IMPLEMENTASI HYBRID CRYPTOSYSTEM MENGGUNAKAN ALGORITMA RSA, 3DES DAN MD5 PADA APLIKASI SMS BERBASIS ANDROID

SKRIPSI

disusun oleh

Khoirul Amri

11.11.5136

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2014

IMPLEMENTASI HYBRID CRYPTOSYSTEM MENGGUNAKAN ALGORITMA RSA, 3DES DAN MD5 PADA APLIKASI SMS BERBASIS ANDROID

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika

disusun oleh

Khoirul Amri

11.11.5136

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA

2014

PERSETUJUAN

SKRIPSI

IMPLEMENTASI HYBRID CRYPTOSYSTEM MENGGUNAKAN ALGORITMA RSA, 3DES DAN MD5 PADA APLIKASI SMS BERBASIS ANDROID

yang disusun oleh

Khoirul Amri
11.11.5136

telah disetujuai oleh Dosen Pembimbing Skripsi
pada tanggal 24 Februari 2014

Dosen Pembimbing,

Dr. Ema Utami, S.Si, M.Kom
NIK. 190302037

PENGESAHAN

SKRIPSI

IMPLEMENTASI HYBRID CRYPTOSYSTEM MENGGUNAKAN ALGORITMA RSA, 3DES DAN MD5 PADA APLIKASI SMS BERBASIS ANDROID

yang disusun oleh

Khoirul Amri

11.11.5136

telah dipertahankan di depan Dewan Penguji
pada tanggal 21 November 2014

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Ferry Wahyu Wibowo, S.Si, M.Cs **NIK. 190302235**	
Yuli Astuti, M.Kom **NIK. 190302146**	
Dr. Ema Utami, S.Si, M.Kom **NIK. 190302037**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 1 Desember 2014

KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 25 November 2014

Khoirul Amri

NIM. 11.11.5136

MOTTO

1. Tidak perlu menunggu atau meminta motivasi dari orang lain, tapi motiavasilah dirimi sendiri supaya bisa menjadi motivator atau inspirator bagi orang lain. (*amrilio quote*)
2. Jangan suka membandingkan kekurangan diri sendiri dengan kelebihan orang lain, karena itu membuat kita tidak bersyukur atas apa pun yang pernah kita raih. (*Mario Teguh quote*)
3. Allah meninggikan orang-orang yang beriman diantara kamu dan orang-orang yang diberi ilmu pengetahuan beberapa derajat. (Depag RI, 1989 : 421)
4. Hidup itu seperti *coding*, selalu menggunakan percabangan dalam pengambilan keputusan, selalu ada perulangan dalam menjalani aktifitas keseharian, dan selalu menggunakan *error handling* dalam menghadapi setiap permasalahan.
5. Bersungguh-sungguhlah meraih kesempurnaan selama waktunya masih luang. Ingat-ingatlah selalu atas waktumu yang telah terbuang sia-sia. (H.R Abu Faraj Bin Al Jauzi)
6. *No effort is wasted. So, break your limit till you can*!
7. ISIS (Ingin Sarjana Ingat Skripsi). *Keep calm and say* "*Bad day* (skripsi) pasti berlalu". (*khusus buat teman-teman yang sedang mengerjakan skripsi*)

PERSEMBAHAN

Sebagai ucapan syukur dan terimakasih atas selesainya skripsi ini saya persembahkan kepada:

1. Allah SWT yang telah melimpahkan semua rahmat dan karunia-Nya serta memberikan kemudahan kepada saya dalam menyelesaikan skripsi ini.
2. Nabi Muhammad SAW yang telah membimbing umat islam menuju jalan yang benar dan lurus, semoga kita mendapat *syafa'at* nya dihari kiamat nanti.
3. Kedua orang tua dan keluarga besar saya yang selalu mendoakan dan memberikan semangat, motivasi, serta dukungan materil.
4. Ibu Dr. Ema Utami, S.Si, M.Kom. selaku dosen pembimbing, terimakasih telah memberi kritik dan saran yang membangun dalam penyusunan skripsi ini.
5. Teman-teman kos perumnas Condong Catur di Jl. Tluki 6 No. 149.
6. Teman-teman 11-S1TI-08 yang telah memberi semangat, kenangan indah, canda tawa, suka duka saat masih di bangku kuliah. Dan bersama kalian tidak akan saya lupakan.
7. Serta semua pihak yang tidak bisa saya sebutkan satu persatu yang telah mendoakan, mendukung, dan memotivasi saya selama ini.

KATA PENGANTAR

Assalammualaikum Wr. Wb.

Puji syukur saya panjatkan kehadirat Allah SWT atas segala limpahan rahmat dan nikmat karunia-Nya. Serta sholawat dan salam saya curahkan kepada junjungan Rasulullah Muhammad SAW, sehingga skripsi yang berjudul "Implementasi Hybrid Cryptosystem Menggunakan Algoritma RSA, 3DES Dan MD5 Pada Aplikasi SMS Berbasis Android" ini dapat diselesaikan dengan baik.

Penyelesaian skripsi ini tidak lepas dari bantuan dari berbagai pihak, oleh karena itu saya ingin mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, MM, selaku ketua STMIK AMIKOM Yogyakarta.
2. Bapak Sudarmawan, M.T. sebagai ketua jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
3. Ibu Dr. Ema Utam, S.Si, M.Kom. selaku dosen pembimbing saya yang telah member kritik dan saran untuk penyelesaian skripsi ini.
4. Kedua orang tua dan keluarga besar saya yang selalu mendoakan dan memberikan semangat, motivasi, serta dukungan materil.
5. Teman-teman 11-S1TI-08 yang telah memberikan semangat dan motivasi untuk menyelesaikan skripsi ini.
6. Dan semua pihak yang tidak bisa saya sebutkan yang telah banyak membantu dalam penyusunan skripsi ini.

Saya menyadari bahwa penyusunan skripsi ini jauh dari kata sempurna, oleh karena itu penulis mengharapkan saran maupun kritik yang membangun agar kedepannya menjadi lebih baik lagi. Akhir kata, semoga skripsi ini dapat bermanfaat bagi pembaca pada umumnya dan saya sendiri.

Wassalamualaikum Wr. Wb.

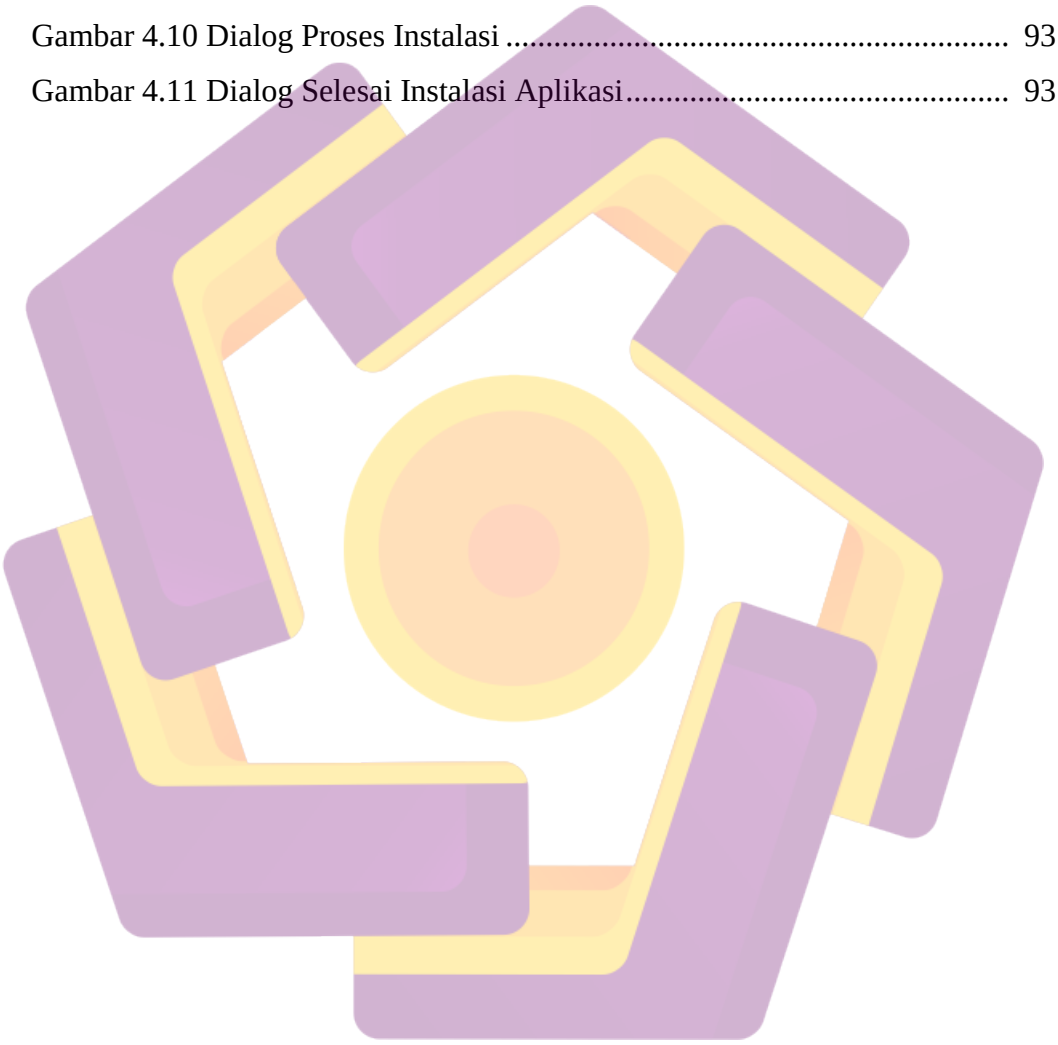
Yogyakarta, 25 November 2014

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR



INTISARI

Kriptografi adalah ilmu atau seni untuk menjaga keamanan pesan meliputi aspek kerahasiaan, integritas data, otentikasi, dan nirpenyangkalan. *Hybrid Cryptosystem* merupakan gabungan dari kriptografi simeteri dan asimeteri, sehingga dipastikan tingkat keamanannya lebih tinggi dibanding menggunakan satu metode saja.

SMS (*Short Message Service*) atau pesan singkat mungkin tak lagi sepopuler dulu, namun penggunanya masih cukup banyak di Indonesia. Dan mungkin masih belum banyak yang tahu bahwa tingkat keamanan SMS sangatlah rendah. Karena SMS hanya diubah kedalam bentuk heksadesimal (PDU) di server operator, sehingga SMS tersebut masih bisa disadap. Salah satu solusinya yaitu metode *Hybrid Cryptosystem* yang diimplentasikan pada sebuah aplikasi SMS. Disini metode *Hybrid Cryptosystem* menggunakan tiga algoritma yaitu RSA, 3DES dan MD5.

Metode *Hybrid Cryptosystem* terdiri atas enkripsi simetris dengan satu kunci (*Session Key*) dan enkripsi asimetris dengan sepasang kunci (*Public* dan *Private Key*). Untuk mengirim pesan, pengirim mengenkripsi pesan dengan Session Key, kemudian Mengenkripsi *Session Key* dengan *Public Key*. Sedangkan untuk menerima SMS, penerima harus mendekripsi *Session Key* dengan *Private Key*, kemudian *Session Key* yang telah terdekripsi digunakan untuk mendekripsi SMS. Untuk cara penggunaan aplikasi, pengguna bisa masuk ke menu help. Namun disarankan pengguna setidaknya mengetahui tentang ilmu kriptografi.

Kata Kunci: Hybrid Cryptosystem, Android, SMS security, RSA, 3DES, MD5

ABSTRACT

Cryptography is a science or art to secure message that include aspects of confidentiality, data integrity, authentication, and non-repudiation. Hybrid Cryptosystem is a combination of simeteri and asimeteri cryptographic, and this ensures a higher level of security than just using one method.

SMS (Short Message Service) may no longer as popular as it used to be, but its still pretty much in Indonesia. And probably still not many people know that the SMS security level is very low. Because SMS is only converted into hexadecimal (PDU) in a operator's server, so that SMS can still be tapped. One solution is Cryptosystem Hybrid method that is implemented by a SMS application Android-Based. Here Hybrid Cryptosystem method using three algorithms namely RSA, 3DES and MD5.

Hybrid Cryptosystem method consists of symmetric encryption with one key (Session Key) and asymmetric encryption with a key pair (Public and Private Key). The sender encrypts the SMS with the Session Key, then Encrypts Session Key with Public Key. While receiver have to decrypt Session Key with Private Key, then decrypts the SMS with the Session Key. To use the application, users can go to the help menu. However, users are advised at least know about cryptography.

Keyword: *Hybrid Cryptosystem, Android, SMS security, RSA, 3DES, MD5*