IMPLEMENTASI APLIKASI SMS TERSANDIKAN DENGAN ALGORITMA AES PADA PLATFORM ANDROID

Agus Sarjuni

41509010002

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA JAKARTA

2013

IMPLEMENTASI APLIKASI SMS TERSANDIKAN DENGAN ALGORITMA AES PADA PLATFORM ANDROID

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh: Agus
Sarjuni
41509010002

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA JAKARTA
2013

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM	: 41509010002
Nama	: Agus Sarjuni
Judul Skripsi	: Implementasi Aplikasi SMS Tersandikan Dengan Algoritma AES pada *Platform* Android

Menyatakan bahwa skripsi dengan judul diatas adalah hasil karya saya sendiri dan bukan plagiat kecuali kutipan-kutipan dan teori-teori yang digunakan dalam skripsi ini. Apabila ternyata ditemukan di dalam laporan skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 20 Februari 2013

Agus Sarjuni

LEMBAR PENGESAHAN

Yang bertanda tangan dibawah ini menyatakan bahwa laporan tugas akhir ini dari mahasiswa berikut ini :

Nim	:	41509010002
Nama	:	Agus Sarjuni
Jurusan	:	Teknik Informatika
Fakultas	:	Ilmu Komputer
Judul Skripsi	:	Implementasi Aplikasi SMS Tersandikan Dengan Algortima AES Pada Platform Android

Skripsi ini telah diperiksa dan disetujui.

Jakarta, 21 Februari 2013

Menyetujui,

Joko Adianto, M.Inf.Sys

Mengetahui,

Sabar Rudiarto, S.Kom, M.Kom

Koord. Tugas Akhir Teknik Informatika

Mengesahkan,

Tri Daryanto, S.Kom, M.T

Kaprodi Teknik Informatika

KATA PENGANTAR

Puji syukur Alhamdulillah kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Jurusan Teknik Informatika Universitas Mercu Buana.

Penulis menyadari bahwa laporan tugas akhir ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa laporan tugas akhir ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Bapak Joko Adianto M.Inf.Sys, selaku Pembimbing Tugas Akhir pada Jurusan Teknik Informatika Universitas Mercu Buana, yang telah berkenan meluangkan waktunya serta memberi dukungan dan pengarahan hingga laporan dan aplikasi tugas akhir ini selesai.
2. Bapak Tri Daryanto, S. Kom. MT, selaku Ketua Program Studi Teknik Informatika Universitas Mercu Buana.
3. Bapak Sabar Rudiarto, S. Kom, M. Kom, selaku Koordinator Tugas Akhir pada Jurusan Teknik Informatika Universitas Mercu Buana.
4. Bapak dan Ibu tercinta yang telah mendukung penulis baik spirit maupun materi.
5. Orang tua dan Kakak tercinta yang telah mendukung penulis dalam segala hal.
6. Teman-teman yang telah bersedia berbagi ilmu, pengalaman motivasi, semangat, dan doa kepada penulis. Serta mahasiswa-mahasiswi Teknik Informatika, khususnya angkatan 2009 yang bersama-sama berjuang bersama penulis meraih gelar Strata-1 (S1).

7. Semua pihak yang tidak dapat penulis sebutkan satu persatu yang telah memberikan dorongan dan membantu serta memberikan saran baik secara langsung maupun tidak langsung kepada penulis sehingga laporan ini dapat terselesaikan.

Semoga Allah SWT membalas kebaikan dan selalu mencurahkan hidayah serta taufikNya, Amin.

Jakarta, 20 Februari 2013

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR ISTILAH

1. *Plaintext* : pesan asli sebelum dienkripsikan (data asli).
2. *Ciphertext* : pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
3. Enkripsi : proses pengubahan plaintext menjadi *ciphertext.*
4. Dekripsi : kebalikan dari enkripsi yakni mengubah ciphertext menjadi *plaintext,* sehingga berupa data awal/asli.
5. Kriptografer : orang yang menggunakan algoritma kriptografi untuk merahasiakan pesan dan mendeskripsikannya kembali.
6. Kriptanalisis (*cryptanalysis*) : ilmu dan seni untuk memecahkan *chipertext*, berupa memperoleh *plaintext* dari *chipertext* tanpa mengetahui kuncinya. Pelakunya disebut kriptanalis.
7. Kriptologi (*cryptology*) : studi mengenai kriptografi dan kriptanalisis.
8. Penyadap (*eavesdropper*) : orang yang mencoba menangkap pesan selama ditransmisikan. Penyadap sama dengan *enemy*(musuh), *interceptor*(pencegat), *attecker*(penyerang).
9. Pesan, dapat berupa data maupun informasi yang dikirim melalui kurir, media komunikasi data, atau yang disimpan didalam media perekaman.
10. *Man-in-the-middle Attack* : menyadap komunikasi data rahasia.
11. *Chiper* : aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi.
12. Kunci (*key*) : parameter yang digunakan untuk transformasi enkripsi dan dekripsi.
13. *Encoding* : transformasi dari plainteks menjadi kode.
14. *Decoding* : transformasi dari kode menjadi plainteks.
15. *Pseudocode*: deskripsi dari algoritma pemrograman computer yang menggunakan struktur sederhana dari beberapa bahasa pemograman tetapi bahasa tersebut hanya ditujukan agar dapat dibaca manusia.

16. *Flowgraph*: Kontrol aliran program yang direpresentasikan menggunakan representasi grafis. Flowgraph terdiri dari sekumpulan *node* dan *edge*.
17. *Independent path*: jalur dalam program yang menunjukkan paling sedikit satu kumpulan proses ataupun kondisi baru.