PERANCANGAN APLIKASI KRIPTOGRAFI DES DAN RSA SEBAGAI MEDIA BELAJAR KRIPTOGRAFI BERBASIS MOBILE

SKRIPSI

disusun oleh :

Yusron Purbo Wiranto

10.11.4162

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

2014

PERANCANGAN APLIKASI KRIPTOGRAFI DES DAN RSA SEBAGAI MEDIA BELAJAR KRIPTOGRAFI BERBASIS MOBILE

SKRIPSI

Sebagai salah satu syarat untuk memperoleh derajat Sarjana S1 pada jurusan

Teknik Informatika Sekolah Tinggi Manajemen Informatika

dan Komputer AMIKOM YOGYAKARTA

disusun oleh

Yusron Purbo Wiranto

10.11.4162

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

2014

PERSETUJUAN

SKRIPSI

PERANCANGAN APLIKASI KRIPTOGRAFI DES DAN RSA SEBAGAI MEDIA BELAJAR KRIPTOGRAFI BERBASIS MOBILE

yang dipersiapkan dan disusun oleh

Yusron Purbo Wiranto

10.11.4162

yang disetujui oleh Dosen Pembimbing Skripsi
pada Tanggal 24 september 2013

Dosen Pembimbing

Ema Utami Dr., S.Si, M. Kom
NIK. 190302037

PENGESAHAN

SKRIPSI

PERANCANGAN APLIKASI KRIPTOGRAFI DES DAN RSA SEBAGAI MEDIA BELAJAR KRIPTOGRAFI BERBASIS MOBILE

yang dipersiapkan dan disusun oleh

Yusron Purbo Wiranto

10.11.4162

telah dipertahankan di depan Dewan Penguji
pada tanggal 17 April 2014

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Armadyah Amborowati, S.Kom, M. Eng **NIK. 190302063**	
Barka Satya, M. Kom **NIK. 190302126**	
Ema Utami Dr., S.Si, M. Kom **NIK. 190302037**	

Skripsi ini telah diterima sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 8 Mei 2014

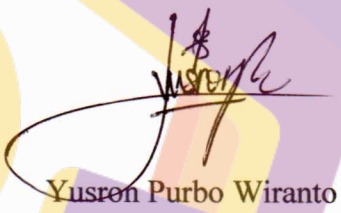
KETUA STMIK AMIKOM YOGYAKARTA

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

PERNYATAAN

Saya yang bertandatanggan 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.

Yogyakarta, 22 Aplil 2014



Yusron Purbo Wiranto

NIM 10.11.4162

HALAMAN MOTO

- Mulailah sesuatu dengan membaca "Bismillahirrahmanirrahim" dan diakhiri dengan "Alhamdulillahirobbil 'alamin" agar sesuatu yang kita kerjakan di ridhoi Allah SWT.
- Manusia hidup hakikatnya sebagai seorang guru dan seorang murid.
- Hari ini harus lebih baik dari hari kemarin dan hari esok adalah harapan.
- Sesali masa lalu karena ada kekecewaan dan kesalahan – kesalahan, tetapi jadikan penyesalan itu sebagai senjata untuk masa depan agar tidak terjadi kesalahan lagi.
- Jangan pernah mengeluh atas kekuranganmu, karena kekurangan mengingatkanmu untuk terus mencari kekuatan yang ada dalam dirimu.
- Jangan terlalu memikirkan apa yang akan terjadi di masa depan. Tak peduli bagaimana kamu merencanakan, rencana Tuhan lebih baik dari rencanamu.

HALAMAN PERSEMBAHAN

Karya tulis Ini saya persembahkan untuk :

Kedua orang tua (Puji Wiranto dan Mulatiningsih) dan kedua adikku (Reang Aji Wiranto dan Suluh Ihsan Wiranto) yang telah mendukung sepenuh hati, baik dengan doa, nasihat dan motivasi.

Ibu Ema Utami, Dr, S.Si, M.Kom sebagai dosen pembimbing yang memberikan arahan dan bimbingannya selama pengerjaan skripsi ini.

Mas Witarko yang membagikan *Source Code* yang sangat membantu dalam penyelesaian skripsi ini.

Kekasihku (Novita Paradhita Wulandari) yang telah memberikan dukungan sepenuh hati, doa, nasihat dan motivasi selama pembutan skripsi ini.

Dosen - dosen STMIK AMIKOM Yogyakarta yang telah mengampu selama perkuliahan.

Teman – teman 10-S1TI-07 dan 10-S1TI-08 yang telah menemaniku selama kuliah di STMIK AMIKOM Yogyakarta.

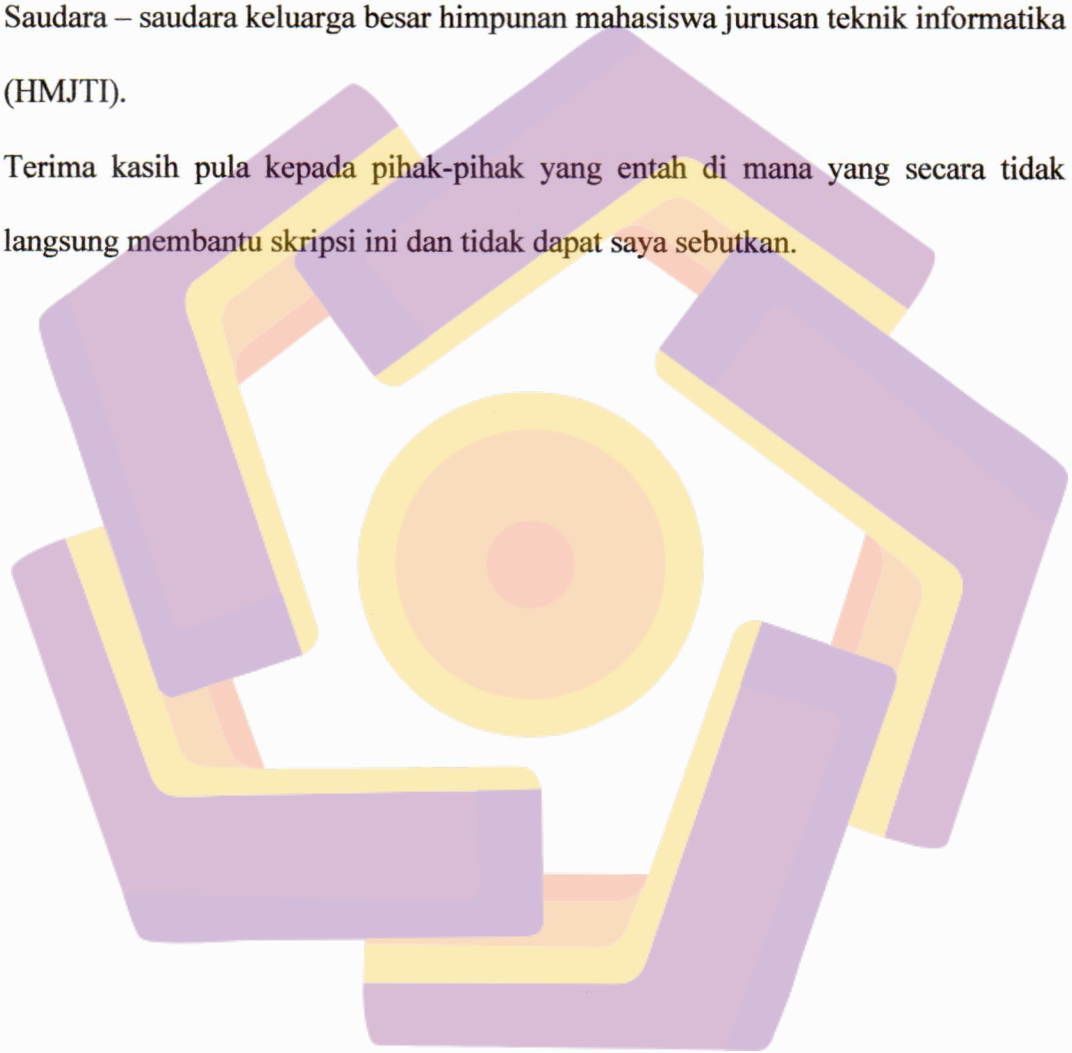
Teman – teman kontrakan Rochman Zaelani, Burhan Alfironi M, Luky Febryanto dan Dwi Ariyanto, terima kasih telah mendukung, menghibur dan menemani selama ini.

Saudara – saudara dari Himpunan Mahasiswa Jurusan Teknik Informatika (HMJTI) seperjuangan angkatan 2010 Nurhidayah Fitriani, Ridho Arji Hermawan, Arifin, Retno Ardhaningtyas Andari, Nurul Al Ayyas Rifai dan

Azhari yang menemani waktu pendadaran dan yang lainnya pula Erwin, Ahmad Fauzi Anggi Ariesta, Witarko, Dwi Hariyanto, Anita, Parsimin, M. Fikri Ritaudin, Randhi Nikson Pantas, I'mal Nur Kholis serta Devansyah Putra Pideksa, Septilia Tri Handayani dan Rizki Nadia Nur'aini, yang menemani perjalanan di HMJTI.

Saudara – saudara keluarga besar himpunan mahasiswa jurusan teknik informatika (HMJTI).

Terima kasih pula kepada pihak-pihak yang entah di mana yang secara tidak langsung membantu skripsi ini dan tidak dapat saya sebutkan.



KATA PENGANTAR

Assalamu'alaikum Warahmatullah Wabarakatuh

Alhamdulillah, Puji syukur kehadirat 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 DES DAN RSA SEBAGAI MEDIA BELAJAR KRIPTOGRAFI BERBASIS MOBILE.**"

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. Ibu Ema Utami, Dr, S.Si, 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, 22 April 2014

Penyusun

DAFTAR ISI

HALAMAN JUDUL i
PERSETUJUAN ii
PENGESAHAN iii
PERNYATAAN iv
HALAMAN MOTO v
HALAMAN 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 2
1.5 Manfaat Penelitian 3
1.6 Metode Penelitian 3
1.7 Sistematika Penulisan 4
BAB II LANDASAN TEORI 6
2.1 Kriptografi 6
2.1.1 Definisi Kriptografi 6
2.1.2 Masalah dan Ancaman Keamanan 7
2.1.3 Tujuan Kriptografi 8
2.1.4 Komponen Kriptografi 10
2.2 Jenis Kriptografi 11
2.2.1 Kriptografi Simetris 12

2.2.2 Kriptografi Asimetris 13
2.2.3 Fungsi Hash 13
2.3 Algoritma DES 14
2.4 Algoritma RSA 14
2.5 UML (Unified Modeling Language) 24
2.5.1 Usecase Diagram 24
2.5.2 Class Diagram 26
2.5.3 Activity Diagram 27
2.5.4 Sequence Diagram 28
2.6 Android 29
2.6.1 Versi-versi Android 29
2.6.2 Android SDK 33
2.6.3 Android Development Tolls (ADT) 34
2.7 Eclipse 34
BAB III ANALISIS DAN PERANCANGAN SISTEM 35
3.1 Gambaran Umum Aplikasi 35
3.2 Analisis SWOT 35
3.3 Analisis kebutuhan Sistem 37
3.3.1 Analisis Kebutuhan Fungsional 37
3.3.2 Analisis Kebutuhan Non Fungsional 38
3.3.3 Analisis Kelayakan Sistem 40
3.3.4 Analisis Data 41
3.4 Perancangan Sistem 47
3.4.1 Perancangan UML 48
3.5 Rancangan Tampilan 58
BAB IV IMPLEMENTASI DAN PEMBAHASAN 64
4.1 Implementasi 64
4.1.1 Implementasi Pembuatan Program 64
4.2 Pembahasan Program 66
4.2.1 enkDesDES.java 66
4.2.2 cEncryptDecryptProses.java 70

4.2.3 BuatKunci.java 82
4.2.4 enkDekRSA.java 84
4.3 Tampilan Aplikasi 86
4.3.1 Form Menu Awal 87
4.3.2 Form Kriptografi DES 87
4.3.3 Form Kriptografi RSA 88
4.3.4 Form Enkripsi dan Dekripsi DES 88
4.3.5 Form Contoh Kriptografi DES 89
4.3.6 Form Penjelasan Kriptografi DES 89
4.3.7 Form Petunjuk Kriptografi DES 90
4.3.8 Form Buat Kunci Kriptografi RSA 90
4.3.9 Form Enkripsi dan Dekripsi Kriptografi RSA 91
4.3.10 Form Contoh Kriptoggrafi RSA 91
4.3.11 Form Penjelasan Kriptografi RSA 92
4.3.12 Form Petunjuk Kriptografi RSA 92
4.4 Uji Coba Program 93
4.5 Instalasi Program dan pembuatan APK 93
4.5.1 Menjalankan Program 94
4.5.2 Pemilihan Device untuk instalasi 94
4.5.3 Lokasi file APK 95
BAB V PENUTUP 96
5.1 Kesimpulan 96
5.2 Saran 97
DAFTAR PUSTAKA 98

DAFTAR TABEL

Tabel 2.1 Permutasi untuk DES 15
Tabel 2.2 Pendefinisian S-boxes dari Algoritma DES 18
Tabel 2.3 Permutasi Pilihan Satu (PC-1) dan Pilihan Permutasi Dua (PC-2) .. 19
Tabel 2.4 Jumlah Pergeseran Bit pada Setiap Putaran 20
Tabel 2.5 Ilustrasi dari Algoritma DES 20
Tabel 2.6 Ilustrasi Iterasi dari Algoritma DES 21
Tabel 2.7 Ilustrasi dari Algoritma RSA 24
Tabel 2.8 Simbol-simbol Use-case Diagram 25
Tabel 3.1 Spesifikasi Komputer 39
Tabel 3.2 Spesifikasi Handpone 39
Tabel 3.3 Perangkat Lunak 40
Tabel 4.1 Tabel Hasil *Black-box Testing* 93

DAFTAR GAMBAR

Gambar 2.1 Kriptografi Simetri 12
Gambar 2.2 Kriptografi Asimetris 13
Gambar 2.3 Gambaran Umum Algoritma DES 14
Gambar 2.4 Diagram Blok Fungsi f dari Algoritma DES 17
Gambar 2.5 Proses Enkripsi dan Dekripsi RSA 22
Gambar 3.1 Use Case Diagram 48
Gambar 3.2 Activity Diagram Menu Enkripsi dan Dekripsi Kriptografi DES 49
Gambar 3.3 Activity Diagram Menu Perhitungsn Manual Kriptografi DES 50
Gambar 3.4 Activity Diagram Menu Penjelasan Kriptografi DES 50
Gambar 3.5 Activity Diagram Menu Pentunjuk Kriptografi DES 51
Gambar 3.6 Activity Diagram Menu Pembuatan Kunci Kriptografi RSA 51
Gambar 3.7 Activity Diagram Menu Enkripsi dan Dekripsi Kripografi RSA 52
Gambar 3.8 Activity Diagram Menu Contoh Perhitungan Manual Kriptografi RSA 52
Gambar 3.9 Activity Diagram Menu Penjelasan Kriptografi RSA 53
Gambar 3.10 Activity Diagram Menu Petunjuk Kriptografi RSA 53
Gambar 3.11 Class Diagram 54
Gambar 3.12 Sequence Diagram Menu Enkripsi dan Dekripsi Kriptografi DES .. 55
Gambar 3.13 Sequence Diagram Menu Contoh Perhitungan Manual Kriptografi DES 55
Gambar 3.14 Sequence Diagram Menu Penjelasan Kriptografi DES 55
Gambar 3.15 Sequence Diagram Menu Petunjuk Kriptografi DES 56
Gambar 3.16 Sequence Diagram Menu Enkripsi dan Dekripsi Kriptografi RSA . 56
Gambar 3.17 Sequence Diagram Menu Buat Kunci RSA 56
Gambar 3.18 Sequence Diagram Menu Contoh Perhitungan Manual Kriptografi RSA 57
Gambar 3.19 Sequence Diagram Menu Penjelasan Kriptografi RSA 57
Gambar 3.20 Sequence Diagram Menu Petujuk Kriptografi RSA 57
Gambar 3.21 Rancang Menu Awal 58
Gambar 3.22 Rancang Menu DES 58

Gambar 3.23Rancang Menu RSA 59
Gambar 3.24Rancang Menu Enkripsi dan Dekripsi Kriptografi DES 59
Gambar 3.25Rancang Menu Contoh Perhitungan Manual Kriptografi DES 60
Gambar 3.26Rancang Menu Penjelasan Kriptografi DES 60
Gambar 3.27Rancang Menu Petunjuk Kriptografi DES 61
Gambar 3.28Rancang Menu Pembuatan Kunci Kriptografi RSA 61
Gambar 3.29Rancang Menu Enkripsi dan Dekripsi kriptografi RSA 62
Gambar 3.30Rancang Menu Contoh Perhitungan Manual Kritografi RSA 62
Gambar 3.31Rancang Menu Penjelasan Kriptografi RSA 63
Gambar 3.32Rancang Menu Pentunjuk Kriptografi RSA 63
Gambar 4.1 New Android Application 65
Gambar 4.2 Halaman Kerja Eclipse 66
Gambar 4.3 Tampilan Form Menu Awal 87
Gambar 4.4 Tampilan Form Kriptografi DES 87
Gambar 4.5 Tampilan Form Kriptografi RSA 88
Gambar 4.6 Tampilan Form Enkripsi dan Dekripsi DES 88
Gambar 4.7 Tampilan Form Contoh Kriptografi DES 89
Gambar 4.8 Tampilan Form Penjelasan Kriptografi DES 89
Gambar 4.9 Tampilan Form Petunjuk Kriptografi DES 90
Gambar 4.10Tampilan Form Buat Kunci Kriptografi RSA 90
Gambar 4.11Tampilan Form Enkripsi dan Dekripsi Kriptografi RSA 91
Gambar 4.12Tampilan Form Contoh Kriptografi RSA 91
Gambar 4.13Tampilan Form Penjelasan Kriptografi RSA 92
Gambar 4.14Tampilan Form Petunjuk Kriptografi RSA 92
Gambar 4.15Menjalankan Program 94
Gambar 4.16Pemulihan *Device* 95
Gambar 4.17Lokasi File APK 95

INTISARI

Kriptografi adalah ilmu yang digunakan untuk menjaga kerahasiaan sebuah data. Dalam perkembangannya kriptografi terdapat banyak algoritma, diantaranya adalah algoritma DES 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 DES 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 DES 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 DES 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, DES, 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 DES 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 DES 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 DES 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 DES 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, DES, RSA, Encryption and Decryption.*