

**APLIKASI MOBILE UNTUK ENKRIPSI DATA GAMBAR  
MENGUNAKAN KOMBINASI FUNGSI XOR DAN  
MODE OPERASI CBC**

**Skripsi**

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



Disusun oleh

**Jannatun Aliyah**

**07.11.1522**

**JURUSAN TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER  
AMIKOM  
YOGYAKARTA  
2011**

**PERSETUJUAN**

**SKRIPSI**

**Aplikasi Mobile untuk Enkripsi Data Gambar  
Menggunakan Kombinasi Fungsi XOR dan  
Mode Operasi CBC**


yang dipersiapkan dan disusun oleh

**Jannatun Aliyah**

**07.11.1522**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 16 Oktober 2010

**Dosen Pembimbing,**



**Andi Sunyoto / M.Kom**

**NIK. 190302052**

PENGESAHAN

**SKRIPSI**

**Aplikasi Mobile untuk Enkripsi Data Gambar  
Menggunakan Kombinasi Fungsi XOR dan  
Mode Operasi CBC**

Yang dipersiapkan dan disusun oleh

**Jannatun Aliyah**

**07.11.1522**

telah dipertahankan di depan Dewan Penguji  
pada tanggal 15 Maret 2011

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**


**Andi Suyoto, M.Kom  
NIK. 190302052**



**Drs. Bambang Sudaryatno, MM  
NIK. 190302029**



**Armadyah Amborewati, S.Kom., M.Eng.  
NIK. 190302063**



Skripsi ini telah diterima sebagai salah satu persyaratan  
Untuk memperoleh gelar Sarjana Komputer

Tanggal 15 Maret 2011

**KETUA STMIK AMIKOM YOGYAKARTA**



**Prof. Dr. M. Suyanto, M.M.**

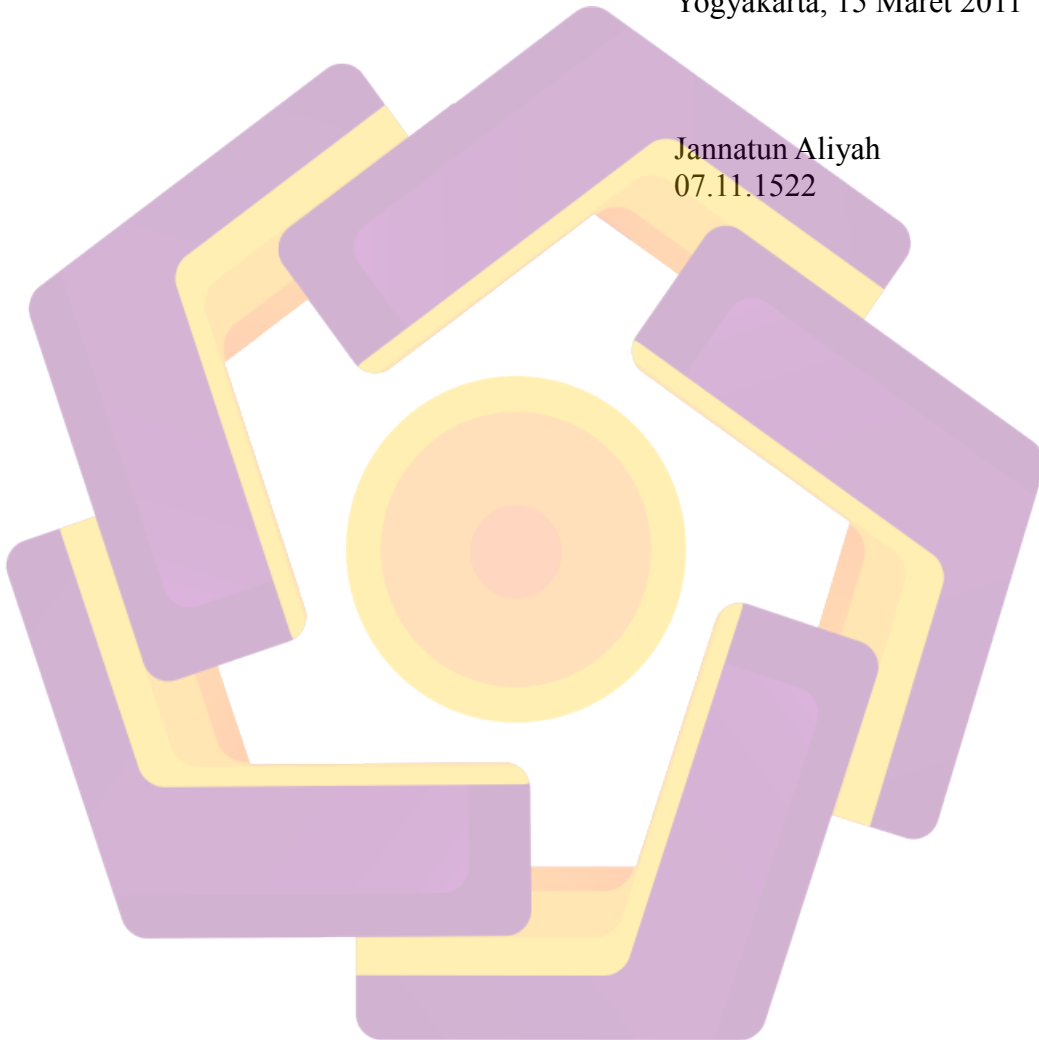
**NIK. 190302001**

**PERNYATAAN**

Saya yang bertandatangan dibawah 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, 15 Maret 2011

Jannatun Aliyah  
07.11.1522



## MOTTO DAN PERSEMBAHAN

### MOTTO :

*Kita tidak bisa menjadi bijaksana dengan kebijaksanaan orang lain, tetapi kita bisa berpengetahuan dengan pengetahuan orang lain (Michel De Moutaigne),,,*

*Kebahagiaan akan terasa nyata bila kita membagikannya kepada orang lain (Christoper Johnson Mccandless),,,*

*Kebaikanmu hari ini adalah coretan cita-cita kehidupanmu untuk masa depanmu,,,*

*Keberanian sejati adalah berani mengevaluasi kekurangan diri sendiri,,,*



**PERSEMBAHAN :**

- ☺ **My God "ALLAH S.W.T" ,,,**
- ☺ *My Beloved Family,,, Bapak (alm) , Ibu ("My inspiration in the life") and My Sister "Nindy" (terima kasih atas doanya selama ini),,,*
- ☺ *For my big Family who have supported Me,,, thanks All,,*
- ☺ *Special for My Lovely "NtaQ" (terima kasih telah memberikan motivasi, dukungan dan selalu setia menemaniku selama ini),,,*
- ☺ *Kawan-kawan belajar kelompok "B\*K\*R Is Nice" Xixixi,,, Terima kasih, kalian sumber inspirasiku di bidang IT, hehe,,,*
- Kawan-kawan "Kost Pondok Biru" :*
- ☺ *Rhe "kak Imoet" dan Rully Ae "Mb' Syukur" (sahabat seperjuangan di kampus, di kost (kawan sesama koki, xixix,,) dan di jalan (kapan neh jalan2 lg??)),*
- ☺ *Nindy (adikku tersayang),, muuph sudah mengganggu kenyamanan belajarmu,, thanks pinjaman kamarnya,,hehe,,*

- 😊 Wulan “Bu RT”, Vivin “De’ Bro” dan Cici Magelang “Xixix,,  
mank nasi goreng” (thanks support dan bantuan  
fasilitasnya serta kekonyolan yang tiada akhir),
- 😊 ibu2 Bidan “Utari, Niken, Lestari, Tina(Wahyu, xixixi,,)”  
thanks vitamin dan tensi darahnya yg gratisssss,, xixixi,,
- 😊 Mb’ Adis (Sebelah kamar yg baik hati, thanks winamp2 nya  
yg menghibur hati, hehe),
- 😊 Mitha, Wiwin, Anis, thanks masukannya buat skripsiku,  
😊 Wuri, De’ Arum, De’ Lisa, De’ Grace, De’ Aul,,  
thanks semuanya, kalian telah mengisi hari-hariku dikost  
menjadi lebih berwarna, hehehe,,



## KATA PENGANTAR

Puji syukur penulis panjatkan kehadiran Allah SWT yang telah memberikan limpahan rahmat, karunia dan petunjuk-Nya kepada penulis, sehingga penulis dapat menyelesaikan penyusunan skripsi yang berjudul “Aplikasi Mobile untuk enkripsi Data Gambar Menggunakan Kombinasi Fungsi XOR dan Mode Operasi CBC”. Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana Komputer Jurusan Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer Amikom Yogyakarta.

Penulisan skripsi ini banyak pihak yang telah memberikan bimbingan, arahan, dan motivasi, karenanya tak lupa penulis mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, M.M., selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
2. Bapak Andi Sunyoto, M.Kom., selaku pembimbing yang telah memberikan saran, masukan, dan bimbingan selama pelaksanaan penelitian hingga terselesaikannya skripsi ini.
3. Bapak Drs. Bambang Sudaryatno, MM dan Ibu Armadyah Amborowati, S.Kom., M.Eng., terima kasih atas kritik dan saran yang diberikan sebagai dosen penguji.
4. Bapak Ir. Abas Ali Pangera, M.Kom, selaku ketua Jurusan Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
5. Bapak Emha Taufik Luthfi, ST, M.Kom., Bapak M. Rudiyanto Arief, MT, dan Bapak Dony Ariyus, M.Kom., yang telah membagikan ilmunya sehingga skripsi ini dapat terselesaikan oleh penulis.



6. Seluruh dosen Jurusan Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta yang telah membimbing dan membagikan ilmunya selama kuliah kepada penulis.
7. Kedua orang tuaku (Bapak Muhammad HA (alm) dan Ibu Sahemah, S.Sos), adikku (Nadratun Nikmah) serta seluruh keluarga penulis yang telah memberikan dukungan, dorongan, bantuan dan cinta kasih yang tiada henti.
8. Rekan-rekan S1TI\_C 2007, terima kasih telah memberikan semangat, dukungan serta pengalaman yang indah dan berharga selama proses belajar di bidang ilmu teknik informatika Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
9. Semua pihak yang tidak bias disebutkan satu persatu, yang telah memberikan bantuannya hingga terselesaikannya skripsi ini.

Sebagaimana pepatah mengatakan bahwa tiada gading yang tak retak, penulis menyadari masih banyak kekurangan dalam penelitian dan skripsi ini. Semoga penelitian ini memberikan manfaat bagi perkembangan ilmu pengetahuan, khususnya dalam bidang Aplikasi Mobile.

Yogyakarta, Maret 2011

Penulis

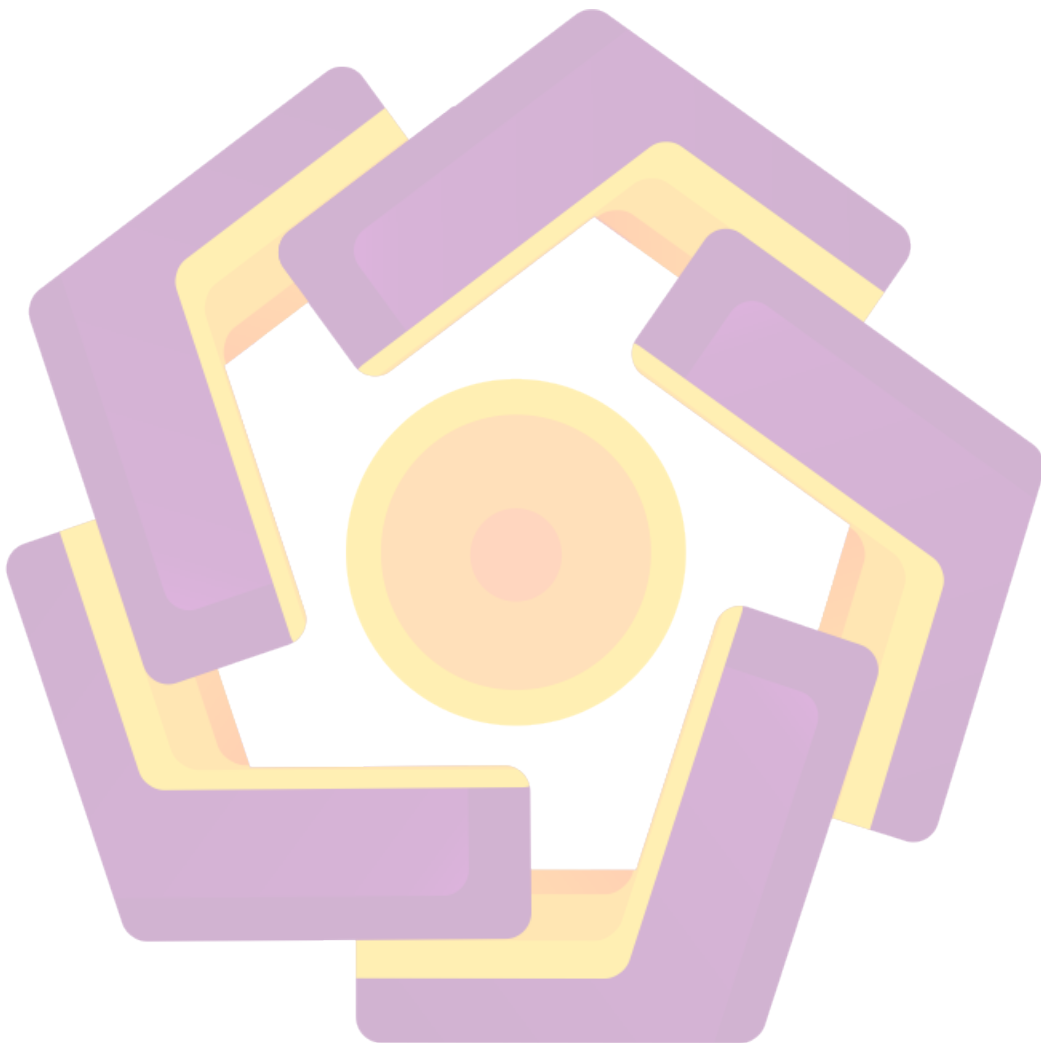
## DAFTAR ISI

Judul .....	i
Lembar Persetujuan .....	ii
Lembar Pengesahan .....	iii
Lembar Pernyataan .....	iv
Motto dan Persembahan .....	v
Kata Pengantar .....	viii
DAFTAR ISI .....	x
DAFTAR TABEL .....	xiii
DAFTAR GAMBAR .....	xiv
DAFTAR SINGKATAN .....	xv
I    PENDAHULUAN .....	1
1.1    Latar Belakang .....	1
1.2    Rumusan Masalah .....	2
1.3    Batasan Masalah .....	3
1.4    Tujuan Penelitian .....	3
1.5    Manfaat Penelitian .....	4
1.6    Metode Penelitian .....	4
1.7    Sistematika Penulisan Skripsi.....	5

II	LANDASAN TEORI .....	7
2.1	Pemrograman Java .....	7
2.1.1	Bahasa Pemrograman Java .....	7
2.1.2	IDE Netbeans .....	8
2.1.3	Java 2 MicroEdition .....	9
2.1.3.1	Konfigurasi J2ME .....	10
2.1.3.2	Profile J2ME .....	12
2.1.3.3	MIDP .....	13
2.1.3.4	RMS .....	13
2.1.4	Bouncy Castle Cryptography API.....	14
2.1.5	Diagram Model Use Case .....	15
2.1.6	Diagram Kelas .....	16
2.1.7	Diagram Sequence.....	18
2.2	Kriptografi .....	19
2.2.1	Keamanan Data .....	19
2.2.2	Definisi Kriptografi .....	20
2.2.3	Algoritma Kriptografi .....	25
2.2.3.1	Kriptografi dengan Fungsi XOR .....	27
2.2.3.2	Mode Operasi CBC .....	27
2.2.4	Tujuan Kriptografi.....	29
III	ANALISIS DAN PERANCANGAN SISTEM .....	30
3.1	Kebutuhan Sistem .....	30

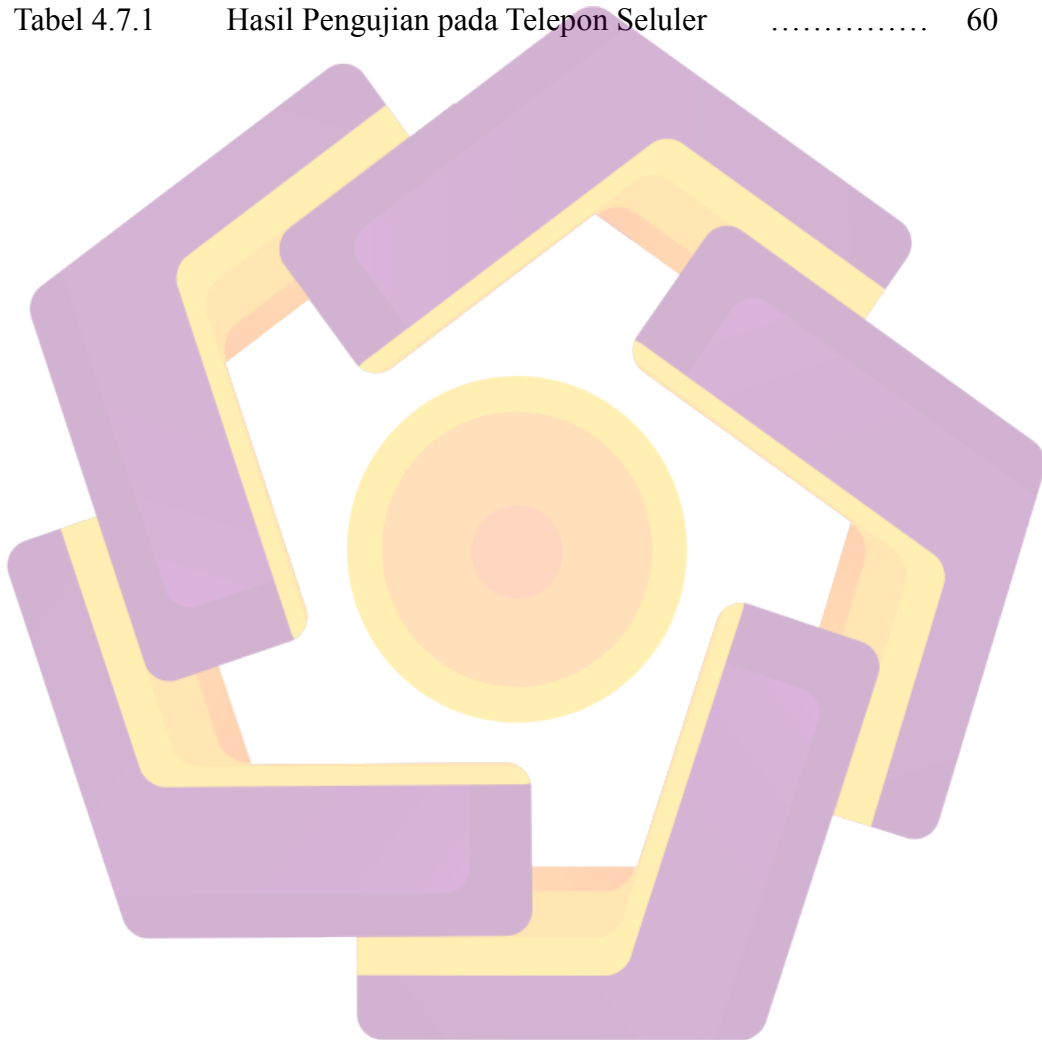
3.2	Aliran Kerja Analisa .....	31
3.2.1	Fungsional Modeling .....	32
3.2.2	Entity Class Modeling .....	33
3.2.3	Interaction Modeling .....	34
3.3	Aliran Kerja Desain .....	38
3.3.1	Rancangan Form Menu Utama .....	38
3.3.2	Rancangan Form Confirm.....	39
3.3.3	Rancangan Form Penyandian Gambar .....	40
3.3.4	Rancangan Form Encrypt dan Form Decrypt .....	41
3.3.5	Rancangan Form File Encrypt dan Form File Decrypt .....	43
3.3.6	Rancangan Form Gallery .....	45
IV	IMPLEMENTASI DAN PEMBAHASAN .....	46
4.1	Implementasi Antar Muka .....	46
4.1.1	Antar Muka Menu Utama .....	47
4.2	Aplikasi CryptoImage.....	52
4.3	Input Data Gambar .....	54
4.4	Kelas Save .....	54
4.5	Kelas Gambar .....	56
4.6	Kelas Kriptografi .....	57
4.6.1	Enkripsi Data Gambar .....	57
4.6.2	Dekripsi Data Gambar .....	58
4.7	Instalasi MIDlet ke Dalam Telepon Seluler .....	58

4.8	Uji Coba Aplikasi .....	59
V	PENUTUP .....	64
5.1	Kesimpulan .....	64
5.2	Saran .....	64
	DAFTAR PUSTAKA .....	66
	LAMPIRAN	



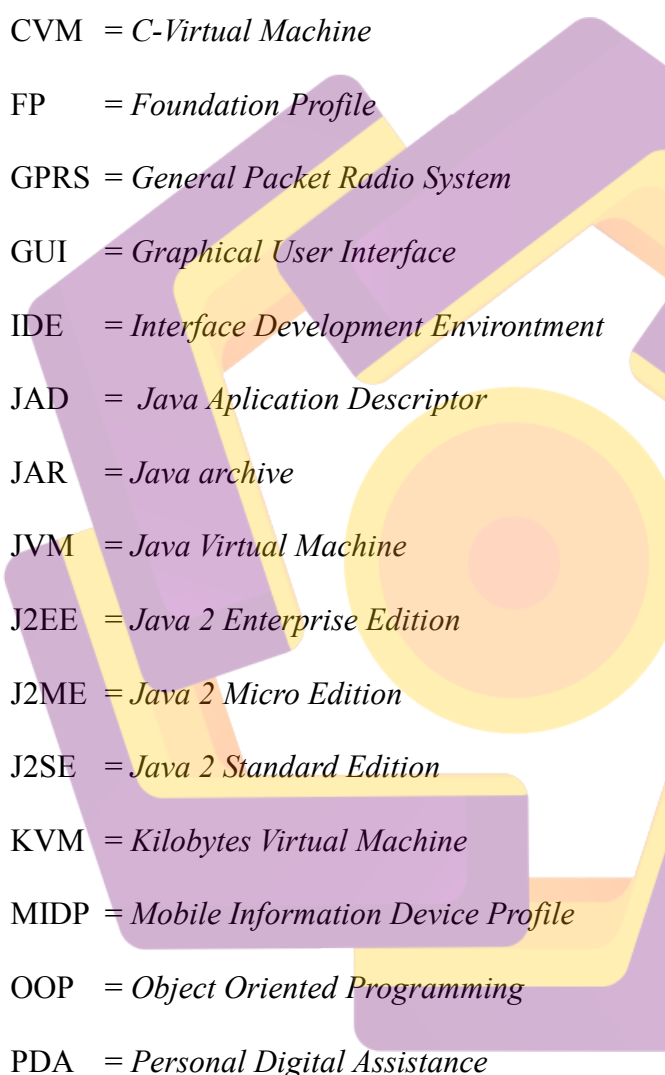
**DAFTAR TABEL**

Tabel 2.1.3.1	J2ME Secara Umum	.....	9
Tabel 2.1.3.1.1	Perbandingan antara CLDC dan CDC	.....	11
Tabel 2.1.4.1	Notasi Use Case Diagram	.....	15
Tabel 2.2.3.1.1	Fungsi XOR.....	.....	27
Tabel 4.2.1	Kelas Aplikasi CryptoImage	.....	53
Tabel 4.7.1	Hasil Pengujian pada Telepon Seluler	.....	60



## DAFTAR GAMBAR

Gambar 2.1.6.1	Contoh Diagram Kelas .....	17
Gambar 2.1.7.1	Contoh Diagram Sequence .....	19
Gambar 2.2.2.1	Pohon Kriptologi .....	24
Gambar 2.2.3.1	Skema Enkripsi dan Dekripsi menggunakan Kunci	26
Gambar 2.2.3.2	Ilustrasi Enkripsi dan Dekripsi terhadap Pesan ...	26
Gambar 2.2.3.2.1	Skema Enkripsi dan Dekripsi dengan Mode CBC	28
Gambar 3.2.1.1	Use Case Diagram .....	32
Gambar 3.2.2.1	Class Diagram.....	33
Gambar 3.2.3.1	Sequence Diagram Enkripsi Gambar.....	35
Gambar 3.2.3.2	Sequence Diagram Dekripsi Gambar.....	37
Gambar 3.3.1	Rancangan Form Menu Utama .....	38
Gambar 3.3.2	Rancangan Form Confirm .....	39
Gambar 3.3.3	Rancangan Form Penyandian Gambar .....	40
Gambar 3.3.4.1	Rancangan Form Encrypt .....	41
Gambar 3.3.4.2	Rancangan Form Decrypt .....	42
Gambar 3.3.5.1	Rancangan Form File Encrypt .....	43
Gambar 3.3.5.2	Rancangan Form File Decrypt .....	44
Gambar 3.3.6	Rancangan Form Gallery .....	45
Gambar 4.1.1	Tampilan Antar Muka Menu Utama .....	47

**DAFTAR SINGKATAN**

AMS	=	<i>Application Management Software</i>
API	=	<i>Application Programming Interface</i>
CBC	=	<i>Cipherblock Chaining</i>
CDC	=	<i>Connected Devide Configuration</i>
CLDC	=	<i>Connected Limited Device Configuration</i>
CVM	=	<i>C-Virtual Machine</i>
FP	=	<i>Foundation Profile</i>
GPRS	=	<i>General Packet Radio System</i>
GUI	=	<i>Graphical User Interface</i>
IDE	=	<i>Interface Development Environment</i>
JAD	=	<i>Java Application Descriptor</i>
JAR	=	<i>Java archive</i>
JVM	=	<i>Java Virtual Machine</i>
J2EE	=	<i>Java 2 Enterprise Edition</i>
J2ME	=	<i>Java 2 Micro Edition</i>
J2SE	=	<i>Java 2 Standard Edition</i>
KVM	=	<i>Kilobytes Virtual Machine</i>
MIDP	=	<i>Mobile Information Device Profile</i>
OOP	=	<i>Object Oriented Programming</i>
PDA	=	<i>Personal Digital Assistance</i>
RMS	=	<i>Record Management System</i>



## INTISARI

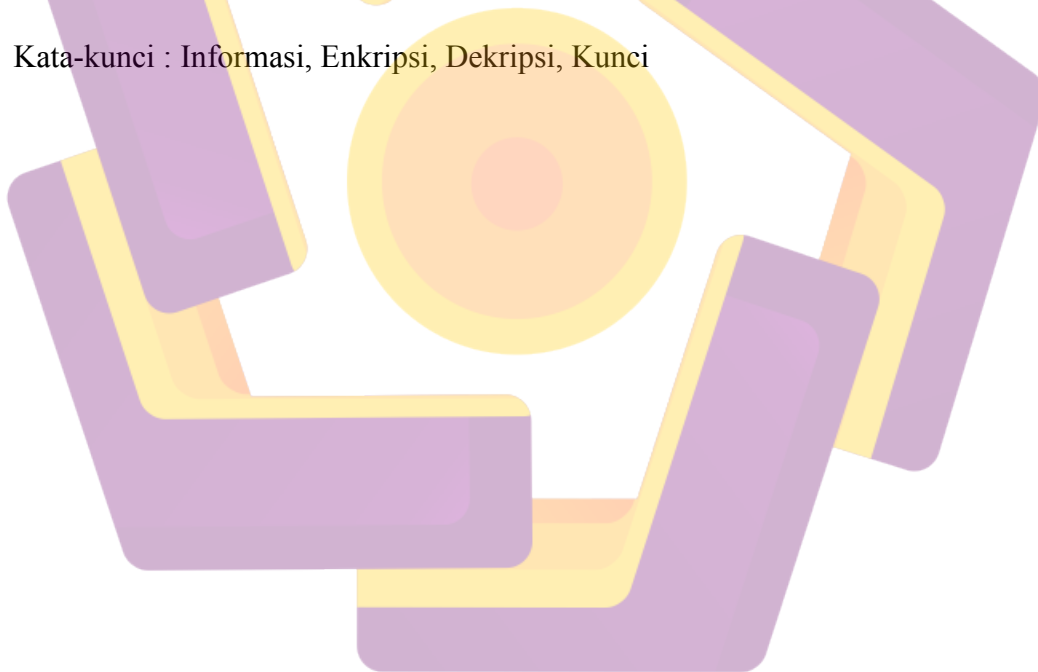
Dalam skripsi ini akan memaparkan cara pembuatan aplikasi kriptografi dan mengimplementasikan model enkripsi pada image atau data gambar. Tujuannya untuk keamanan pada penyimpanan file gambar. Proses enkripsi pada gambar akan menghasilkan hasil enkripsi yang dapat merahasiakan gambar. Sebaliknya, proses dekripsi akan mengembalikan gambar yang dirahasiakan tersebut kembali menjadi gambar aslinya.

Metode yang digunakan dalam enkripsi dan dekripsi data gambar ini adalah kombinasi fungsi XOR dan mode operasi CBC (Cipherblock Chaining). Dimana enkripsi yang dilakukan pertama kali dengan fungsi XOR kemudian dilanjutkan dengan enkripsi menggunakan mode operasi CBC. Mengkombinasikan fungsi XOR dengan mode CBC bertujuan untuk meningkatkan keamanan data gambar sehingga kriptanalisis menjadi lebih sulit untuk menampilkan plaintext (gambar aslinya).

Dalam pembuatan aplikasi *CryptoImage* ini menggunakan Netbeans 6.5 yang merupakan salah satu aplikasi Integrated Development Environment (IDE) Java. Aplikasi ini digunakan khusus untuk mengembangkan program java.

Dalam Netbeans 6.5 ini, untuk aplikasi mobile menggunakan Java 2 Platform, Micro Edition (J2ME). Ketersediaan fasilitas kriptografi pada platform J2ME ini memungkinkan kita untuk memanipulasi data-data agar kerahasiaannya bisa terjaga.

Kata-kunci : Informasi, Enkripsi, Dekripsi, Kunci



## ABSTRACT

In this paper will explain how making the application of cryptography and implement encryption model in image or picture data. The goal for the security of the image file storage. The process of encryption on the picture will produce results that can keep the image encryption. Conversely, the decryption process will restore the image that is re-classified into the original image.

The method used in encryption and decryption of data this figure is a combination of XOR function and CBC operation mode (Cipherblock Chaining). Where encryption is performed first with XOR function was followed by encryption using CBC mode of operation. Combining XOR function with CBC operation mode aims to improve the security of image data, so that kriptanalisis become more difficult to display the plaintext (the original picture).

In making this CryptoImage application using NetBeans 6.5 which is one application Integrated Development Environment (IDE) Java. This application is used specifically to develop a Java program.

In Netbeans 6.5, for mobile applications using Java 2 Platform, Micro Edition (J2ME). The availability of cryptographic facility on J2ME platform allows us to manipulate the data for confidentiality can be guaranteed.

**Keywords :** *Information, Encryption, Decryption, Key*

