Penggunaan Teknik Kriptografi *Hybrid* untuk Pengamanan SMS pada Perangkat Android

TESIS

Oleh:

Muhammad Akbar

1111601058

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCA SARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2014

Penggunaan Teknik Kriptografi *Hybrid* untuk Pengamanan SMS pada Perangkat Android

TESIS

Diajukan sebagai salah satu persyaratan
untuk mendapatkan gelar Magister Ilmu Komputer (MKom)

Oleh:
Muhammad Akbar
1111601058

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

JAKARTA
2014

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDILUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : Muhammad Akbar
NIM : 1111601058
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Strata 2
Judul : Penggunaan Teknik Kriptografi *Hybrid* untuk Pengamanan SMS pada Perangkat Android.

Jakarta, 18 Februari 2014

Tim Penguji:	Tanda Tangan:
Ketua Dr. Moedjiono, M.Sc.	
Anggota, Hari Soetanto, S.Kom, M.Sc	
Pembimbing, Dr. Ir. Nazori AZ., M.T	

Ketua Program Studi

Dr. Ir. Nazori AZ., M.T

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCA SARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : MUHAMMAD AKBAR
NIM : 1111601058
Program Studi : MAGISTER ILMU KOMPUTER
Program : PASCASARJANA

menyatakan bahwa Tesis yang berjudul:

PENGGUNAAN TEKNIK KRIPTOGRAFI HYBRID UNTUK PENGAMANAN SMS PADA PERANGKAT ANDROID

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik pihak lain.
2. Saya izinkan 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 yang berlaku apabila di kemudian hari pernyataan ini tidak benar.

Jakarta, 18 Februari 2014

(MUHAMMAD AKBAR)

ABSTRAK

Salah satu alat komunikasi yang berkembang saat ini dan banyak digunakan adalah telepon seluler khususnya *smartphone*. Ponsel ataupun *smartphone* menyediakan berbagai media dan dapat digunakan untuk berbagai jenis kegiatan. Salah satu fitur yang tersedia dan cukup populer adalah media SMS, dimana SMS adalah merupakan suatu layanan pengiriman pesan singkat kepada pengguna ponsel lainnya dengan cepat dan dengan biaya yang murah. Ada berbagai kemudahan yang ditawarkan oleh layanan SMS antara lain informasi sesuai permintaan, pengunduhan nada dering, sampai dengan transaksi perbankan berupa mobile banking. Salah satu *smartphone* yang cukup populer saat ini adalah yang berbasis Android dikarenakan Android merupakan *OS mobile* yang *open platform* yang memberikan kemudahan dan keleluasaan bagi pengembang aplikasi untuk membangun aplikasi pada perangkat *smartphone*. Namun seiring perkembangan teknologi yang semakin canggih menimbulkan pertanyaan mengenai aspek keamanan informasi yang dikirimkan melalui SMS. Secara umum keterbatasan layanan SMS saat ini adalah tidak terjaminnya kerahasiaan dan keutuhan pesan yang dikirim. Oleh karenanya dibutuhkan suatu sistem keamanan yang kuat untuk penyampaian pesan SMS tersebut. Untuk melindungi informasi yang sensitif yang dikirimkan melalui SMS maka perlu diterapkan hal-hal yang terkait dengan keamanan informasi yang meliputi aspek keamanan kerahasiaan (*confidentiality*), keutuhan (*data integrity*), keaslian (*authentication*) dan tidak terdapat penyangkalan (*non-repudiation*). Pada penelitian tesis ini penulis mengajukan metode pengamanan komunikasi SMS pada perangkat Android dengan menggunakan teknik kriptografi *hybrid* yang merupakan kombinasi dari algoritma kriptografi simetrik AES-256, algoritma asimetrik *EC-Cryptography*, fungsi *message digest* SHA-256, fungsi *digital signing* dan sistem pembangkit kunci acak, yang diharapkan dapat memenuhi seluruh aspek keamanan informasi. Adapun dari hasil penelitian yang telah dilakukan maka kesimpulan yang diperoleh adalah bahwa dengan metode kriptografi *hybrid* yang diterapkan sebagai sistem pengamanan komunikasi SMS pada perangkat Android dapat memenuhi keseluruhan aspek keamanan informasi yang terdiri dari *confidentiality*, *data integrity*, *authentication*, dan *non-repudiation*

Kata Kunci: *SMS, enkripsi, fungsi hash, kriptografi hybrid, android*

ABSTRACT

One of the communication tools developed at this time and is widely used is cellular phones especially smartphones . Mobile phone or smartphone provides a variety of media and can be used for various types of activities . One feature that is available and quite popular is SMS services, which SMS is a short messaging service to other mobile users quickly and with little cost. There are various facilities offered by the SMS service , among others, information on demand, downloading ring tones , until the banking transactions such as mobile banking. One fairly popular smartphones today are based on Android because Android is an open mobile OS platform that provides convenience and flexibility for application developers to build applications on smartphones . But with the development of increasingly sophisticated technology raises questions about the security aspects of information transmitted via SMS . In general, the limitations of the current SMS service is no guarantee of confidentiality and integrity of the messages sent . Therefore we need a strong security system for the delivery of SMS messages. To protect sensitive information transmitted via SMS it is necessary to apply the things related to information security that includes security aspects of confidentiality, data integrity, authentication non-repudiation. In this thesis the authors propose methods of securing SMS communication on Android devices using hybrid cryptographic technique that is a combination of symmetric cryptographic algorithms AES-256 , EC-asymmetric cryptography algorithms , message digest function SHA-256 , digital signing functions and random key generation systems , which is expected to meet all aspects of information security . The results of the research that has been done then the conclusions reached is that the method is implemented as a hybrid cryptographic security system for SMS communication on android device can meet all aspects of information security consists of confidentiality , data integrity , authentication , and non–repudiation

Keywords: *SMS, encryption, hash function, hybrid cryptography, android.*

KATA PENGANTAR

Assalamu'alaikum wr, wb.

Segala puji bagi Allah SWT Tuhan semesta alam dan sudah selayaknya pujian itu kita sampaikan hanya kepadaNya. Dengan izinNya pula, naskah akhir tesis yang berjudul "PENGGUNAAN TEKNIK KRIPTOGRAFI *HYBRID* UNTUK PENGAMANAN SMS PADA PERANGKAT ANDROID" ini dapat diselesaikan. Dalam penyusunan naskah akhir tesis ini, penulis ingin menyampaikan ucapan terima kasih kepada:

1. Allah SWT, atas segala rahmat dan izinNya;
2. Kedua orang tua atas semua dukungan serta doanya;
3. Istri tercinta, atas motivasi dan energi yang selalu diberikan.
4. Bapak Dr. Ir. Nazori AZ, MT, selaku pembimbing yang telah memberikan saran dan masukan dalam penyusunan naskah akhir tesis ini;
5. Bapak Dr. Moedjiono, M.Sc, selaku Direktur Program Pascasarjana yang telah memberikan saran dan masukan dalam penyusunan naskah akhir tesis ini;
6. Serta semua pihak yang tidak dapat dituliskan.

Sebagai seorang manusia yang selalu memiliki kekurangan, penulis menyadari bahwa naskah akhir tesis ini masih banyak kekurangan. Oleh karena itu demi menyempurnakan naskah tesis ini, segala bentuk saran dan kritik mohon dapat dikirimkan melalui e-mail ke alamat muh_akbar@yahoo.com.

Wassalamu'alaikum wr, wb.

Jakarta, Februari 2014

Muhammad Akbar

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

[Android 2012] Android Developers website. "What is Android?". 2012. http://developer.android.com/guide/basics/what-is-android.html. (Diakses 25 November 2013).

[Aris 2013] Aris Kusuma Wijaya, Martinus, Abdul Rahman, Jurnal Jurusan Teknik Informatika STMIK MDP, 2013.

[Arthur 2012] Arthur Hefti website. "Encryption in PowerBuilder". 2012. http://arthurhefti.sys-con.com/node/107040/mobile. (Diakses 26 November 2013).

[Bodic 2005] 8. G. Le Bodic, "Mobile Messaging Technologies and Services SMS, EMS and MMS ", 2nd ed., John Wiley & Sons Ltd, (2005)..

[Croft 2005] N. Croft and M. Olivier, "Using an approximated One Time Pad to Secure Short Messaging Service (SMS)" , In Proceedings of the Southern African Telecommunication Networks and Applications Conference. South Africa, 2005.

[GSM 2009] GSM document, "Short Message Service", (2009, July). Available: http://www.gsmfavorites.com/documents/sms/

[Gong 1993] Li Gong. "Variations on the themes of message freshness and replay - or thediculty in devising formal methods to analyze cryptographic protocols". In In Proceedings of the Computer Security Foundations Workshop VI, pages

[Houghton 2000] Houghton Mifflin, "*Gadget",* 2000, http://www.thefreedictionary.com/gadget, (Diakses 17 Juni 2013).

[Ingrid 2012] Ingrid Lunden, Gartner: "*Android Accounted For 72% Of Smartphone Sales In Q3, Overall Sales Of Mobile Handsets Down 3%,* 2012", http://techcrunch.com/2012/11/14/gartner-samsung-widens-its-lead-over-apple-in-smartphones-in-q33-but-overall-sales-of-mobile-handsets-down-3/, (Diakses 17 Oktober 2013).

[Kusbandono 2004] Kusbandono, Arif., "Implementasi Algoritma AES-128 pada Mikrokontroler 8051." Bachelor Thesis, Institut Teknologi Bandung, Bandung, 2004.

[Larman 1998] "Applying UML And Patterns : An Introduction to Object