PENGEMBANGAN APLIKASI PENGAMANAN *ELECTRONIC MAIL* (*E-MAIL*) *MENGGUNAKAN HYBRID CRYPTOSYSTEM* PADA PERANGKAT *MOBILE* BERBASIS ANDROID

TESIS

Oleh:
ANDRI ZAKARIYA
0911601524

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

JAKARTA
2012

PENGEMBANGAN APLIKASI PENGAMANAN *ELECTRONIC MAIL* (*E-MAIL*) *MENGGUNAKAN HYBRID CRYPTOSYSTEM* PADA PERANGKAT *MOBILE* BERBASIS ANDROID

TESIS

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

Oleh:
ANDRI ZAKARIYA
0911601524

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

JAKARTA
2012

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJAN
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : Andri Zakariya
NIM : 0911601524
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Strata 2
Topik/Judul Tesis : Pengembangan Aplikasi Pengamanan *Electronic Mail* (*E-Mail*) Menggunakan *Hybrid Cryptosystem* Pada Perangkat Mobile Berbasis Android

Jakarta, 1 September 2012

Tim Penguji: Tanda tangan:

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

Anggota,
Hadi Syahrial, M.M., M.Kom .....

Pembimbing,
Dr. Ir. Nazori AZ, M.T .....

Ketua Program Studi

Dr. Ir. Nazori AZ, M.T

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJAN
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : ANDRI ZAKARIYA

NIM : 0911601524

Program Studi : MAGISTER ILMU KOMPUTER

Program : PASCASARJANA

menyatakan bahwa Tesis yang berjudul:

PENGEMBANGAN APLIKASI PENGAMANAN ELECTRONIC MAIL (E-MAIL) MENGGUNAKAN HYBRID CRYPTOSYSTEM PADA PERANGKAT MOBILE 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 hokum 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, 1 September 2012

(ANDRI ZAKARIYA)

Catatan: isian ditulis tangan

ABSTRAK

Saat ini hampir seluruh layanan internet dapat dinikmati secara *mobile* dimanapun dan kapanpun menggunakan perangkat *mobile* seperti *notebook*, *smartphone*, *tablet* PC dan lain sebagainya. Dengan makin meningkatnya mobilitas masyarakat, peranan perangkat *mobile* sebagai alat berkomunikasi dan bertukar informasi juga semakin berkembang pesat. Salah satu layanan internet yang paling populer adalah *e-mail*. Dengan menggunakan perangkat *mobile* yang terhubung dengan internet, layanan *e-mail* dapat digunakan secara luas oleh berbagai kalangan untuk saling bertukar informasi dimanapun dan kapanpun mulai dari informasi berklasifikasi biasa sampai yang berklasifikasi rahasia atau sensitif. Apabila informasi yang sensitif dikirimkan melalui *e-mail* maka dibalik berbagai kemudahan yang ditawarkan oleh layanan *e-mail*, keamanan merupakan isu yang tidak dapat dihindari karena internet menggunakan sistem jaringan terbuka yang sangat rentan terhadap kemungkinan pemanfaatan dan penyalahgunaan informasi oleh pihak-pihak yang tidak berhak. Untuk melindungi informasi yang sensitif yang dikomunikasikan melalui *e-mail*, maka perlu diimplementasikan aspek-aspek keamanan informasi yang meliputi aspek kerahasiaan (*confidentiality*), keutuhan data (*data integrity*), keaslian (*authentication*) dan tidak dapat dilakukan penyangkalan (*non-repudiation*). Pada penelitian tesis ini penulis mengajukan metode pengamanan komunikasi *e-mail* pada perangkat *mobile* berbasis Android dengan menggunakan *hybrid cryptosystem* yang merupakan kombinasi dari algoritma kriptografi simetrik, algoritma kriptografi asimetrik, fungsi *hash* dan sistem pembangkit kunci acak yang diharapkan dapat memenuhi seluruh aspek keamanan informasi. Dari hasil penelitian yang telah dilakukan, maka kesimpulan yang diperoleh untuk menjawab pertanyaan pada rumusan masalah adalah bahwa dengan metode *hybrid cryptosystem* yang diterapkan sebagai sistem pengamanan komunikasi *e-mail* pada perangkat *mobile* berbasis Android, dapat memenuhi seluruh aspek keamanan informasi yang terdiri dari *confidentiality*, *data integrity*, *authentication* dan *non-repudiation*.

Kata kunci: *e-mail*, enkripsi, fungsi *hash*, *hybrid cryptosystem*, dan Android.

ABSTRACT

Nowadays, most of internet services can be enjoyed in mobile anywhere and anytime using mobile devices such as notebooks, smartphones, tablet PCs and so on. In the manner of increasing mobility of people, the role of mobile devices as a tools of communication and exchange of information is also growing rapidly. One of the most popular internet services is electronic mail (e-mail). By using mobile devices which connected to the Internet, e-mail can be widely used by various groups to exchange information anywhere and anytime whether for public or confidential information. If confidential information sent via e-mail so behind some facilities offered by the e-mail, security is an issue that cannot be avoided because the internet uses an open system networks are highly vulnerable to misuse of information by parties who are not entitled to. In order to protect confidential information sent via e-mail, it is necessary to implement those aspects of information security consists of confidentiality, data integrity, authentication, and non-repudiation aspect. This study proposes a secure method of e-mail communication on Android-based mobile devices using a hybrid cryptosystem which combines symmetric encryption, asymmetric encryption, hash function, and random key generation are expected to comply with all aspects of information security. The experimental results show that the proposed method succeeded in meeting those aspects of information security including confidentiality, data integrity, authentication, and non-repudiation.

***Key words**: e-mail, encryption, hash function, hybrid cryptosystem, and Android.*

KATA PENGANTAR

Assalamu'alaikum Warohamtullohi Wabarokatuh.

Puji syukur marilah selalu kita panjatkan atas kehadirat Allah SWT Sang Pencipta semesta alam, karena hanya kehendak-Nya-lah naskah akhir tesis yang berjudul "PENGEMBANGAN APLIKASI PENGAMANAN *ELECTRONIC MAIL* (*E-MAIL*) MENGGUNAKAN *HYBRID CRYPTOSYSTEM* PADA PERANGKAT *MOBILE* BERBASIS ANDROID" ini dapat diselesaikan. Dalam penyusunan naskah akhir tesis ini, penulis ingin menyampaikan ucapan terima kasih kepada:

1. Allah SWT, atas segala rahmat dan ridho-Nya yang selalu menyertai seluruh aktivitas penulis;
2. Kedua orang tua, kakak dan adik, atas semua dukungan serta doanya;
3. Marsekal Ratih Anjasmami, atas motivasi dan energi yang selalu diberikan kepada penulis;
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 andri.zakariya@gmail.com.

Wassalamu'alaikum Warohmatullohi Wabarokatuh.

Jakarta, Agustus 2012

Andri Zakariya

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

Lampiran Halaman

DAFTAR PUSTAKA

[Adinagara 2011] Adinagara, Yudhistira T., et.al., "Enkripsi E-mail Dengan Menggunakan Metode ElGamal pada Perangkat Mobile", Institut Teknologi Sepuluh Nopember, Surabaya, 2011.

[Android 2012] Android Developers website. *What is Android?*. 2012. http://developer.android.com/guide/basics/what-is-android.html. (Diakses 10 Juni 2012).

[Arthur 2012] Arthur Hefti website. *Encryption in PowerBuilder*. 2012. http://arthurhefti.sys-con.com/node/107040/mobile. (Diakses 22 Juli 2012).

[Banerjee 2010] Banerjee, Usha., et.al., "Evaluation of the Capabilities of WireShark as a Tool for Intrusion Detection", *International Journal of Computer Applications*, vol. 6, (September, 2010): 1-5.

[Bang 2010] Bang, HeyJa. and Noh, BaekLin., "Design Approaches of Android for Students", *International Journal of Computer Science and Network Security*, vol. 10, (Desember, 2010): 225-230.

[Bazar 2008] Bazar, Husein., et.al., "A New Approach to Enhance E-mail Performance Through SMTP Protocol", *International Journal of Computer Science and Network Security*, vol. 8, (April, 2008): 299-303.

[Bharathi 2010] Bharati, Mani J., et.al., "Advancement in Mobile Communication using Android", *International Journal of Computer Applications*, vol. 1, (2010): 95-98.

[Budiono 2008] Budiono., "Penerapan Tanda Tangan Digital untuk Otentifikasi SMS-Banking." Bachelor Thesis, Institut Teknologi Bandung, Bandung, 2008.

[comScore 2011] comScore Inc. 2011. *Digital Omnivores: How Tablets, Smartphones and Connected Devices are Changing U.S. Digital Media Consumption Habits*. Seattle.

[Cutra 2007] Cutra, Angga, O., "Aplikasi Pengamanan Pesan Pada Mail Client Dengan Menggunakan Algoritma CAST-128." Bachelor Thesis, Universitas Komputer Indonesia, Bandung, 2007.

[Fernando 2009] Fernando, Ricky G., "Pembangunan Add-On Pada Mozilla Thunderbird Untuk Enkripsi Surat Elektronik Dengan Corrected Block Tiny Encryption Algorithm." Bachelor Thesis, Institut Teknologi Bandung, Bandung, 2009.

[Freed 1996] Freed, N. and Borenstein, N., *RFC 2045, Multipurpose Internet Mail Extensions (MIME), Part One: Format of Internet Message Bodies*. 1996. http://www.ietf.org/rfc/rfc2045.txt. (Diakses 5 Juni 2012).