IMPLEMENTASI ALGORITMA AES UNTUK KRIPTOGRAFI SMS BERBASIS ANDROID

Skripsi

oleh :
MARKUS WIWIT D.L
22094643

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2013

MPLEMENTASI ALGORITMA AES UNTUK KRIPTOGRAFI SMS BERBASIS ANDROID

Skripsi

Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

MARKUS WIWIT D.L
22094643

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2013

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

IMPLEMENTASI ALGORITMA AES UNTUK KRIPTOGRAFI SMS BERBASIS ANDROID

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 27 Mei 2013

MARKUS WIWIT D.L
22094643

HALAMAN PERSETUJUAN

Judul Skripsi	:	IMPLEMENTASI ALGORITMA AES UNTUK KRIPTOGRAFI SMS BERBASIS ANDROID
Nama Mahasiswa	:	MARKUS WIWIT D.L
N I M	:	22094643
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Genap
Tahun Akademik	:	2012/2013

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 14 Mei 2013

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, SKom.,M.Cs	Antonius Rachmat C., SKom.,M.Cs

HALAMAN PENGESAHAN

IMPLEMENTASI ALGORITMA AES UNTUK KRIPTOGRAFI SMS BERBASIS ANDROID

Oleh: MARKUS WIWIT D.L / 22094643

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer
pada tanggal 24 Mei 2013

Yogyakarta, 27 Mei 2013
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, SKom.,M.Cs
2. Antonius Rachmat C., SKom.,M.Cs
3. Hendro Setiadi, M.Eng
4. Yuan Lukito, S.Kom

Dekan

(Drs. Wimmie Handiwidjojo, MIT.)

Ketua Program Studi

(Nugroho Agus Haryono, M.Si)

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa yang telah melimpahkan rahmat dan anugerah, sehingga penulis dapat menyelesaikan program dan laporan untuk kelengkapan dan pemenuhan matakuliah Tugas Akhir yang berjudul "**IMPLEMENTASI ALGORITMA AES UNTUK KRIPTOGRAFI SMS BERBASIS ANDROID**" ini dengan baik dan tepat waktu.

Dalam menyelesaikan pembuatan program dan laporan Tugas Akhir ini, penulis menyadari banyak menerima masukkan dan saran dari berbagai pihak, baik secara langsung maupun secara tidak langsung. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan terima kasih kepada :

1. Keluargaku terkasih yang selalu mendukung dan memberikan motivasi kepada penulis selama ini.
2. Willy Sudiarto Raharjo., S.Kom., M.Cs. dan Antonius Rachmat C., S.Kom., M.Cs. selaku dosen pembimbing yang telah banyak membimbing penulis dalam menyelesaikan tugas akhir ini.
3. Budi Susanto, S.Kom., MT. selaku koordinator Tugas Akhir.
4. Semua pihak yang telah membantu penulis dalam penyelesaian tugas akhir ini yang tidak dapat penulis sebutkan satu per satu.

Akhir kata penulis ingin meminta maaf bila ada kesalahan baik dalam penyusunan laporan maupun yang pernah penulis lakukan sewaktu membuat program tugas akhir. Sekali lagi penulis mohon maaf yang sebesar-besarnya. Dan semoga ini dapat berguna bagi kita semua.

Yogyakarta, 28 Mei 2013

Markus Wiwit D.L

INTISARI

SMS merupakan fasilitas komunikasi yang murah dan mudah, namun keamanan data yang dikirim melalui SMS tidaklah terjamin karena bisa disadap. Untuk menangani masalah ini dibuatlah sebuah aplikasi SMS berbasis *Android* dengan *provider BouncyCastle* dan implementasi Algoritma *Advanced Encryption Standard (AES)* mode *counter* (*CTR)* atau lebih dikenal dengan *segmented integer counter (SIC) di API BouncyCastle.*

Penelitian dimulai dengan analisa pengiriman pesan dimana penulis meneliti panjang maksimum pesan yang dapat terkirim dengan penerapan algoritma *AES* mode *CTR.* Dilanjutkan dengan analisis *resource* yang dipakai perangkat dalam menjalankan aplikasi. Terakhir analisa pengaruh keutuhan pesan bila SMS yang terkirim mengalami kerusakan.

Hasil analisis dari data-data mentah menunjukkan kesimpulan dari tugas akhir ini, yaitu : 1) Untuk menangani keterbatasan isi SMS dan penerapan algoritma *AES* mode *CTR*, aplikasi dapat melakukan perpotongan pesan berdasarkan kata dengan jumlah karakter maksimal 101 karakter per SMS. 2) Aplikasi beroperasi menggunakan *resource* perangkat *mobile* yang minimal. 3) Proses dekripsi dapat dilakukan selama panjang *ciphertext* bukan merupakan kelipatan 4 ditambah 1 karakter dan *Initialization Vector* tidak rusak.

Kata Kunci : *Android*, *AES*, *BouncyCastle*, Kriptografi, SMS

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Sekitar 2,27 triliun orang menggunakan layanan SMS (*Short Message Service*) pada tahun 2012 saja berdasarkan hasil survei dari (CTIA, 2012). Berdasarkan hasil survei tersebut, SMS merupakan fitur komunikasi yang luas digunakan dan diminati, tetapi memiliki kelemahan dalam rawannya akan serangan penyadapan. Didalam dunia bisnis kerahasiaan sebuah informasi sangatlah penting, dimana persaingan antar perusahaan terjadi secara kompetitif. Kebocoran dalam informasi pada suatu perusahaan dapat membawa kerugian pada perusahaan tersebut.

Kriptografi merupakan salah satu metode pengamanan data yang sering digunakan dalam menjaga kerahasiaan data. Menurut Katz dan Lindell didalam buku *Introduction to Modern Cryptography* menyatakan kriptografi adalah, "*. . .is the scientific study of techniques for securing digital information, transactions, and distributed computations."* (Katz & Lindell, 2008, p. 3). Dalam pengertian ini, kriptografi merupakan sebuah studi teknik untuk mengamankan informasi, transaksi atau distribusi digital.

Didalam tugas akhir ini, penulis membawakan solusi dalam bentuk sebuah progam aplikasi SMS yang memiliki kemampuan untuk mengenkripsi pesan sebelum proses pengiriman. Aplikasi ini menggunakan algoritma kriptografi *AES* mode *CTR (Counter)* dalam proses enkripsi pesan. Algoritma *AES* yang digunakan merupakan implementasi dari pustaka *Bouncy Castle* yang merupakan pustaka yang digunakan oleh *Android.* Diharapkan dengan menggunakan aplikasi ini, informasi yang tersadap tidak dapat digunakan secara mudah karena memerlukan proses kriptoanalisis untuk mendekripsi pesan.

1.2. Perumusan Masalah

Adapun rumusan masalah pada penelitian ini :

1. Bagaimana menanggulangi masalah dalam keterbatasan isi SMS (160 karakter), dengan adanya ekspansi karakter yang dialami dalam proses enkripsi?
2. Berapa *resource* perangkat yang dibutuhkan aplikasi ketika dijalankan di perangkat *mobile*?
3. Bagaimana pengaruh keutuhan pesan terenkripsi terhadap proses dekripsi?

1.3. Batasan Masalah

Batasan-batasan masalah pada sistem ini adalah :

1. Sistem yang akan dibuat berbasis *Android* keluaran versi 4.0.4 *ICS* (*Ice Cream Sandwich*) dan *Bouncy Castle* versi 1.46.
2. Sistem menggunakan algoritma *AES* mode *CTR* dalam mengenkripsi SMS.
3. Sistem hanya menerima *ASCII* karakter dalam proses enkripsi dan dekripsi.
4. Format penulisan SMS yang dikirim merupakan format yang wajar dimana setiap kata diselingi dengan spasi.
5. Pertukaran kunci dilakukan diluar sistem dijalur yang aman merupakan tanggung jawab dari pengguna aplikasi.

1.4. Tujuan Penelitian

Tujuan penelitian ini adalah membangun sebuah perangkat lunak yang mampu mengenkripsikan pesan SMS menggunakan algoritma *AES*, sehingga orang yang tidak berkepentingan, tidak dapat mengetahui isi SMS tersebut.

1.5. Metode Penelitian

Penulis menggunakan beberapa metode yang digunakan untuk mendapatkan sumber, guna menyusun penulisan tugas akhir ini, antara lain :

a. Literatur

Melalui studi literatur, dipelajari teori-teori yang berhubungan dengan algoritma *AES*.

b. Observasi

Dengan melakukan bimbingan kepada dosen pembimbing dan juga mencari informasi kepada orang-orang yang lebih mengerti mengenai kriptografi.

c. Internet

Mencari sumber referensi melalui Internet.

1.6. Sistematika Penulisan

Sistematika laporan tugas akhir ini secara garis besar dapat dituliskan sebagai berikut :

BAB I : PENDAHULUAN

Dalam bab I, penulis membahas latar belakang masalah, rumusan masalah, batasan penelitian, tujuan penelitian, metode penelitian dan sistematika penelitian.

BAB II : TINJAUAN PUSTAKA

Dalam bab II, penulis membahas mengenai landasan teori yang melandasi penelitian antara lain pengertian SMS, *Android 4.0 (ICS)*, pengertian algoritma *AES*, dan pengertian *BouncyCastle.org*.

BAB III : ANALISIS DAN PERANCANGAN SISTEM

Dalam bab III, penulis membahas mengenai perancangan sistem yang akan digunakan secara keseluruhan yang meliputi perancangan *input*, proses dan *output*. Bab ini juga meliputi analisis kebutuhan sistem.

BAB IV : IMPLEMENTASI DAN ANALISIS SISTEM

Dalam bab IV, penulis membahas mengenai hasil penelitian antara lain hasil pengujian instrumen penelitian, analisis hasil terhadap pengujian algoritma *AES*.

BAB V : KESIMPULAN DAN SARAN

Dalam bab V, penulis membahas kesimpulan penelitian dan saran mengenai pengembangan penelitian dimasa mendatang.

BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Dari analisis berbagai percobaan yang dilakukan di bab IV, Sistem yang telah dibangun memiliki beberapa poin kesimpulan sebagai berikut.

a. Untuk menanggulangi keterbatasan isi SMS, aplikasi dapat memotong pesan perkata sesuai panjang SMS yang diijinkan yaitu 101 karakter.
b. Sistem ini memiliki *CPU Load* yang ringan dengan proses enkripsi memiliki *CPU Load* sebesar 14,15% dan proses dekripsi sebesar 4,4%.
c. *Initialization Vector* SMS adalah 22 karakter *Base64* pertama disetiap *ciphertext*.
d. Ketika proses enkoding ke *Base64* setelah enkripsi, terdapat anomali yaitu penambahan karakter *enter* diakhir cipher dan ditengah cipher.
e. *Ciphertext* menghasilkan *error "Bad Base-64"*, ketika panjang karakter merupakan kelipatan 4 ditambah 1 karakter, jika karakter anomali *enter* dihiraukan.

5.2. Saran

Penelitian tentang implementasi algoritma AES pada aplikasi SMS berbasis Android dapat dikembangkan lebih lanjut dengan melakukan pengembangan di bagian penyebaran kunci. Penyebaran kunci dapat dikembangkan dengan metode seperti *Diffie Hellman Agreement* sehingga kebocoran kunci ketika penyebaran dapat dihindari. Selain itu juga dapat ditambahkan dengan penambahan fitur *keystore* sehingga pengguna tidak perlu mengingat kunci setiap orang. Penambahan fitur pembantu seperti *contact picker* dan tampilan aplikasi perlu dipercantik.

DAFTAR PUSTAKA

Cartrysse, K., & van der Lub, J. (2004). *The Advanced Encryption Standard: Rijndael.* Diakses pada tanggal 18 Januari 2013 dari http://mail.vssd.nl/hlf/e012rijndael.pdf

CTIA. (2012). *CTIA Semi-Annual Wireless Industry Survey*. Diakses pada tanggal 28 Januari 2013 dari http://files.ctia.org/pdf/CTIA_Survey_MY_2012_Graphics-_final.pdf

Damjanović, B., & Simić, D. (2011). COMPARATIVE IMPLEMENTATION ANALYSIS OF AES ALGORITHM. *Journal of Information Technology and Applications (JITA)* , 119-126.

Dictionary.com. (n.d.). Diakses pada tanggal 21 April 2013 dari Dictionary.com: http://dictionary.reference.com/browse/cryptography

Dworkin, M. (2001). *Recommendation for Block Cipher Modes of Operation Methods and Techniques.* Diakses pada tanggal 12 Februari 2013 dari http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

FIPS. (2001). *FIPS 197: Announcing the ADVANCED ENCRYPTION STANDARD (AES).* Diakses pada tanggal 20 Januari 2012 dari http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Housley, R. (2004). *RFC3686.* Diakses pada tanggal 28 April 2013 dari http://tools.ietf.org/html/rfc3686#section-7

Katz, J., & Lindell, Y. (2008). *Introduction to Modern Cryptography.* Boca Raton: Chapman & Hall/CRC.

Lee, W.-M. (2012). *BEGINNING Android™ 4 Application Development.* Indianapolis: John Wiley & Sons, Inc.

Lipmaa, H., Rogaway, P., & Wagner, D. (2000). *Comments to NIST concerning AES Modes of Operations: CTR-Mode Encryption.* Diakses pada tanggal Februari 20 Februari 2013 dari http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ctr/ctr-spec.pdf

Madhwani, M., Kavyashree, C., & George, J. P. (2012). Cryptography On Android Message Application Using Look Up Table And Dynamic Key (Cama). *IOSR Journal of Computer Engineering (IOSRJCE)* , 54-59.

Mahmoud, T. M., Abdel-latef, B. A., Ahmed, A. A., & Mahfouz, A. M. (2009). Hybrid Compression Encryption Technique for Securing SMS. *International Journal of Computer Science and Security (IJCSS)* , 473-481.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1997). *Handbook of Applied Cryptography.* Florida: CRC Press.