APLIKASI MOBILE UNTUK ENKRIPSI DATA GAMBAR MENGGUNAKAN 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 Sunyoto, M.Kom **NIK. 190302052**	
Drs. Bambang Sudaryatno, MM **NIK. 190302029**	
Armadyah Amborowati, 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 menggangu 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 winamp2nya 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 kehadirat Allah SWT yang telah memberikan limpahan rahmat, karunia dan petunjuk-Nya kepada penulis, sehingga penulis dapat menyelesikan 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.

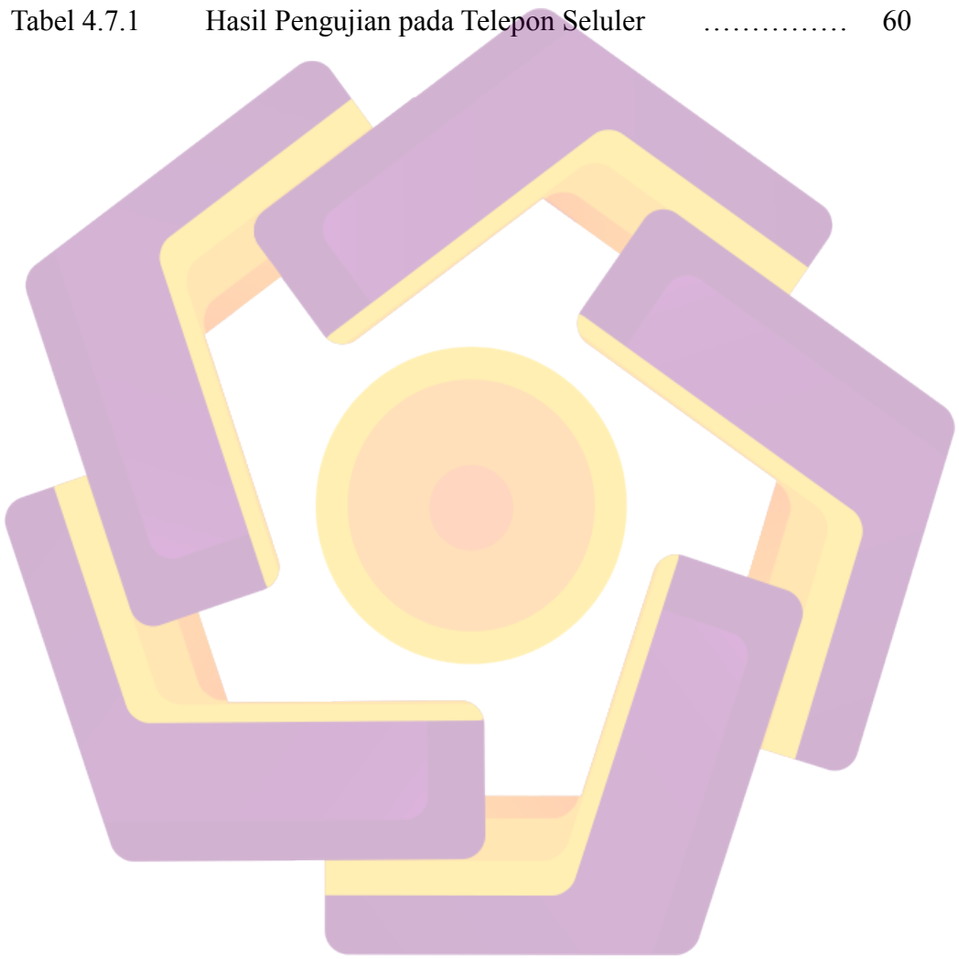
Sebagaimana pepatah mengatakan bahwa tiada gading yang tak retak, penulis menyadari masih banyak kekurangan dalam penelitian dan skripsi ini. Semoga penelitian ini memberikan manfaat bagi perkembangan ilmu pengetahuan, khususnya dalam bidang Aplikasi Mobile.

Yogyakarta, Maret 2011

Penulis

DAFTAR ISI

DAFTAR TABEL



DAFTAR GAMBAR

DAFTAR SINGKATAN

AMS = *Application Management Software*

API = *Application Programming Interface*

CBC = *Cipherblock Chaining*

CDC = *Connected Devide Configuration*

CLDC = *Connected Limited Device Configuration*

CVM = *C-Virtual Machine*

FP = *Foundation Profile*

GPRS = *General Packet Radio System*

GUI = *Graphical User Interface*

IDE = *Interface Development Environtment*

JAD = *Java Aplication Descriptor*

JAR = *Java archive*

JVM = *Java Virtual Machine*

J2EE = *Java 2 Enterprise Edition*

J2ME = *Java 2 Micro Edition*

J2SE = *Java 2 Standard Edition*

KVM = *Kilobytes Virtual Machine*

MIDP = *Mobile Information Device Profile*

OOP = *Object Oriented Programming*

PDA = *Personal Digital Assistance*

RMS = *Record Management System*

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 kriptanalis 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 terjamin.

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 imahe 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 kriptanalis 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 isused 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*