

SKRIPSI

KAMUS KRIPTOGRAFI KLASIK BERBASIS ANDROID

Oleh :

RAHMADI JULIAN

2010-51-034



PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MURIA KUDUS

2015

SKRIPSI

KAMUS KRIPTOGRAFI KLASIK BERBASIS ANDROID

Oleh :

RAHMADI JULIAN

2010-51-034



PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MURIA KUDUS

2015



UNIVERSITAS MURIA KUDUS
PENGESAHAN STATUS SKRIPSI

JUDUL : KAMUS KRIPTOGRAFI KLASIK BERBASIS ANDROID

NAMA : RAHMADI JULIAN

Mengijinkan Skripsi Teknik Informatika Ini Disimpan Di Perpustakaan Program Studi Teknik Informatika Universitas Muria Kudus Dengan Syarat – Syarat Kegunaan Sebagai Berikut :

1. Skripsi Adalah Hak Milik Program Studi Teknik Informatika Universitas Muria Kudus
2. Perpustakaan Teknik Informatika UMK Dibenarkan Membuat Salinan Untuk Tujuan Referensi Saja
3. Perpustakaan Juga Dibenarkan Membuat Salinan Skripsi Ini Sebagai Bahan Pertukaran Antar Institusi Pendidikan Tinggi
4. Berikan Tanda ✓ Sesuai Dengan Kategori Skripsi

Sangat rahasia (Mengandung isi tentang keselamatan / kepentingan Negara Republik Indonesia)

Rahasia (mengandung isi tentang kerahasiaan dari suatu organisasi / badan tepat penelitian Skripsi ini dikerjakan)

Biasa

Disahkan Oleh :

Penulis

Rahmadi Julian
2010-51-034

Pembimbing Utama

Mukhamad Nurkamid, S.Kom, M.Cs
NIDN.0620068302

Alamat: Menawan RT 01 RW 01, Kudus
Kudus, 16 Februari 2015

Kudus, 16 Februari 2015



UNIVERSITAS MURIA KUDUS

PERNYATAAN PENULIS

JUDUL : KAMUS KRIPTOGRAFI KLASIK BERBASIS ANDROID
NAMA : RAHMADI JULIAN
NIM : 2010-51-034

“Saya menyatakan dan bertanggung jawab dengan sebenarnya bahwa Skripsi ini adalah hasil karya saya sendiri kecuali cuplikan dan ringkasan yang masing-masing telah saya jelaskan sumbernya. Jika pada waktunya selanjutnya ada pihak lain yang mengklaim bahwa Skripsi ini sebagai karyanya, yang disertai dengan bukti-bukti yang cukup, maka saya bersedia untuk dibatalkan gelar Sarjana Komputer saya beserta segala hak dan kewajiban yang melekat pada gelar tersebut”.

Kudus, 16 Februari 2015



Rahmadi Julian

Penulis



UNIVERSITAS MURIA KUDUS
PERSETUJUAN SKRIPSI

JUDUL : KAMUS KRIPTOGRAFI KLASIK BERBASIS ANDROID
NAMA : RAHMADI JULIAN
NIM : 2010-51-034

Skripsi ini telah diperiksa dan disetujui,

Kudus, 16 Februari 2015

Pembimbing Utama

Pembimbing Pembantu

Mukhamad Nurkamid, S.Kom, M.Cs

NIDN. 0620068302

Tutik Khotimah, M.Kom

NIDN. 0608068502

Mengetahui

Kaprodi Teknik Informatika

Ahmad Jazuli, M.Kom

NIDN. 0406107004



UNIVERSITAS MURIA KUDUS

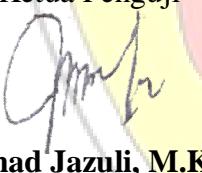
PENGESAHAN SKRIPSI

JUDUL : KAMUS KRIPTOGRAFI KLASIK BERBASIS ANDROID
NAMA : RAHMADI JULIAN
NIM : 2010-51-034

Skripsi ini telah diujikan dan dipertahankan di hadapan Dewan Pengaji pada Sidang Skripsi tanggal 26 Februari 2015. Menurut pandangan kami, Skripsi ini memadai dari segi kualitas untuk tujuan penganugerahan gelar Sarjana Komputer (S.Kom)

Kudus, 27 Februari 2015

Ketua Pengaji


Ahmad Jazuli, M.Kom
NIDN. 0406107004

Anggota Pengaji 1


Anastasya Latubessy, S.Kom, M.Cs
NIDN. 0604048702

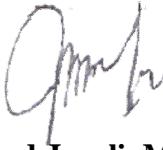
Mengetahui

Dekan Fakultas Teknik



Rochmad Winarso, S.T., M.T.
NIS. 0610701000001138

Kaprodi Teknik Informatika

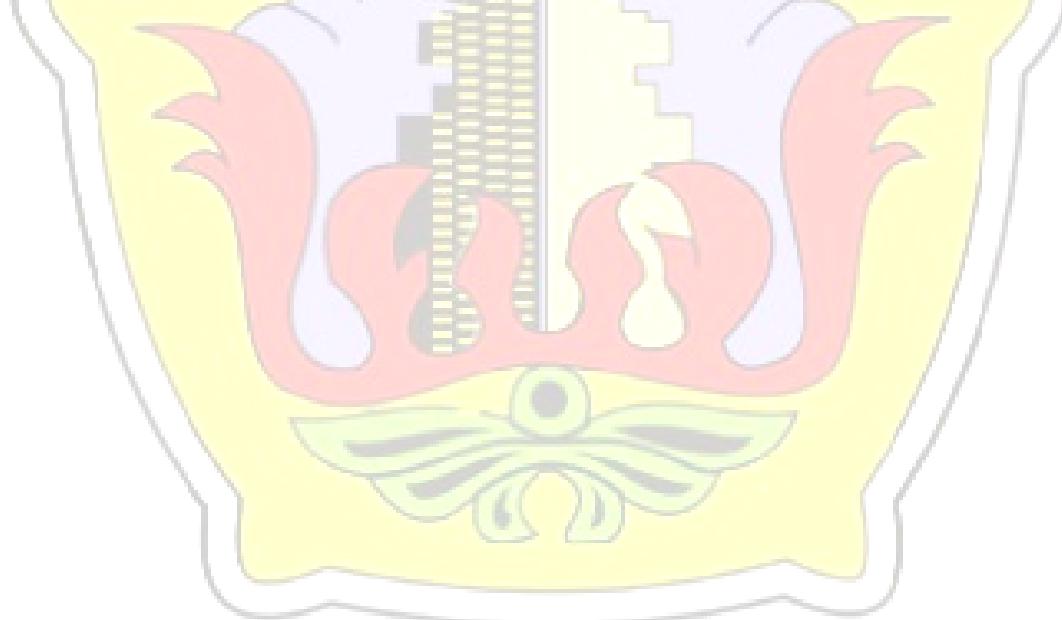


Ahmad Jazuli, M.Kom
NIDN. 0406107004

ABSTRACT

Communication is a very important thing for human life, the form of communication with exchange messages. Many people try to protect the confidentiality of information in a various ways through certain media to the intended person. Cryptography is the science or art of maintaining the confidentiality of messages and news by way of encrypting it into a form that can not be understood its meaning. The Science about of encryption technique in which data is encrypted into something that is hard to read by someone who does not have the decryption key. Decryption uses a random key to get back the original message or data. The purpose of cryptography is a message delivered only be understood by a person who is entitled to read. The method used in designing and building this application is needs analysis, planning concepts and design, application development and testing and revision applications. In this research, the use of cryptographic techniques include Caesar cipher with a key substitution alphabet, letter cipher, Vigenere cipher numbers, transposition cipher and Onetimepad. The benefits of this research is to introduce cryptographic techniques that can be used as a data security.

Keywords: Dictionary, Classical Cryptography, Android.



ABSTRAK

Komunikasi merupakan suatu hal yang sangat penting bagi kehidupan manusia, bentuk komunikasinya dengan saling bertukar pesan. Banyak orang berusaha melindungi kerahasiaan informasi dengan berbagai cara melalui media tertentu kepada orang yang dimaksud. Kriptografi adalah ilmu atau seni menjaga kerahasiaan pesan dan berita dengan cara menyandikannya ke bentuk yang tidak dapat dimengerti maknanya. Ilmu mengenai teknik enkripsi dimana data diacak menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci acak untuk mendapatkan kembali pesan atau data asli. Tujuan dari kriptografi agar suatu pesan yang disampaikan hanya dapat dimengerti oleh orang yang berhak membacanya. Metode yang digunakan dalam merancang dan membangun aplikasi ini adalah analisa kebutuhan, perancangan konsep dan desain, pembuatan aplikasi serta testing dan revisi aplikasi. Pada penelitian ini, kriptografi yang digunakan meliputi teknik substitusi Caesar *cipher* dengan kunci alphabet, Letter *cipher*, Vigenere *cipher* angka, Transposisi *cipher* dan Onetimepad. Manfaat dari penelitian ini untuk mengenalkan teknik kriptografi yang dapat digunakan sebagai keamanan data.

Kata Kunci: *Kamus, Kriptografi Klasik, Android.*

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas segala Rahmat dan Hidayah-Nya sehingga penulis mampu menyelesaikan penyusunan skripsi ini dengan judul “Kamus Kriptografi Klasik Berbasis Android”.

Skripsi ini disusun guna melengkapi salah satu persyaratan untuk memperoleh Gelar Kesarjanaan Program Studi Teknik Informatika Fakultas Teknik Universitas Muria Kudus. Pada kesempatan ini, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada :

1. Tuhan Yang Maha Esa yang selalu menunjukkan kebesaran-Nya.
2. Bapak Dr. Soeparnyo, SH, MT selaku Rektor Universitas Muria Kudus.
3. Bapak Rochmad Winarso, ST, MT, selaku Dekan Fakultas Teknik Universitas Muria Kudus.
4. Bapak Ahmad Jazuli, M.Kom, selaku Ketua Program Studi Teknik Informatika Universitas Muria Kudus.
5. Bapak Mukhamad Nurkamid, S.Kom, M.Cs, selaku pembimbing utama Skripsi penulis.
6. Ibu Tutik Khotimah, M.Kom, selaku pembimbing pembantu Skripsi penulis.
7. Keluarga Gendul TI-A, selaku Keluarga selama Kuliah penulis.
8. Semua pihak yang tidak bisa disebutkan satu persatu.

Semoga beliau-beliau diatas mendapatkan imbalan yang lebih besar dari Tuhan yang maha kuasa melebihi apa yang beliau-beliau diberikan kepada penulis.

Kudus, 16 Februari 2015

Penulis

DAFTAR ISI

Halaman

HALAMAN SAMPUL	i
HALAMAN JUDUL	ii
PENGESAHAN STATUS SKRIPSI.....	iii
PERNYATAAN PENULIS	iv
PERSETUJUAN SKRIPSI	v
PENGESAHAN SKRIPSI	vi
ABSTRACT	vii
ABSTRAK	viii
KATA PENGANTAR	ix
DAFTAR ISI	x
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiv
DAFTAR LAMPIRAN.....	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Batasan Masalah	2
1.3 Rumusan Masalah.....	3
1.4 Tujuan Masalah	3
1.5 Manfaat Penelitian	3
BAB II TINJAUAN PUSTAKA	5
2.1 Penelitian Terkait.....	5
2.2 Landasan Teori	6
2.2.1 Pengertian Kriptografi	6
2.2.2 Algoritma Kriptografi.....	6
2.2.3 Jenis Algoritma Kriptografi	7
2.2.4 Teknik Algoritma Kriptografi Klasik.....	8
2.2.5 Algoritma Kriptografi Klasik Yang Digunakan...	10

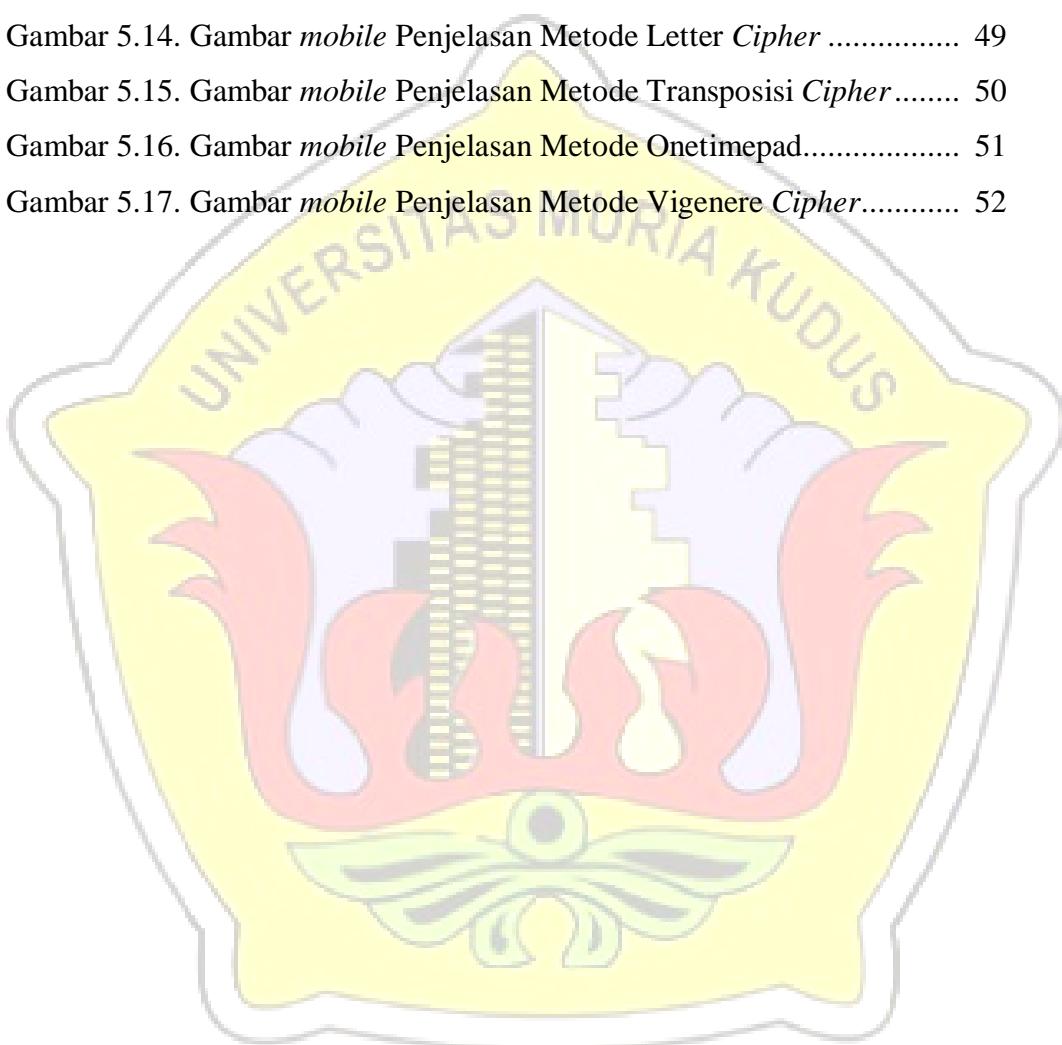
2.2.6	Java	12
2.2.7	Eclipse IDE	14
2.2.8	Sejarah Dan Perkembangan Android	15
2.2.9	<i>Flowchart</i>	17
2.2.9.1	Pengertian <i>Flowchart</i>	17
2.2.9.2	Simbol-Simbol <i>Flowchart</i>	18
2.2.9.3	<i>Flow Direction Symbols</i>	18
2.2.9.4	<i>Processing Symbols</i>	19
2.2.9.5	<i>Input-output Symbols</i>	20
2.3	Kerangka Pemikiran.....	21
BAB III	METODE PENELITIAN	23
3.1	Metode Pengembangan	23
BAB IV	PERANCANGAN SISTEM.....	25
4.1	Perancangan Aplikasi.....	25
4.1.1	Struktur Menu	25
4.1.2	<i>Storyboard</i> Aplikasi.....	25
4.1.3	<i>Flowchart</i> Enkripsi Dan Dekripsi 5 Metode.....	33
BAB V	IMPLEMENTASI DAN TESTING.....	39
5.1	Implementasi User Interface	39
5.2	Algoritma Sistem.....	55
5.3	Pengujian	79
5.3.1	Pengujian BlackBox	79
5.3.2	Perhitungan Manual.....	81
5.3.3	Rekapitulasi Kuisioner	85
BAB VI	PENUTUP	87
6.1	Kesimpulan.....	87
6.2	Saran.....	87

DAFTAR PUSTAKA

DAFTAR GAMBAR

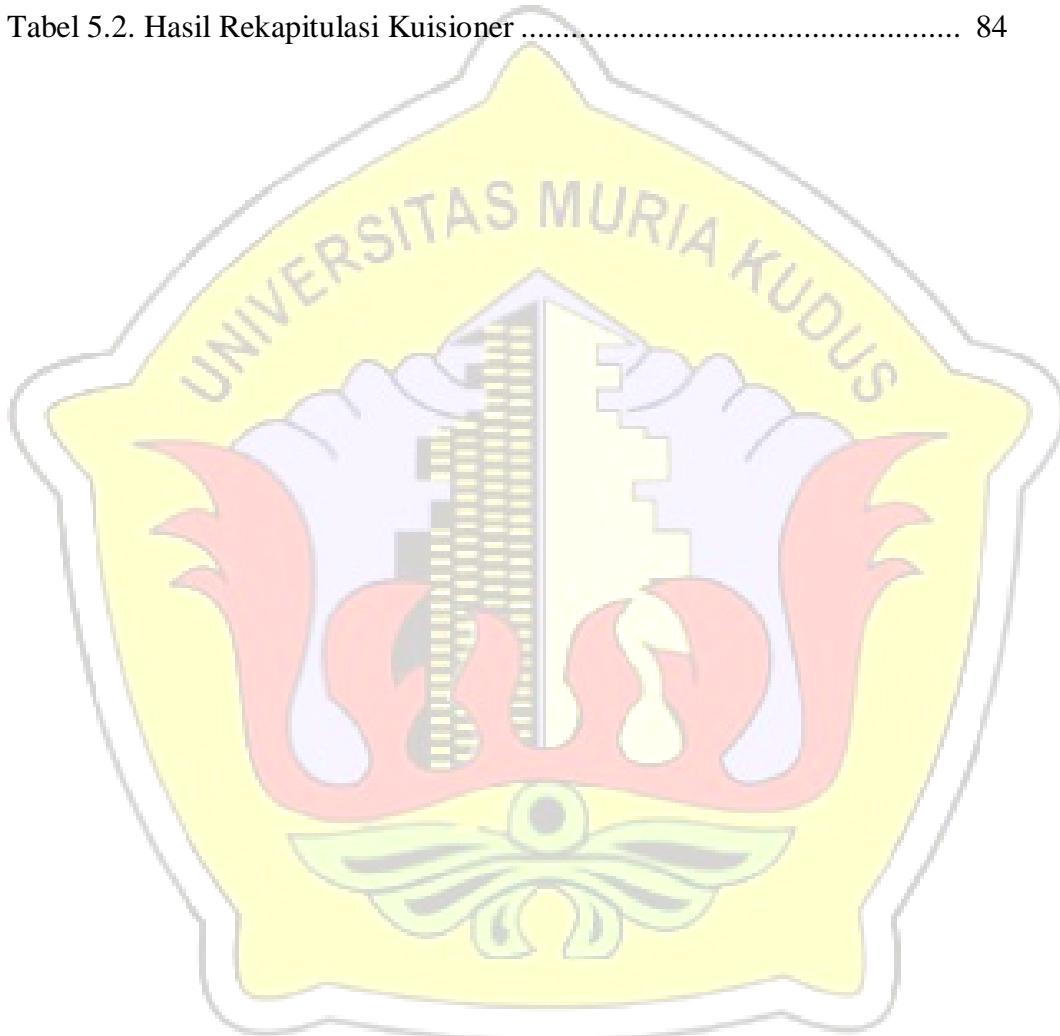
Gambar 2.1. Skema proses enkripsi dekripsi	6
Gambar 2.2. Contoh proses enkripsi dekripsi	6
Gambar 2.3. Contoh teknik Blocking	8
Gambar 2.4. Contoh teknik Permutasi.....	9
Gambar 2.5. Kerangka Pemikiran	20
Gambar 4.1. Bagan Struktur Menu.....	22
Gambar 4.2. <i>Storyboard</i> Menu Utama.....	23
Gambar 4.3. <i>Storyboard</i> Caesar Enkripsi	24
Gambar 4.4. <i>Storyboard</i> Caesar Dekripsi	24
Gambar 4.5. <i>Storyboard</i> Letter Enkripsi.....	25
Gambar 4.6. <i>Storyboard</i> Letter Dekripsi.....	26
Gambar 4.7. <i>Storyboard</i> Transposisi Enkripsi	26
Gambar 4.8. <i>Storyboard</i> Transposisi Dekripsi	27
Gambar 4.9. <i>Storyboard</i> Onetimepad Enkripsi	28
Gambar 4.10. <i>Storyboard</i> Onetimepad Dekripsi	28
Gambar 4.11. <i>Storyboard</i> Vigenere Enkripsi	29
Gambar 4.12. <i>Storyboard</i> Vigenere Dekripsi	30
Gambar 4.13. <i>Flowchart</i> Enkripsi dan Dekripsi Caesar <i>cipher</i>	31
Gambar 4.14. <i>Flowchart</i> Enkripsi dan Dekripsi Letter <i>cipher</i>	32
Gambar 4.15. <i>Flowchart</i> Enkripsi dan Dekripsi Transposisi <i>cipher</i>	33
Gambar 4.16. <i>Flowchart</i> Enkripsi dan Dekripsi Onetimepad.....	34
Gambar 4.17. <i>Flowchart</i> Enkripsi dan Dekripsi Vigenere <i>Cipher</i>	35
Gambar 5.1. Gambar <i>mobile</i> Menu Utama	36
Gambar 5.2. Gambar <i>mobile</i> Caesar Enkripsi.....	37
Gambar 5.3. Gambar <i>mobile</i> Caesar Dekripsi.....	38
Gambar 5.4. Gambar <i>mobile</i> Letter Enkripsi	39
Gambar 5.5. Gambar <i>mobile</i> Letter Dekripsi	40
Gambar 5.6. Gambar <i>mobile</i> Transposisi Enkripsi.....	41
Gambar 5.7. Gambar <i>mobile</i> Transposisi Dekripsi	42

Gambar 5.8. Gambar <i>mobile</i> Onetimepad Enkripsi.....	43
Gambar 5.9. Gambar <i>mobile</i> Onetimepad Dekripsi	44
Gambar 5.10. Gambar <i>mobile</i> Vigenere Enkripsi	45
Gambar 5.11. Gambar <i>mobile</i> Vigenere Dekripsi	46
Gambar 5.12. Gambar <i>mobile</i> About.....	47
Gambar 5.13. Gambar <i>mobile</i> Penjelasan Metode Caesar <i>Cipher</i>	48
Gambar 5.14. Gambar <i>mobile</i> Penjelasan Metode Letter <i>Cipher</i>	49
Gambar 5.15. Gambar <i>mobile</i> Penjelasan Metode Transposisi <i>Cipher</i>	50
Gambar 5.16. Gambar <i>mobile</i> Penjelasan Metode Onetimepad.....	51
Gambar 5.17. Gambar <i>mobile</i> Penjelasan Metode Vigenere <i>Cipher</i>	52



DAFTAR TABEL

Tabel 2.1. <i>Flow Direction Symbol</i>	18
Tabel 2.2. <i>Processing Symbol</i>	18
Tabel 2.3. <i>Input-output Symbol</i>	19
Tabel 5.1. Hasil Pengujian aplikasi	77
Tabel 5.2. Hasil Rekapitulasi Kuisioner	84



DAFTAR LAMPIRAN

Lampiran I : Lembar Konsultasi Skripsi

Lampiran II : Lembar Revisi Ujian Skripsi

Lampiran III : Kuisioner

