PERANCANGAN APLIKASI ENKRIPSI DAN DEKRIPSI SMS DENGAN ALGORITMA SIMETRI AES PADA TELEPON SELULER

SKRIPSI

Disusun oleh

Miftahul Choiril Huda

06.11.1129

JURUSAN TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

AMIKOM

YOGYAKARTA

2010

PERANCANGAN APLIKASI ENKRIPSI DAN DEKRIPSI SMS DENGAN ALGORITMA SIMETRI AES PADA TELEPON SELULER

Skripsi

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

Disusun oleh

Miftahul Choiril Huda

06.11.1129

JURUSAN TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

AMIKOM

YOGYAKARTA

2010

PERSETUJUAN

SKRIPSI

Perancangan Aplikasi Enkripsi Dan Dekripsi SMS Dengan Algoritma Simetri AES Pada Telepon Seluler

Yang dipersiapkan dan disusun oleh

Miftahul Choiril Huda

06.11.1129

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 29 Mei 2010

Dosen Pembimbing,

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

PENGESAHAN

SKRIPSI

Perancangan Aplikasi Enkripsi Dan Dekripsi SMS Dengan Algoritma Simetri AES Pada Telepon Seluler

Yang dipersiapkan dan disusun oleh

Miftahul Choiril Huda

06.11.1129

telah dipertahankan di depan Dewan Penguji
pada tanggal 29 Mei 2010

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Dr. Abidarin Rosidi, MMA **NIK. 190302034**	
Emha Taufiq Luthfi, ST, M.Kom **NIK. 190302125**	
Andi Sunyoto, M.Kom **NIK. 190302052**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 29 Mei 2010

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, 29 Mei 2010

Miftahul Choiril Huda

NIM. 06.11.1129

MOTTO

HIDUP ADALAH KESEIMBANGAN ANTARA KEPERCAYAAN DAN TANGGUNG JAWAB,
ANTARA PELUANG DAN RESIKO,
ANTARA HATI DAN LOGIKA.

DEMI WAKTU MATAHARI SEPENGGALAHAN NAIK,
DEMI MALAM APABILA TELAH SUNYI,
TUHANMU TIADA MENINGGALKAN KAMU DAN TIADA PULA BENCI KEPADAMU,
DAN SESUNGGUHNYA AHIR ITU LEBIH BAIKBAGIMU DARI PERMULAAN,
DAN KELAK TUHANMU PASTI MEMBERIKAN KARUNIA-NYA KEPADAMU, LALU KAMU MENJADI PUAS,
BUKANKAH DIA MENDAPATIMU SEBAGAI SEORANG YATIM, LALU MELINDUNGIMU,
DAN DIA MENDAPATIMU SEBAGAI SEORANG YANG BINGUNG LALU DIA MEMBERIKAN PETUNJUK,
DAN DIA MENDAPATIMU SEBAGAI SEORANG YANG KEKURANGAN, LALU DIA MEMBERIKAN KECUKUPAN.

SEGALA PUJI BAGI ALLAH PENCIPTA LANGIT DAN BUMI, YANG MENJADIKAN MALAIKAT SEBAGAI UTUSAN YANG MEMPUNYAI SAYAP MASING2 DUA,
TIGA DAN EMPAT. ALLAH MENAMBAHKAN PENCIPTAAN-NYA APA YANG DIKEHENDAKI-NYA. SESUNGGUHNYA
ALLAH MAHA KUASA ATAS SEGALA SESUATU

HALAMAN PERSEMBAHAN

Dengan karunia Allah SWT atas segala rahmat-NYA beserta ridho-NYA, karya tulis ini berhasil disusun. Dengan rasa syukur Karya tulis ini saya persembahkan Kepada :

- ***Ibu dan Ayahku*** *(almarhum)* ***beserta kedua kakakku****, yang sangat aku cintai, Terimakasih atas kasih sayang, kepercayaan, dukungan dan do'a yang tiada putus untuk kemudahan dan kebahagiaan putranya.*
- ***Sahabat dekatku Dian, Aulia, Hany, Citra, Endah, Nora, Abu, Sihab dan Daniel ,*** *termakasih atas do'a, dukungan dan semangat yang kalian berikan, hingga karya ini berhasil disusun.*
- ***Bapak Margono beserta Keluarga,*** *saya ucapkan banyak terima kasih atas kepercayaan dan kesempatan atas fasilitas yang luar biasa, sehingga punulisan karya ini dapat berjalan lancar.*
- ***Kerabatku Budhi, Fitri, Kelik, dan sekawan lainnya,*** *terimakasih atas pengertiannya untuk tidak mengganggu dalam proses penulisan karya ini. Somaga kalian berkenan dan tidak kecewa atas ketidak hadiranku bersama kalian. Jangan lupa untuk mencarikan aku Pekerjaan.*
- ***Teman- teman Semuanya, Teguh, yahya, Aditya, Rajiv, Adi, kang Arjo, Tutut, Ivan, kang sono, Aan, Azis, ipul, tino, fai, Fauzy, Roy, Wahyu, Dedi, Sugeng, Anggit, Indra,Ismi, Ida, Ike dan yang lainnya.*** *Terimakasih atas bantuan dan suport yang kalian berikan selama penyusunan karya ini berlangsung. Tak lupa doa kan kusertakan untuk kesuksesan kalian semuanya. Terimakasih banyak.*

KATA PENGANTAR

Assalamu'alaikum Wr.Wb.

Puji syukur penyusun panjatkan kehadirat Allah SWT yang telah memberi rahamat dan hidayah-Nya kepada penyusun, sehingga dapat menyelesaikan skripsi dengan judul "Perancangan Aplikasi Enkripsi Dan Dekripsi SMS Dengan Algoritma Simetri AES Pada Telepon Seluler.".

Terselesaikannya skripsi ini tidak lepas dari dukungan moril maupun spiritual dan juga bimbingan ilmu pengetahuan. Penulis ingin mengucapkan banyak terima kasih kepada semua pihak yang telah membantu baik secara langsung maupun tidak langsung terutama kepada :

1. Bapak Prof. Dr. M. Suyanto, M.M selaku Ketua STMIK AMIKOM Yogyakarta.
2. Bapak Emha Taufiq Luthfi, ST, M.Kom selaku dosen Pembimbing yang telah meluangkan waktu, banyak membantu, serta petunjuk yang sangat berguna dalam penyusunan skripsi ini.
3. Bapak Andi Sunyoto, M.Kom yang telah memberi arahan, saran dan juga ilmu yang telah diberikan kepada penulis.
4. Kedua orang tuaku beserta kedua kakakku tercinta, yang telah banyak memberi dukungan, perhatian dan doa yang tulus tiada henti.
5. Seluruh Dosen-dosen STMIK "AMIKOM" Yogyakarta serta karyawan.
6. Teman-teman seperjuangan meski tak senasip yaitu kelas TI-B Angkatan 2006.

7. Rekan-rekanku yang tidak dapat disebutkan satu-persatu, yang ada lingkungan kampus STMIK AMIKOM Yogyakarta yang telah banyak membantu penulis dalam menyelesaikan skripsi ini.

Dalam penulisan skripsi ini penulis menyadari dengan keterbatasan ilmu dan kemampuan yang dimiliki, untuk itu penulis mengharapkan kritik dan saran dari semua pihak yang bersifat membangun untuk memperbaiki karya tulis ini di masa mendatang.

Akhir kata semoga skripsi ini dapat bermanfaat dan berguna.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 29 Mei 2010

Penulis

DAFTAR ISI

HALAMAN JUDUL i

HALAMAN PERSETUJUAN ii

HALAMAN PENGESAHAN iii

PERNYATAAN KEASLIAN iv

MOTTO v

HALAMAN PERSEMBAHAN vi

KATA PENGANTAR vii

DAFTAR ISI viii

DAFTAR TABEL xii

DAFTAR GAMBAR xiii

INTISARI xvi

ABSTRAKSI xvii

BAB I. PENDAHULUAN

1.1 Latar Belakang Masalah 1

1.2 Rumusan Masalah 3

1.3 Batasan Masalah 3

1.4 Tujuan Penelitian 3

1.5 Manfaat penelitian 4

1.6 Metodologi penelitian 4

1.7 Sistematika penulisan 5

BAB II. LANDASAN TEORI

2.1 Kriptografi 7

2.1.1 Pengertian Kriptografi 7

2.1.2. Macam-macam Kriptografi 8

2.1.2.1 Kriptografi Klasik 8

2.1.2.2 Kriptografi Modern 9

2.1.2.2.1 Kriptografi simetri 9

2.1.2.2.2 Kriptografi asimetri 10

2.1.3 AES (Advanced Encryption Standard) 11

2.1.4 Algoritma Advanced Encryption Standard (AES) 12

2.1.5 Fungsi / Tujuan Kriptografi 19

2.1.6 Istilah-Istilah 20

2.2 Short Message Service (SMS) 21

2.2.1 Prinsip kerja SMS 21

2.2.2 Keuntungan dan Kerugian SMS 23

2.3 Java 2 Micro Edition 24

2.3.1 Konfigurasi J2ME 26

2.3.2 Profil J2ME 28

2.3.3 MIDP 28

2.3.4 Record Management System (RMS) 30

2.3.5 Diagram Model Use Case 31

2.3.6 Diagram Kelas 32

2.4 Bounchy Castle Cryptography API 33

BAB III. ANALISIS DAN PERANCANGAN

3.1 Aliran Kerja Kebutuhan 36

3.1.1 Area Aplikasi 36

3.1.2 Kebutuhan Awal 37

3.2 Aliran Kerja Analisa 40

3.2.1 Fungsional Modeling 40

3.2.2 Entity class modeling 42

3.2.3 Interaction Modeling 48

3.2.4 Dinamic Modeling 50

3.3 Analisa Kerja Desain 52

3.3.1 Membuat RMS 50

3.3.2 Rancangan Antar Muka 54

3.3.2.1 Peancangan Antar Muka Menu Utama 55

3.3.2.2 Peancangan Antar Muka Pembangunan Contact 55

3.3.2.3 Peancangan Antar Muka Daftar Contact 57

3.3.2.4 Perancangan form Pembangunan Pesan 58

3.3.2.5 Perancangan Antar Muka Menentukan Tujuan dan Kunci . 59

3.3.2.6 Perancangan Antar Muka Pesan Masuk 60

3.3.2.7 Perancangan Antar Muka Pesan Terkirim 61

BAB IV. IMPLEMENTASI DAN PEMBAHASAN

4.1 Implementasi Antar Muka 63

4.1.1 Antar Muka Menu Utama 63

4.2 Kelas cryptoMidlet 65
4.3 Pengaturan Contact 67
4.4 Pengaturan Pesan 69
4.5 Record Store 69
4.6 Kelas User 74
4.7 Kelas Pesan 75
4.8 Pengiriman dan Enkripsi SMS 76
4.9 Penerimaan SMS 82
4.10 Deskripsi SMS 84
4.11 Pengujian 88
4.11.1 Lingkungan Pengujian 88
4.11.2 Pengujian pada Telepon Seluler 88
4.12 Hasil Pengujian 91

BAB V. PENUTUP

5.1 Kesimpulan 93
5.2 Saran 94

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR TABEL

Tabel 2.1 Jumlah putaran operasi pada AES 13

Tabel 2.2 Tabel S-box untuk transformasi Bytesub()AES 16

Tabel 2.3 Tabel perbandingan antara CDC dan CLDC 27

Tabel 2.4 Notasi Use Case Diagram 31

Tabel 3.1 record store rdContact 53

Tabel 3.2 record store rdSent 53

Tabel 3.3 record store rdInbox 53

Tabel 4.1 tabel lingkungan pengujian 88

Tabel 4.2 tabel implementasi pada handphone 90

DAFTAR GAMBAR

Gambar 2.1 Skema proses enkripsi dan dekripsi 8

Gambar 2.2 Skema kriptografi kunci simetri 9

Gambar 2.3 Skema kriptografi kunci asimetri 10

Gambar 2.4 Skema proses umum Enkripsi 15

Gambar 2.5 Skema transformasi ByteSub()..... 16

Gambar 2.6 Skema transformasi ShiftRow()..... 16

Gambar 2.7 Skema transformasi MixColoumn() AES 17

Gambar 2.8 Skema transformasi AddRoundKey() AES 17

Gambar 2.9 Skema Enkripsi dan Deskripsi dengan ChiperBlock 19

Gambar 2.10 Cara kerja SMS..... 21

Gambar 2.11 J2ME secara umum 26

Gambar 3.1 Skema area aplikasi 37

Gambar 3.2 Use Case Diagram 41

Gambar 3.3 Entity class diagram 43

Gambar 3.4 Sequence diaram use case input contact 49

Gambar 3.5 Sequence diaram use case mengirim sms 49

Gambar 3.6 Sequence diaram use case menerima sms 50

Gambar 3.7 Statechart diagram 51

Gambar 3.8 Perancangan menu utama 55

Gambar 3.9 Perancangan form New contact 57

Gambar 3.10 Perancangan form Contact list 58

Gambar 3.11 Perancangan textbox new message 59
Gambar 3.12 Perancangan form new message 59
Gambar 3.13 Perancangan list inbox 60
Gambar 3.14 Perancangan list message sent 61
Gambar 4.1 Tampilan menu utama 64
Gambar 4.2 Potongan kode program kelas Menu 64
Gambar 4.3 Potongan kode program getDisplay()..... 65
Gambar 4.4 Potongan kode program memulai MIDlet 66
Gambar 4.5 Potongan kode program untuk menampilkan daftarContact 67
Gambar 4.6 tampilan daftarContact 68
Gambar 4.7 Potongan kode program untuk membuat contact baru 68
Gambar 4.8 tampilan Inbox 69
Gambar 4.9 tampilan Sent atau pesan keluar 70
Gambar 4.10 Potongan kode program untuk menampilkan textbox pesan baru ..70
Gambar 4.11 tampilan Textbox pesan baru 71
Gambar 4.12 tampilan Form pesan baru 71
Gambar 4.13 tampilan Form Contact 72
Gambar 4.14 Potongan kode program untuk membuat record store 73
Gambar 4.15 Potongan kode program untuk menulis record pada vector 74
Gambar 4.16 Potongan kode program kelas user 75
Gambar 4.17 Potongan kode program kelas Pesan 76
Gambar 4.18 Potongan kode constructor kelas kirimPesan 77
Gambar 4.19 Potongan kode untuk mengeset pesan binary 78

Gambar 4.20 Tampilan alert pesan dikirim 78

Gambar 4.21 potongan kode untuk proses enkripsi 79

Gambar 4.22 tampilan pesan terenkripsi 82

Gambar 4.23 potongan kode untuk mendapatkan nama pengirim 83

Gambar 4.24 tampilan alert pesan baru diterima 84

Gambar 4.25 tampilan form Decryption key 84

Gambar 4.26 potongan kode untuk proses dekripsi 85

Gambar 4.27 tampilan pesan hasil dekripsi 87

Gambar 4.28 dari kiri tampilan W960i, 7610 dan k660 91

INTISARI

Komunikasi merupakan mekanisme untuk menyampaikan informasi dari satu piha ke pihak lain. Sejalan dengan perkembangan teknologi, kebutuhan akan media komunikasi pun meningkat. Saat ini, teknologi komunikasi bermacam-macam dan semakin memanjakan penggunanya. Mulai dari telephone, faximile, e-mail, dan masih banyak yang lainnya diantaranya adalah teknologi SMS.

Teknologi SMS hingga saat ini masih menjadi media komunikasi yang digemari oleh halayak umum, selain penggunaannya yang mudah biayanya pun murah. Namun di lain sisi teknologi SMS juga memiliki kelemahan. Teknologi SMS tidak menjamin keamanan dan kerahasiaan pesan yang dikirimkan. Beberapa resiko juga menjadi ancaman bagi kemanan pesan SMS diataranya SMS spoofing, SMS snooping, dan SMS interception. Dari beberapa ancaman yang menjadi resiko pesan SMS tersebut, maka perlu dibangun sebuah aplikasi yang mampu mengamankan dan merahasiakan pesan SMS, sehingga apabila terjadi sebuah ancaman dan pesan tersebut dibuka, maka isi dari pesan tersebut tetap terahasiakan. Salah satu solusi untuk mengamankan dan merahasiakan pesan tersebut adalah menengkripsikan pesan SMS sebelum dikirimkan.

Pembuatan aplikasi enkripsi dan dekripsi SMS ini diharapkan dapat menjadi solusi dari permasalahan di atas. Selain dapat mengamankan dan merahasiakan pesan, aplikasi yang dibangun harus mudah digunakan (*userfriendly*) oleh orang yang menggunakan dan memanfaatkan aplikasi ini.

Kata kunci : SMS, enkripsi, dekripsi, AES, BouncyCastle.

ABSTRACT

Communication is a mekanism to convey information from one party to another party. In line as growing of technology, a need of communication media increased. Currently, a variety of communications technologies and increasingly pamper people. Starting from telephone, facsimile, e-mail, and many others such as SMS technology.

SMS technology to this day remains a popular medium of communication by the people, besides easy to use it is also cheaper cost. But on the other side of the SMS technology also has disadvantages. SMS technology does not guarantee the security and confidentiality of messages sent. Some risks are also a threat to security including SMS spoofing, SMS snooping , and SMS interception. From some of the threats to the risk of such an SMS message, it is necessary to build an application that is able to secure and keep confidential SMS messages, so that in the event of a threat and that message is opened, the contents of the message remains secret. One solution to secure and keep the message is to encrypt SMS messages before sending.

Making encryption and decryption SMS application is expected to be the solution of the problems above. In addition to securing and keeping the message, the application built to be easy to use (userfriendly) by people who using and take advantage of this application.

Keywords: SMS, encryption, decryption, AES, BouncyCastle.