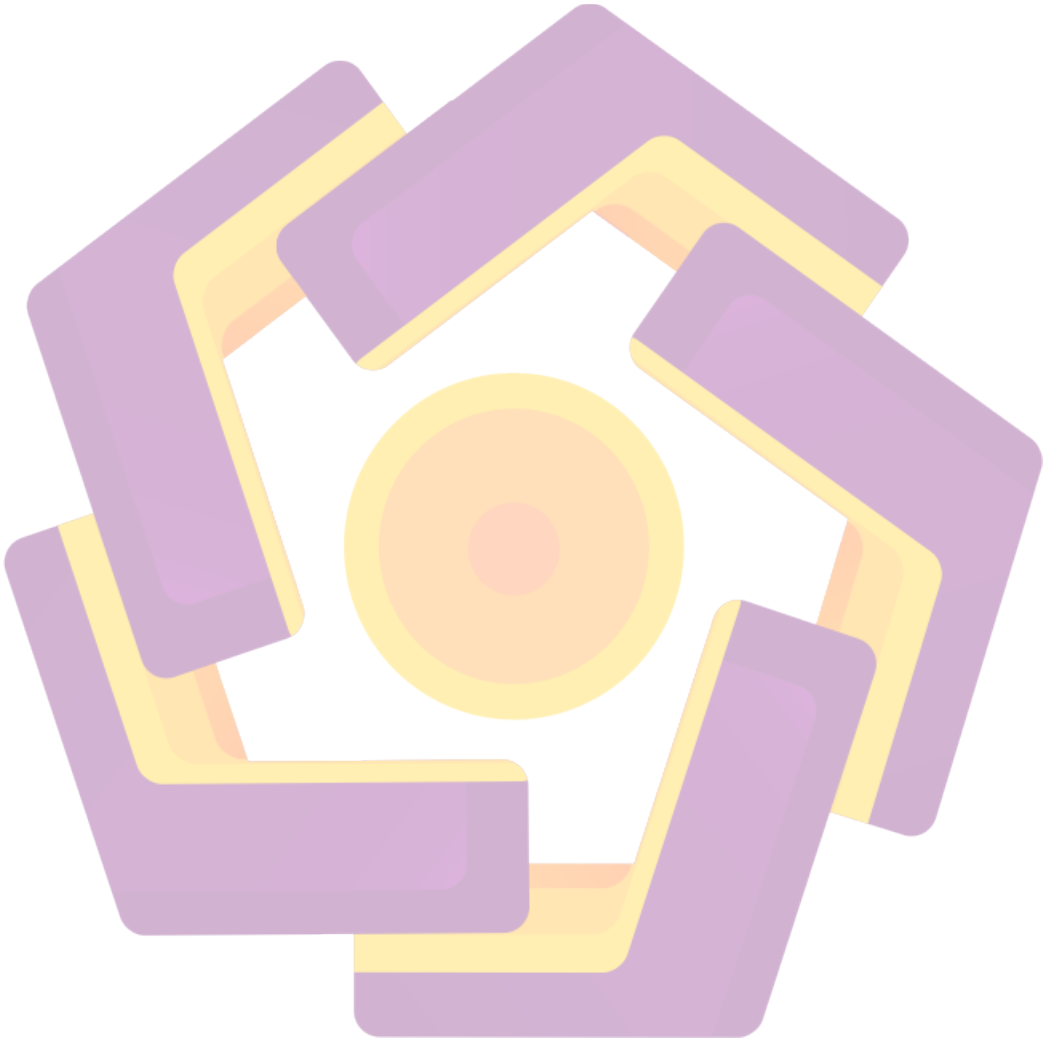
Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 20 Maret 2017

Handy Thadius
NIM. 12.11.6449

MOTTO

I’m Here, I’m Ready.



PERSEMBAHAN

Dengan mengucapkan rasa syukur yang tak terhingga atas karunia Tuhan yang maha kuasa. Skripsi ini dipersembahkan kepada mareka yang telah berjasa dan menginspirasi penulis.

1. Tuhan yang maha kuasa yang terus menyertai dan memberi kekuatan dalam menghadapi rintangan-rintangan yang penulis hadapi.
2. Kedua orang tua yang senantiasa bersabar dalam mendukung, berdoa, dan memberi semangat untuk penulis.
3. Seluruh teman-teman kelas 12 S1TI 10 yang telah memberi kenangan yang tak terlupakan semasa kuliah dan saling bahu-membahu dalam menyelesaikan setiap *final project.*
4. Saudara seperantauan di asrama TPN yang memberi dukungan dalam setiap keseharian.
5. Serta seluruh pihak yang telah banyak membantu dan tidak bisa disebutkan satu per satu, dengan penuh rasa bahagia penulis ucapkan terima kasih bayak.

KATA PENGANTAR

Puji dan syukur penulis persembahkan kepada Tuhan yang maha kuasa yang telah meyertai penulis dalam menyelesaikan skripsi yang berjudul Media Pembelajaran Algoritma Kriptografi AES dan RSA berbasis Android dapat terselesaikan.

Penulisan skripsi ini di ajukan untuk memenuhi salah satu syarat kelulusan dalam jenjang perkuliahan Strata 1 Universitas AMIKOM Yogyakarta, penulis menyadari bahwa dalam penyelesaian penulisan skripsi ini juga berkat dukungan, dorongan, dan bimbingan dari berbagai pihak, untuk itu penulis ucapkan terima kasih kepada:

1. Bapak Prof. Dr. M. Suyanto, MM selaku Ketua Universitas AMIKOM Yogyakarta.
2. Ibu Kusriri, Dr., M. Kom. selaku dosen pembimbing yang telah membantu dalam pembuatan skripsi ini.
3. Segenap Staf Pengajar di Universitas AMIKOM Yogyakarta yang telah memberi ilmu dan pemahaman tentang dunia informatika.
4. Keluarga besar yang selalu memberikan doa dan dukungan selama kuliah.
5. Teman-teman yang telah banyak membantu dalam menyelesaikan skripsi ini.

Disadari bahwa dalam penyusunan laporan skripsi ini masih jauh dari kata sempurna. Oleh karna itu kritik dan saran yang bersifat membntu sangat di butuhkan.

Akhir kata, semoga penyusunan skripsi ini bermanfaat di kemudian hari, khususnya bagi penulisan dan umumnya bagi kita semua dalam rangka menambah wawasan pengetahuan dan pemikiran kita.

Yogyakarta, 18 Maret 2017

Penulis,

Handy Thadius

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
BAB I PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Rumusan Masalah.....2
1.3 Batasan Masalah 2
1.4 Maksud dan Tujuan Penelitian.....3
1.5 Manfaat Penelitian 3
1.6 Metode Penelitian 4
1.7 Sistematika Penulisan 4
BAB II LANDASAN TEORI.....6
2.1 Tinjauan Pustaka.....6
2.2 Kriptografi.....7
2.2.1 Algoritma AES (*Advanced Encryption Standard*).....8
2.2.2 Algoritma RSA *(Rivest Shamir Adleman)* 8
2.3 *Unified Modeling Language* (UML).....9
2.3.1 *Use Case Diagram*.....9
2.3.2 *Class Diagram* 10

2.3.3 *Activity Diagram* 11
2.3.4 *Sequence Diagram* 12
2.4 Android 13
2.5 Android Studio 13
BAB III ANALISIS DAN PERANCANGAN 15
3.1 Gambaran Umum 15
3.2 Analisis SWOT 15
3.3 Analisis Kebutuhan Sistem 16
3.3.1 Kebutuhan Fungsional 17
3.3.2 Kebutuhan Non Fungsional 17
3.4 Analisis Kelayakan Sistem 19
3.4.1 Kelayakan Teknologi 19
3.4.2 Kelayakan Operasional 19
3.4.3 Kelayakan Hukum 19
3.4.4 Kebutuhan Pengguna 19
3.5 Perancangan Sistem 19
3.5.1 Perancangan UML 20
3.5.1.1 *Use Case Diagram* 20
3.5.1.2 *Activity Diagram* 21
3.5.1.3 *Class Diagram* 23
3.5.1.4 *Sequence Diagram* 25
3.5.2 Perancangan *Interface* 27
BAB IV IMPLEMENTASI DAN PEMBAHASAN 30
4.1 Implementasi 30
4.1.1 Implementasi *Class* 30
4.1.1.1 Class Menu Utama 30
4.1.1.2 Class AES 32
4.1.1.3 Class Enkrip/Dekrip AES 33
4.1.1.4 Class Generate AES 35
4.1.1.5 Class RSA 42
4.1.1.6 Class Enkrip/Dekrip RSA 44

4.1.1.7 Class Converter 46
4.1.2 Pengujian Sistem 48
4.1.2.1 Menu Utama 49
4.1.2.2 Menu AES 52
4.1.2.3 Enkrip/Dekrip AES 57
4.1.2.4 Menu RSA 59
4.1.2.5 Enkrip/Dekrip RSA 63
4.1.2.6 Menu Konversi Bilangan 64
4.1.3 Pengujian Kompatibilitas 66
4.2 Pembahasan 66
4.2.1 Manual Aplikasi 66
4.2.1.1 Tampilan Menu Utama 66
4.2.1.2 Tampilan Menu AES 67
4.2.1.3 Tampilan Menu Enkrip/Dekrip AES 68
4.2.1.4 Tampilan Menu RSA 69
4.2.1.5 Tampilan Menu Enkrip/Dekrip RSA 70
4.2.1.6 Tampilan Menu Konversi Bilangan 71
4.2.2 Manual Instalasi 72
4.2.3 Pengembangan Sistem 73
BAB V PENUTUP 74
5.1 KESIMPULAN 74
5.2 SARAN 74
DAFTAR PUSTAKA 76

DAFTAR TABEL

Tabel 2.1 *Use Case Diagram* 9
Tabel 2.2 *Class Diagram*.....11
Tabel 2.3 *Activity Diagram* 12
Tabel 2.4 *Sequence Diagram*.....12
Tabel 3.1 Tabel Analisis SWOT.....16
Tabel 3.2 Spesifikasi Komputer 17
Tabel 3.3 Spesifikasi Mobile 18
Tabel 3.4 Sistem Operasi Komputer.....18
Tabel 3.5 Sistem Operasi Mobile 18
Tabel 4.1 Pengujian Menu Utama 47
Tabel 4.2 Pengujian Menu AES 50
Tabel 4.3 Pengujian Enkrip/Dekrip AES 56
Tabel 4.4 Pengujian Menu RSA 58
Tabel 4.5 Pengujian Enkrip/Dekrip RSA 61
Tabel 4.6 Pengujian Menu Konversi Bilangan.....63
Tabel 4.7 Pengujian Aplikasi di berbagai device 66

DAFTAR GAMBAR

Gambar 3.1 *Use Case Diagram* 20
Gambar 3.2 *Activity Diagram* 22
Gambar 3.3 *Class Diagram* 24
Gambar 3.4 *Sequence Diagram* 26
Gambar 3.5 Menu Utama Aplikasi 27
Gambar 3.6 Menu AES 27
Gambar 3.7 Menu RSA 28
Gambar 3.8 Menu *Converter* 28
Gambar 3.9 Enkrip/Dekrip AES 29
Gambar 3.10 Enkrip/Dekrip RSA 29
Gambar 4.1 *Source Code* Menu Utama 31
Gambar 4.2 *Source Code* Menu AES 33
Gambar 4.3 *Source Code* Enkrip/Dekrip AES 35
Gambar 4.4 *Source Code Generate* AES 42
Gambar 4.5 *Source Code* Menu RSA 43
Gambar 4.6 *Source Code* Enkrip/Dekrip RSA 46
Gambar 4.7 *Source Code* Menu Konversi Bilangan 48
Gambar 4.8 Testing *Navigation Drawer* Menu Utama 50
Gambar 4.9 Testing Tombol AES 50
Gambar 4.10 Testing Tombol RSA 51
Gambar 4.11 Testing Tombol *Converter* 51
Gambar 4.12 Testing *Navigation Drawer* AES 53
Gambar 4.13 Testing Tombol *Overview* AES 54
Gambar 4.14 Testing Tombol *SubBytes* 54
Gambar 4.15 Testing Tombol *ShiftRow* 55
Gambar 4.16 Testing Tombol *MixColumn* 55
Gambar 4.17 Testing Tombol *AddRoundKey* 56
Gambar 4.18 Testing Tombol *Key Schedule* 56

Gambar 4.19 Testing Tombol Enkrip/Dekrip 57
Gambar 4.20 Testing Tombol Enkrip 58
Gambar 4.21 Testing Tombol Dekrip 58
Gambar 4.22 Testing Tombol Dekrip (dengan kunci yang salah) 59
Gambar 4.23 Testing *Navigation Drawer* RSA 60
Gambar 4.24 Testing Tombol *Overview* RSA 61
Gambar 4.25 Testing Tombol Pemilihan Kunci 61
Gambar 4.26 Testing Tombol Manual RSA 62
Gambar 4.27 Testing Tombol Enkrip/Dekrip RSA 62
Gambar 4.28 Testing Tombol Enkrip RSA 63
Gambar 4.29 Testing Tombol Dekrip RSA 64
Gambar 4.30 Testing Tombol *Calculate* 65
Gambar 4.31 Testing Tombol *Clear* 65
Gambar 4.32 Tampilan Menu Utama (*MainActivity*) 67
Gambar 4.33 Tampilan Menu AES 68
Gambar 4.34 Tampilan Menu Enkrip/Dekrip AES 69
Gambar 4.35 Tampilan Menu RSA 70
Gambar 4.36 Tampilan Menu Enkrip/Dekrip RSA 71
Gambar 4.37 Tampilan Menu Konversi Bilangan 72
Gambar 4.38 File .apk Aplikasi 72
Gambar 4.39 Proses instalasi 73

INTISARI

Kriptografi adalah metode yang digunakan untuk menjaga keamanan dari sebuah data atau informasi. Dalam perkembangannya kriptografi memiliki dua tipe, simetris dan asimetris yang dimana setiap algoritma memiliki metode yang berbeda pada tingkat kerumitan ataupun proses pengkodean, maka dengan demikian masih banyak kesulitan untuk mempelajari kriptografi.

Dalam aplikasi ini terdapat dua jenis algoritma yang akan dipelajari yaitu *Advanced Encryption Standard (AES)* dan *Rivest Shamir Adleman Encryption (RSA Encryption)* yang masing-masing memilki contoh perhitungan manual, sehingga dapat membantu dalam proses mempelajari algoritma tersebut.

Dalam perancangan aplikasi ini digunakan program bahasa Java dengan software Android Studio IDE. Software di pilih karena aplikasi akan dibuat berbasis mobile dengan sistem operasi android.

Kata Kunci : Berbasis Android, Aplikasi, Kriptografi, AES, RSA.

ABSTRACT

Cryptography is a method used to maintain the security of data or information. In its development cryptography has two types, symmetric and asymmetric where each algorithm has different methods on the level of complexity or encoding process, so there is still much difficulty to learn cryptography.

In this application there are two types of algorithms that will be learned which is Advanced Encryption Standard (AES) and Rivest Shamir Adleman Encryption (RSA Encryption) which each have manual calculation example, so it can help in the process of studying the algorithm.

In designing this application used Java language program with Android Studio IDE software. Software is selected because the application will be made based on android operating system.

Keywords: *Android Based, Application, Cryptography, AES, RSA.*