PENERAPAN ALGORITMA RSA DAN ALGORITMA HUFFMAN PADA APLIKASI KRIPTOGRAFI DAN KOMPRESI SMS BERBASIS ANDROID

TESIS

Oleh :
LAURENTINUS
1311601601

PROGRAM STUDI : MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

JAKARTA
2016

PENERAPAN ALGORITMA RSA DAN ALGORITMA HUFFMAN PADA APLIKASI KRIPTOGRAFI DAN KOMPRESI SMS BERBASIS ANDROID

TESIS

Diajukan untuk memenuhi salah satu persyaratan memperoleh gelar Magister Ilmu Komputer (MKOM)

Oleh :
LAURENTINUS
1311601601

PROGRAM STUDI : MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

JAKARTA
2016

PROGRAM STUDI : MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertandatangan dibawah ini,

Nama Mahasiswa	:	Laurentinus
Nomor Induk Mahasiswa	:	1311601601
Jenjang Studi	:	Strata 2
Konsentrasi	:	Rekayasa Komputasi Terapan
Fakultas/Program	:	Magister Ilmu Komputer

Menyatakan bahwa TESIS yang berjudul :
Penerapan Algoritma RSA dan Algoritma Huffman pada Aplikasi Kriptografi dan Kompresi SMS Berbasis Android

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain,
2. Saya ijinkan untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan apabila di kemudian pernyataan ini tidak benar.

Jakarta, 10 Februari 2016

(Laurentinus)

PROGRAM STUDI : MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama	:	Laurentinus
Nomor Induk Mahasiswa	:	1311601601
Konsentrasi	:	Rekayasa Komputasi Terapan
Jenjang Studi	:	Strata 2
Judul	:	Penerapan Algoritma RSA dan Algoritma Huffman Pada Aplikasi Kriptografi dan Kompresi SMS Berbasis Android

Jakarta, 15 Februari 2016

Tim Penguji: Tanda tangan :

Ketua,
Prof. Dr. Moedjiono, M.Sc .....

Anggota,
Dr. Ir. Nazori Az, M.T .....

Pembimbing Utama,
Mardi Hardjianto, M.kom .....

Pembimbing Pendamping,
Dr. Ir. Nazori Az, M.T .....

Ketua Program Studi

(Dr. Ir. Nazori Az, M.T)

Abstrak

Perkembangan teknologi telekomunikasi memungkinkan manusia untuk berkomunikasi salah satunya yaitu menggunakan perangkat telepon. Namun tidak adanya security yang menjamin Keamanan dan menjaga kerahasiaan data atau informasi dalam pengiriman SMS mengakibatkan pesan mudah dicuri oleh pihak yang tidak berwenang. SMS yang dikirimkan melalui BTS akan diterima Message Service Center (SMSC) Operator sehingga menimbulkan celah penyalahgunaan informasi. Salah satu cara untuk mengamankan data dari proses komunikasi data yaitu dengan kriptografi. Penelitian ini menggunakan metode penelitian statistik deskriptif. Penelitian ini dilakukan dengan melakukan analisa keamanan dengan menerapkan algoritma RSA pada aplikasi kriptografi dan kompresi SMS berbasis android. Algoritma RSA merupakan algoritma kriptografi asimetri yang menggunakan kunci publik dan kunci privat dalam enkripsi dan dekripsi untuk menghasilkan modulus dan ciphertext. Dengan aplikasi tersebut maka semua pesan yang dikirim telah dienkripsi menggunakan kunci yang digenerate, dan untuk membuka pesan tersebut maka dibutuhkan kunci yang digunakan untuk dekripsi pesan. Dikarenakan hasil ciphertext menggunakan algoritma RSA sangat panjang maka dibutuhkan kompresi text. Algoritma Huffman merupakan algoritma lossless data compression dimana kompresi data tidak menghilangkan satu byte pun dan disimpan sesuai aslinya. sehingga hasil dekompres sama dgn ciphertext original. Pengujian dilakukan menggunakan Metode Blackbox dan model ISO 9126 untuk menghasilkan aplikasi yang memiliki standarisasi tinggi.

Kata Kunci : *Kriptografi, Enkripsi, Dekripsi, SMS, mobile, RSA, kompresi, Huffman, android*

ABSTRACT

Development of telecommunications technology allows humans to communication, one of them is using mobile phone device. Unfortunatly, there are no security guarantees authenticity and confidentiality of data or information, the process delivery of SMS easily stolen by unauthorized parties because SMS sent via BTS will be accepted by Message Service Center (SMSC), And the operator can view the message contents. One of the ways to secure information from the data communication process that is uses cryptography. This research used descriptive statistics research.This research was conducted by analysing security by implementing the RSA algorithm Encryption and Decryption to SMS Application based on Android, RSA algorithm is an asymmetric cryptographic algorithm which uses a public key and a private key in the encryption and decryption to generate the modulus and ciphertext. With the application, all messages sent has been encrypted using a key that is generated, to open the message then takes the key used to decrypt the message. Because the results of the ciphertext using RSA algorithm is very long, it takes compression of the text. Huffman algorithm is an algorithm of Lossless compression that compresses the text without losing the original data so that decompress data same with the ciphertext. Testing Protype in this research, we use the Blackbox method and ISO 9126models to generate applications that have a high standardization.

Keywords : Cryptography, Encryption, Decryption, SMS, mobile, RSA, android

KATA PENGANTAR

Segala Puji bagi Tuhan Yesus Kristus atas segala anugrah, akal dan pikiran yang diberikan-Nya, sehingga penulis dapat menyelesaikan penelitian tesis dengan judul "PENERAPAN ALGORITMA RSA DAN ALGORITMA HUFFMAN PADA APLIKASI KRIPTOGRAFI DAN KOMPRESI SMS BERBASIS ANDROID".

Tujuan pembuatan tesis ini yaitu untuk memenuhi salah satu syarat dalam menyelesaikan jenjang Strata Dua (S-2) pada Program Studi Magister Ilmu Komputer (M.Kom) Progam Pascasarjana Universitas Budi Luhur.

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

1. Tuhan Yesus Kristus yang telah memberikan segalanya untuk menyelesaikan laporan ini.
2. Orang Tua yang senantiasa mendoakan dan mencurahkan cinta, kasih sayang, dan dukungan baik moral maupun materil.
3. Bapak Prof. Dr. Moedjiono, M.Sc selaku Ketua STMIK Atma Luhur Pangkalpinang.
4. Bapak Mardi Hardjianto, M.kom selaku Pembimbing Laporan Tesis.
5. Teman-teman yang telah mendukung dan berjuang bersama.
6. Lisia yang terus memberi dukungan.

Penulis menyadari penulisan laporan tesis ini masih jauh dari sempurna. Maka dari itu penulis menerima kritik serta saran yang bertujuan membangun. Semoga penelitian tesis ini dapat berguna serta bermanfaat bagi semua pihak.

Jakarta, 10 Januari 2016

Laurentinus

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Gambar **Halaman**

DAFTAR TABEL

Tabel **Halaman**

DAFTAR LAMPIRAN

Lampiran **Halaman**

DAFTAR PUSTAKA

[ALVIANTO 2015] Alvianto, Andi Riski, Darmaji, 2015, "Pengamanan Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android", Jurnal Sains dan Seni ITS, No.1

[AL-QUTAISH 2010] Al-Qutaish, Rafa E. 2010."Quality Models in Software Engineering Literature : An Analytical and Comparative Study", Journal of American Science.

I. [ARIYUS 2006] ARIYUS, DONY, " KRIPTOGRAFI KEAMANAN DATA DAN KOMUNIKASI", YOGYAKARTA:GRAHA ILMU, 2006.

[ARIYUS 2008] Ariyus, Dony, "Pengantar ilmu Kriptografi, Teori, Analisis & Implementasi". Yogyakarta:Andi, 2008.

[ASSHIDQI 2008] Asshidqi, Yanuar, Adiwijawa, Andrian Rakhmatsyah, 2008, "Aplikasi Enkripsi SMS Berbasis Java Menggunakan Algoritma RSA", Univ. Telkom

[BAMBANG 2010] Bambang, Hariyanto. "Esensi-esensi bahasa pemrograman Java", Edisi Ketiga, Informatika: Bandung, 2010.

[BRUCE 1996] Schneier, Bruce. "Applied Cryptography, Protocols, Algorithms, and Source Code in C", New York: Wiley & Sons, Inc: 1996.

[BUDIHANI 2012] Budihani, Herix Saputra, 2012, "Membangun Aplikasi Keamanan Data Teks dengan Metode RSA – CRT Berbasis Android"

[BURNETT 2001] Burnett, S., & Paine, S, 2001," *RSA Security's Official Guide to Cryptography",* New York: McGraw-Hill.

[CLEMENTS 2003] Clements, Tom , " SMS – Short but Sweet", 2003, http://www.oracle.com/technetwork/systems/sms-155850.html (Diakses Oktober 2015).

[DEWANTO 2013] Dewanto, Joko, Verdy Yanto, 2013, "Pembuatan Aplikasi SMS Kriptografi RSA dengan Android", Forum Ilmiah Vol. 10 No.2, Mei 2013