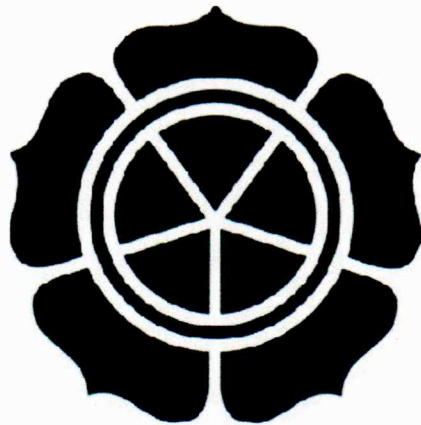


**ENKRIPSI SMS MENGGUNAKAN ADVANCED ENCRYPTION
STANDARD PADA J2ME DENGAN BANTUAN BOUNCY CASTLE
CRYPTOGRAPHY API**

SKRIPSI



disusun oleh
Eli Pujastuti
07.11.1620

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

**ENKRIPSI SMS MENGGUNAKAN ADVANCED ENCRYPTION
STANDARD PADA J2ME DENGAN BANTUAN BOUNCY CASTLE
CRYPTOGRAPHY API**

Skripsi

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



disusun oleh :

Eli Pujastuti

07.11.1620

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

PERSETUJUAN

SKRIPSI

**Enkripsi SMS Menggunakan Advanced Encryption Standard pada J2ME
dengan Bantuan Bouncy Castle Cryptography API**

yang dipersiapkan dan disusun oleh

Eli Pujastuti

07.11.1620

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 17 Februari 2011

Dosen Pembimbing


Emha Taufiq Luthfi, ST, M.Kom
NIK. 190302125

PENGESAHAN

SKRIPSI

**Enkripsi SMS Menggunakan Advanced Encryption Standard pada J2ME
dengan Bantuan Bouncy Castle Cryptography API**

yang dipersiapkan dan disusun oleh

Eli Pujastuti

07.11.1620

telah dipertahankan di depan Dewan Penguji
pada tanggal 15 Maret 2011

Susunan Dewan Penguji

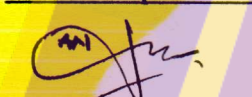
Nama Penguji

**Kusnawi, S.Kom., M.Eng
NIK. 190302112**

**Sudarmawan, MT.
NIK. 190302035**

**Arief Setyanto, S.Si., MT.
NIK. 190302036**

Tanda Tangan



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

Tanggal 15 Maret 2011

KETUA STMIK AMIKOM, YOGYAKARTA



Prof. Dr. M. Suvanto, M.M.

NIK. 19030200

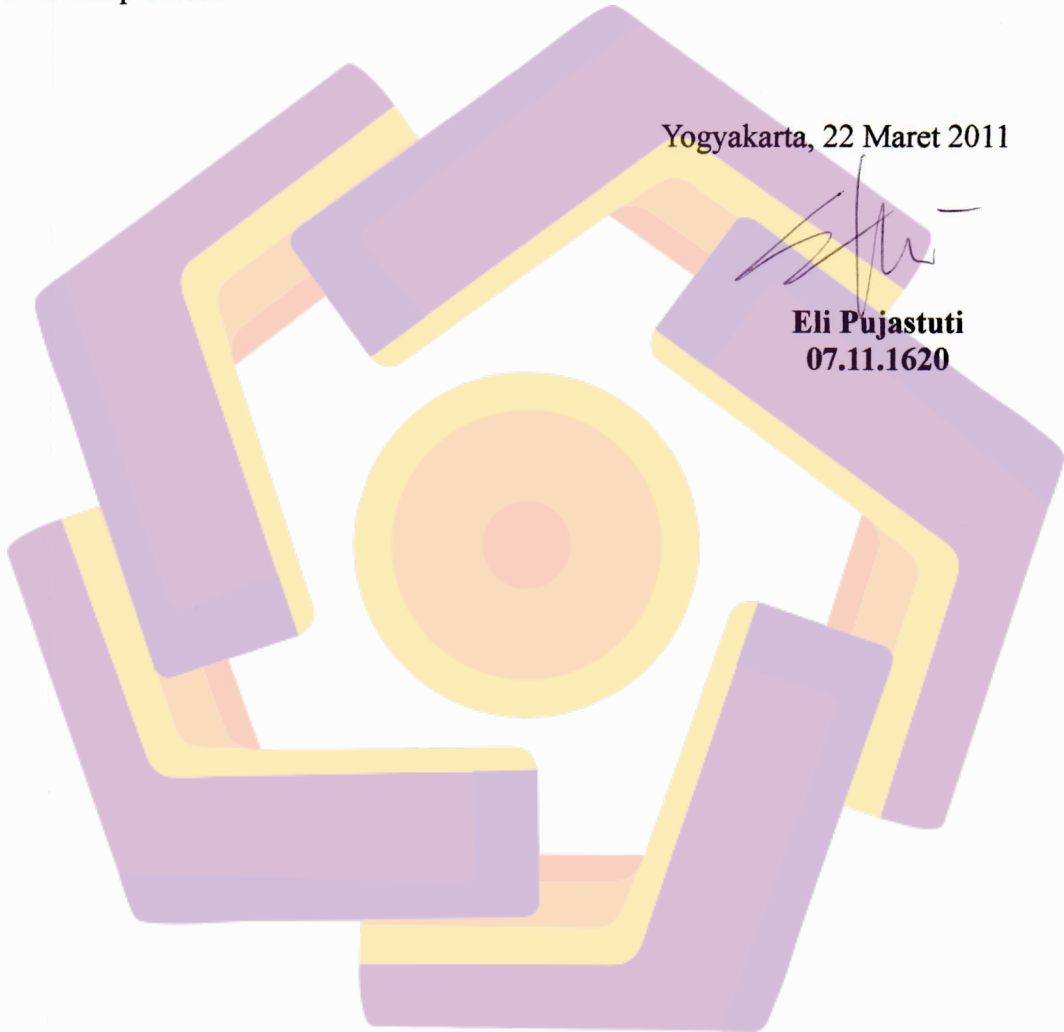
PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa, Skripsi ini merupakan karya sendiri (ASLI), dan isi dalam Skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain atau kelompok lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan kami juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain atau kelompok laon, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 22 Maret 2011



Eli Pujastuti
07.11.1620



HALAMAN MOTTO

"Terkadang bayangan kita lebih menakutkan dibanding kenyataan yang sebenarnya belum kita hadapi" 😊

"Pentingnya Persepsi dan Cara Kita Berpikir tentang sesuatu. sangat berpengaruh terhadap respon emosional, perilaku dan psikologis terhadap sesuatu itu sendiri (Dwi Iriyanto)" 😊

"Bila kamu takut akan sesuatu maka masuklah dalam sesuatu yang menakutimu itu, karena rasa takutmu lebih berbahaya dari apa yang kamu takutkan" 😊

"Selalu berusaha merubah batu sandungan menjadi batu pijakan, merubah halangan menjadi peluang, dan merubah kekalahan menjadi kemenangan yang tertunda" 😊

HALAMAN PERSEMBAHAN

Segala Puji hanya untuk Allah, yang Maha mengetahui apa-apa yang ada dilangit dan dibumi, yang telah mempersatukan hati kita sehingga dengan karunia-Nya kita bersaudara. Allah yang selalu memberikan apa yang terbaik bagi hambanya dengan cinta yang tiada tara. Penulis ingin mempersembahkan skripsi ini kepada orang-orang yang senantiasa mendukung dengan penuh senyum kepercayaan:

- ❖ **Ibu Ris Sumijarsih dan Bapak Suwanto, B.sc**, yang sangat aku cintai dan mencintai aku. Terimakasih untuk dukungan sempurna menurutku, yang telah Ibu & Bapak berikan. Love u mom,, love u dad ,, ♡
- ❖ **Saudara-saudaraku Wartyo's Fam yang aku sayangi**. Mbak endah partiningsih [jika aku sukses, itu semua tidak terlepas dari mu mbak dan aku berjanji akan berusaha membalas kebaikanmu], Mas heru [makasih untuk leptopnya mas ^^], Mas Iwan [makasih dan maaf mas], Mas Antok [terus memberikan ide-ide mu ya mas... meskipun kita sering bersebrangan pendapat, namun itulah yang akan aku rindukan], Mbak Endra [nuwun yo ndrut,, kamu teknisi printer yang OK haha], Dek Hasti [maap ya gara2 aku mau pendadaran, km jadi dimarahin waktu bersin didepanku ☺hihi], Dek Nurul [kita sama-sama berjuang ul.. ☺].
- ❖ **Sahabat-sahabatku yang aku sayangi**, Sahabat adie [kita memang berperang tanpa senjata sahabat, tapi kita punya keyakinan yang membawa kita pada hal yang tidak terduga, makasih sahabat ☺], Merrita Dewi [pilihan hidup yang memisahkan, tp persahabatan tetap menyatu, makasih sahabatku].
- ❖ **D'kids n Crew**, Arie [akan aku rindukan "nyekak" kita ☺], Rini [nuwun yo mbok.. ☺], Yoga [jangan lupakan mitos ayam bebeg di dnc.. ☺], Andre [tetep setia seperti itu aja ndre,,], Dani [semangatmu menginspirasi ku bug..], Sari [moga tetep jadi ibu indra p. yang baik ☺], Sumijan[nuwun pakde], Cahyo [ayo ndang nyusul..] → kalian adalah sahabat2 terbaikku di kampus ungu ini love u guys.
- ❖ **Student Staff Humas**, didi [ayo kita "ngedance" di ci**a lagi], aji ["ngedance" adalah hal yang paling akan ku rindukan haha], ayu [semoga kamu bisa berlatih memanggilku eli bukan umi T.T], lela [tetep jadi lela yang dewasa bug, seperti itu], fadya [u re best boz], feby wibisono [thx karna udah dengerin keluhan waktu ngejar acc.. thx 4 ur gud solution brada], novan [u re awesome, your fans here ☺], reiza [smoga tetep jadi ustad b.arab kita yang paling baik, hihi], olive [jangan ngambil makanan sisa kunjungan lagi yaa.. piss], igga [begadang jangan begadang ☺], neyna [narsis dimana aja ok.haha], Yuliana [smoga bisa terus exist di ss ya], ibu-ibu CS: mbak devi, lista, ulfa [tetep kompak ya my sista] → thanks SS untuk jiwa professional yang aku pelajari dari kalian.
- ❖ **Dosen-dosen ganteng**, Pak Emha Taufiq Luthfi, ST, M.Kom [makasih pak untuk kesabarannya membimbing mahasiswamu yang bandel ini], Pak Erik Hadi Saputra, S.Kom, M.Eng. [makasih untuk motifasi, inspirasi, dan kesempatan yang telah diberikan], Pak Kusnawi, S.Kom, M. Eng [makasih untuk nilai maksimalnya pak ☺], Pak Dony Arius [makasih untuk ilmu kriptografinya pak], Pak Ratno Kutiawan [makasih pak sudah banyak membantu di awal].

- ❖ **My Dear, MASyaif.** [thankz dukungan dan doa nya yah.. ada saat-saat dalam hidup ini ketika seperti api dan kayu, ☺]
- ❖ **Teman-teman yang melengkapiku,** Suhendri [makasih my bro, untuk niat yang baik untuk terus membantuku], S1-Teknik Informatika D'07 [makasih teman-teman, karena kalianlah aku bisa terus berjuang,], noni, dimas, dwi, widya [makasih udah nemenin aku waktu pendadaran] → kalian melengkapiku



KATA PENGANTAR

Assalaamu'alaykum Warahmatullahi Wabarakaatu

Alhamdulillah, Puji Syukur kehadiran Allah SWT yang telah melimpahkan rahmat, hidayah dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan skripsi ini yang diberi judul “ENKRIPSI SMS MENGGUNAKAN ADVANCED ENCRYPTION STANDARD PADA J2ME DENGAN BANTUAN BOUNCY CASTLE CRYPTOGRAPHY API”.

Laporan skripsi ini disusun sebagai syarat kelulusan di Sekolah Tinggi Manajemen Informatika dan Komputer “AMIKOM” Jurusan Teknik Informatika. Laporan ini dimaksudkan untuk memberikan kesempatan pada mahasiswa agar melihat, mengamati, membandingkan, menganalisis, serta menerapkan pengetahuan yang diperoleh diperkuliahan.

Dalam penyusunan skripsi ini, penulis tidak terlepas dari berbagai pihak yang telah rela membantu baik moril maupun materil yang dapat membuat penulis selalu optimis. Maka dari itu, sebagai rasa hormat penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Kedua Orang tua, saudara – saudaraku yang telah memberikan dorongan moril maupun materil
2. Bapak Prof. Dr. Mohammad Suyanto, MM selaku ketua Sekolah Tinggi Manajemen Informatika dan Komputer “AMIKOM” Yogyakarta.
3. Bapak Ir. Abbas Ali Pangera selaku ketua jurusan S1 Teknik Informatika STMIK ”AMIKOM” Yogyakarta.

4. Bapak Emha Taufiq Luthfi, ST. M.Kom selaku dosen pembimbing yang selalu sabar memberikan bimbingan, waktu dan arahan serta segala kemurahan hati kepada kami.
5. Seluruh Dosen dan karyawan STMIK AMIKOM Yogyakarta yang telah memberikan ilmunya kepada penulis.
6. All Crew Student Staff Humas STMIK AMIKOM Yogyakarta.
7. Keluarga besar S1-Teknik Informatika STMIK AMIKOM.
8. Keluarga besar Suwarno
9. Semua pihak yang telah membantu kelancaran penyusunan skripsi yang tidak dapat penulis sebutkan satu – persatu.

Penulis menyadari sepenuhnya bahwa laporan ini jauh dari sebuah kesempurnaan, itu semua karena keterbatasan penulis. Kritik dan saran yang bersifat membangun akan selalu penulis harapkan sehingga dapat lebih baik dan bermanfaat bagi penulis serta pihak-pihak yang membutuhkan.

Akhirnya dengan doa kepada Allah SWT, semoga laporan skripsi ini bermanfaat bagi semua pihak yang membutuhkan.

Wassalaamu'alaykum Warahmatullahi Wabarakatu

Yogyakarta, Maret 2011

Penyusun

DAFTAR ISI

	HALAMAN
HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN	iv
HALAMAN PERNYATAAN.....	v
HALAMAN MOTTO.....	vi
HALAMAN PERSEMBAHAN	vii
KATA PENGANTAR	ix
DAFTAR ISI.....	xi
DAFTAR GAMBAR.....	xiv
DAFTAR TABEL.....	xvii
INTISARI.....	xviii
ABSTRACT.....	xix
BAB I. PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan	4
BAB II. LANDASAN TEORI	
2.1 Short Message Service (SMS).....	6
2.1.1 Pengertian SMS	6
2.1.2 Karakteristik SMS.....	6
2.1.3 Arsitektur Jaringan SMS.....	7
2.1.4 Jenis Layanan SMS.....	10
2.1.4.1 Cell Broadcast.....	10
2.1.4.2 Point to Point.....	10

2.1.5 Tipe Pesan SMS.....	10
2.2 Java Micro Edition.....	11
2.2.1 Java Overview	11
2.2.2 Konfigurasi Java 2 Micro Edition.....	13
2.2.3 Profile Java 2 Micro Edition.....	14
2.2.3.1 MIDP	15
2.2.4 Record Management System.....	15
2.3 Kriptografi.....	17
2.3.1 Pengertian Kriptografi	17
2.3.2 Macam-macam Kriptografi.....	17
2.3.2.1 Kriptografi Klasik	17
2.3.2.2 Kriptografi Modern.....	18
2.3.2.2.1 Kriptografi Simetri.....	18
2.3.2.2.2 Kriptografi Asimetri	19
2.3.3 Tujuan Kriptografi	20
2.3.4 Advanced Encryption Standard	20
2.3.5 Algoritma Advanced Encryption Standard.....	21
2.4 Bouncy Castle Cryptography API	26
BAB III. ANALIS DAN PERANCANGAN	
3.1 Analisis Kebutuhan.....	28
3.1.1 Kebutuhan Awal	29
3.2 Perancangan Sistem.....	30
3.2.1 Arsitektur Sistem.....	30
3.2.2 Perancangan Proses.....	31
3.2.2.1 Use Case Diagram	31
3.2.2.2 Activity Diagram	34
3.2.2.3 Class Diagram.....	36
3.2.2.4 Sequence Diagram.....	41
3.3 Perancangan Record Store	43
3.4 Perancangan Antarmuka	45

BAB IV. IMPLEMENTASI DAN PEMBAHASAN

4.1 Implementasi Antarmuka.....	51
4.1.1 Antarmuka Menu Utama.....	51
4.1.2 Batasan Implementasi.....	52
4.2 Kelas MyMIDlet.....	54
4.3 Pengaturan Contact.....	55
4.4 Pengaturan SMS.....	61
4.5 Record Store.....	64
4.6 Kelas MyPeople.....	65
4.7 Kelas MyMessage.....	66
4.8 Pengiriman dan Enkripsi SMS.....	67
4.9 Penerimaan SMS.....	72
4.10 Dekripsi SMS.....	73
4.11 Pengujian.....	76
4.11.1 Lingkungan Pengujian.....	78

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan.....	80
5.2 Saran.....	80

DAFTAR PUSTAKA

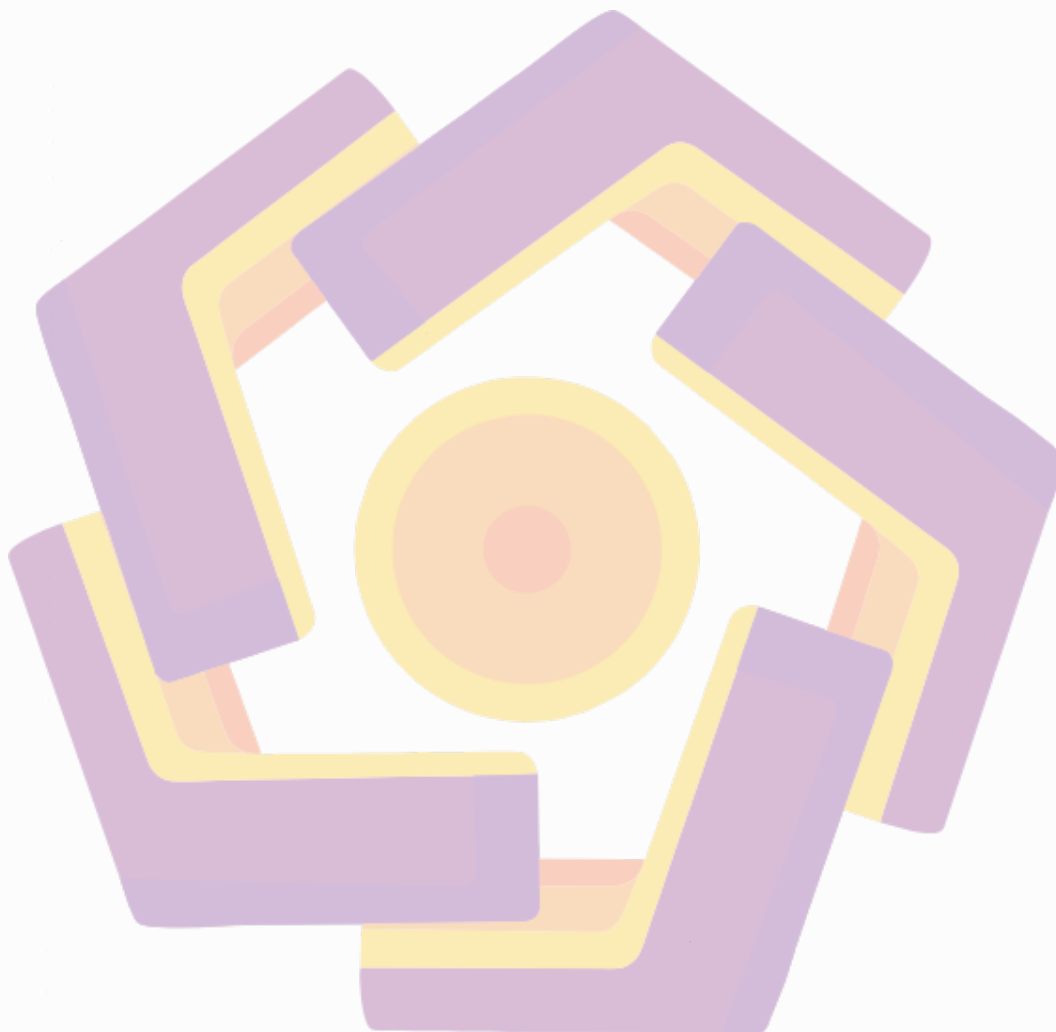
LAMPIRAN

DAFTAR GAMBAR

Gambar 2.1	Arsitektur SMS	7
Gambar 2.2	Keterkaitan MIDlet dengan Record Store	16
Gambar 2.3	Kriptografi Kunci Simetri	18
Gambar 2.4	Kriptografi Kunci Asimetri.....	19
Gambar 2.5	Proses Umum Enkripsi dan Dekripsi AES	23
Gambar 2.6	Operasi Transformasi Substitusi Byte dengan S-Box.....	24
Gambar 2.7	Operasi Transformasi ShiftRow.....	25
Gambar 2.8	Operasi Transformasi MixColumn	25
Gambar 2.9	Operasi Transformasi Penambahan Kolom	26
Gambar 3.1	Arsitektur Sistem Umum.....	30
Gambar 3.2	Use Case Diagram Enkripsi SMS.....	32
Gambar 3.3	Activity Diagram.....	35
Gambar 3.4	Class Diagram.....	37
Gambar 3.5	Sequence Diagram Input Kontak.....	42
Gambar 3.6	Sequence Diagram Mengirim Pesan.....	43
Gambar 3.7	Sequence Diagram Menerima Pesan.....	43
Gambar 3.8	Rancangan Menu Utama.....	46
Gambar 3.9	Form Pesan Baru	46
Gambar 3.10	Rancangan Inbox.....	47
Gambar 3.11	Rancangan Input Password.....	47
Gambar 3.12	Rancangan Daftar Contact.....	48
Gambar 3.13	Rancangan Form Kontak Baru.....	49

Gambar 3.14 Rancangan Menu Keterangan	50
Gambar 4.1 Tampilan Menu Utama	52
Gambar 4.2 Potongan Kode Program Kelas MyMenu.java	53
Gambar 4.3 Potongan Kode getDisplay.....	54
Gambar 4.4 Potongan Kode Kelas MyMIDlet	55
Gambar 4.5 Potongan Kode Program untuk Menampilkan Contact List	56
Gambar 4.6 Tampilan Antarmuka Daftar Kontak	57
Gambar 4.7 Tampilan Input Password pada Edit Kontak.....	58
Gambar 4.8 Tampilan Form Edit Kontak.....	58
Gambar 4.9 Tampilan Alert Salah Password.....	59
Gambar 4.10 Cuplikan Kode Untuk Membuat Kontak Baru	60
Gambar 4.11 Tampilan Form Kontak Baru	61
Gambar 4.12 Tampilan Inbox.....	62
Gambar 4.13 Tampilan Sent	62
Gambar 4.14 Tampilan Alert dengan Hasil Enkripsi.....	63
Gambar 4.15 Potongan Kode Program Menulis Pesan Baru.....	64
Gambar 4.16 Potongan Kode Program untuk Record Store.....	65
Gambar 4.17 Potongan Kode Program Kelas MyPeople.....	66
Gambar 4.18 Potongan Kode Program Kelas MyMessage	67
Gambar 4.19 Potongan Kode Program Kelas MyMessageSender	68
Gambar 4.20 Potongan Kode Program Proses Enkripsi	69
Gambar 4.21 Potongan Kode Program untuk Mendapat Nama Pengirim.....	72
Gambar 4.22 Tampilan Input Password Dekripsi.....	73

Gambar 4.23 Potongan Kode Program untuk Dekripsi	74
Gambar 4.24 Tampilan Pesan yang Sudah didekripsi	76
Gambar 4.25 Uji Coba Pada HP SAMSUNG S5620	77
Gambar 4.26 Uji Coba pada HP LG Cookie.....	77



DAFTAR TABEL

Tabel 2.1	Perbedaan CLDC dan CDC	14
Tabel 2.2	Penyimpanan Record dalam Record Store	16
Tabel 2.3	Parameter AES.....	22
Tabel 2.4	S-Box AES.....	23
Tabel 3.1	Deskripsi Input Contact	32
Tabel 3.2	Deskripsi Mengirim Pesan.....	33
Tabel 3.3	Deskripsi Input Contact	34
Tabel 3.4	Record Store Untuk dbContact	43
Tabel 3.5	Record Store Untuk dbSent	43
Tabel 3.6	Record Store Untuk dbInbox	44
Tabel 4.1	Lingkungan Pengujian	78

INTISARI

Keamanan komunikasi bagi sebagian orang merupakan hal yang sangat vital. Dengan berkembangnya sarana komunikasi pengamanan komunikasi pun berkembang beriringan. Teknologi email security, https, ssl pun muncul mengamankan komunikasi di jaringan internet. Kenyataannya, berbagai ancaman keamanan pada sms terjadi. Hal yang perlu dicatat terutama bagi user yang menggunakan sms untuk aktivitas bisnis adalah bahwa sms bukan merupakan *environment* yang aman.

Java ME *standard library* didesain agar sesuai pada *mobile device* dengan keterbatasannya, sehingga tidak memiliki kemampuan enkripsi.

Beberapa developer telah mengembangkan API untuk tujuan enkripsi. Yang paling terkenal dan banyak digunakan adalah Bouncy Castle Cryptography API, yang menyediakan banyak dukungan untuk berbagai metode enkripsi termasuk *Advance Encryption Standard (AES)*.

Pada skripsi ini penulis mencoba membuat aplikasi *mobile* untuk mengamankan isi SMS menggunakan algoritma AES dan dengan bantuan Bouncy Castle Cryptography API.

Kata kunci: Enkripsi, AES, SMS, J2ME.

ABSTRACT

Security of communication for some people is a vital matter. With the development of communication means communication security is growing hand in hand. Email technology security, https, ssl appears secure communications in the Internet network. In fact, various security threats on sms occur. The important thing to note, especially for users who use SMS for business activities is that the sms is not a safe environment.

Java ME standard library is designed to fit on mobile devices with its limitations, so it does not have encryption capabilities.

Some developers have developed APIs for encryption purposes. The most famous and widely used is Bouncy Castle Cryptography APIs, which provide much support for various encryption methods, including Advanced Encryption Standard (AES).

In this mini thesis the author tries to create mobile applications for securing the contents of SMS uses the AES algorithm and with the help of Bouncy Castle Cryptography APIs.

Keywords: Encryption, AES, SMS, J2ME.

