

Implementasi Algoritma Enkripsi RSA Untuk Aplikasi Komunikasi Berbasis Teks Menggunakan *Bluetooth* Pada OS Android

Wahyu Tri Suseno
(07.04.111.00168)

Pembimbing 1 : Cucun Very Angkoso, S.T., M.T.

Pembimbing 2 : Ari Kusumaningsih, S.T., M.T.

ABSTRAK

Perkembangan teknologi komunikasi yang begitu cepat memicu perkembangan teknologi telepon seluler sebagai salah satu alat komunikasi modern. Komunikasi data yang diimplementasikan juga beragam, teks, gambar bahkan suara. Medium yang digunakan-pun kini beragam baik itu internet, *local connection* hingga *bluetooth*. *Bluetooth* dapat dipilih sebagai alternatif medium untuk menghubungkan satu perangkat dengan perangkat lain. Ditambah lagi dengan perkembangan android yang belakangan ini juga semakin pesat.

Bluetooth mampu menghubungkan perangkat yang satu dengan perangkat yang lainnya. Ini kemudian memungkinkan antar perangkat dapat saling bertukar atau berkirim data. Namun, dalam proses pengiriman data tersebut tidak ada yang dapat menjamin keamanannya. Hal ini yang kemudian membuat proses enkripsi menjadi hal yang sangat penting. *RSA* kemudian muncul sebagai salah satu alternatif algoritma yang dapat digunakan menangani proses enkripsi tersebut.

RSA memiliki teknik pemfaktoran yang cukup rumit, hal ini membuat tingkat keamanannya cukup tinggi. Selain itu, *RSA* juga cocok diaplikasikan dalam platform mobile karena memiliki struktur yang asimetris sehingga tidak terlalu membebani sistem yang dimiliki oleh perangkat mobile tersebut. Pengujian aplikasi ini sudah teruji melalui perhitungan manual dan dari pengambilan *device* yang berbeda - beda.

Kata Kunci : *bluetooth*, *RSA*, enkripsi, dekripsi

(Halaman ini Sengaja dikosongkan)

KATA PENGANTAR

Segala puji bagi Allah *Subhanahuwata 'ala* karena atas rahmat dan hidayah-Nya sehingga laporan Tugas Akhir dengan judul “Implementasi Algoritma Enkripsi RSA Untuk Aplikasi Komunikasi Berbasis Teks Menggunakan *Bluetooth* Pada OS Android” dapat terselesaikan dengan baik dan tepat pada waktunya.

Penulis menyadari bahwa masih banyak kekurangan dan ketidaksempurnaan pada penulisan maupun pemrograman yang telah dibuat, namun dari ketidaksempurnaan inilah yang akan mendorong seseorang menuju arah yang lebih baik guna penyempurnaannya.

Selama penulisan Tugas Akhir ini, Penulis menyadari banyak pihak yang telah memberikan waktunya untuk membantu dalam penyelesaian Tugas Akhir ini untuk semua itu Penulis ingin mengucapkan terima kasih yang tulus kepada:

1. Bapak Cucun Very Angkoso, S.T., M.T. selaku dosen pembimbing I
2. Ibu Ari Kusumaningsih, S.T., M.T. selaku dosen pembimbing II
3. Ibu Fika Hastarita, S.T., M.Eng. selaku kordinator tugas akhir
4. Seluruh Staf pengajar Teknik Informatika atas ilmu yang diberikan selama proses perkuliahan, semoga Allah menjadikan semua ini amal sholeh yang bermanfaat.
5. Staf Tata Usaha Jurusan atas bantuan melayani segala administrasi selama perkuliahan ini.
6. Seluruh anggota keluarga untuk doa dan dukungannya selama ini yang telah diberikan tanpa pamrih khususnya untuk bapak H. Suftiono dan ibu Hj. Nyamik Setyowati.
7. Teman-teman seperjuangan teknik informatika angkatan 2007(Tekratu) di universitas trunojoyo madura.

8. Spesial Nur Fauziah S.E, Zhomi fero dan didin yang sempat-sempatnya meluangkan waktunya untuk membantu dalam hal apapun.
9. Semua pihak yang tidak dapat kami sebutkan satu persatu, yang telah membantu dalam penyusunan laporan Tugas Akhir.

Penulis menyadari bahwa dalam pembuatan tugas akhir ini masih terdapat kekurangan-kekurangan. Untuk itu saran dan kritik membangun sangat penulis harapkan demi kesempurnaan tugas akhir ini. Akhir kata, penulis berharap tugas akhir ini dapat bermanfaat bagi semua pihak. Amien Yaa Robbaal Alamiin.

Bangkalan, Juli 2013

Penulis

DAFTAR ISI

	Hal.
ABSTRAK	iii
KATA PENGANTAR.....	v
DAFTAR ISI	vii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xiii
DAFTAR ISTILAH.....	xiv
DAFTAR LAMPIRAN	xv
BAB I	Error! Bookmark not defined.
PENDAHULUAN.....	Error! Bookmark not defined.
1.1 Latar Belakang.....	Error! Bookmark not defined.
1.2 Rumusan Masalah.....	Error! Bookmark not defined.
1.3 Tujuan.....	Error! Bookmark not defined.
1.4 Batasan Masalah	Error! Bookmark not defined.
1.5 Metodologi Penelitian.....	Error! Bookmark not defined.
1.6 Sistematika Penulisan	Error! Bookmark not defined.
BAB II	Error! Bookmark not defined.
TINJAUAN PUSTAKA	Error! Bookmark not defined.
2.1 Tinjauan Pustaka	Error! Bookmark not defined.
2.2 Android	Error! Bookmark not defined.
2.3 <i>Bluetooth</i>	Error! Bookmark not defined.

2.4	<i>Rivest Shamir Adleman (RSA) ...</i>	Error! Bookmark not defined.
2.5	Kriptografi	Error! Bookmark not defined.
2.6	Penelitian Sebelumnya.....	Error! Bookmark not defined.
2.6.1	Pengujian Enkripsi-Dekripsi untuk Pengamanan Dokumen	Error! Bookmark not defined.
2.6.2	<i>Hybrid Compression Encryption Technique for Securing SMS</i>	Error! Bookmark not defined.
2.6.3	Aplikasi Group Chat Dengan <i>Bluetooth</i> Pada Telepon Seluler	Error! Bookmark not defined.
2.6.4	Implementasi algoritma kriptografi kunci – public ElGamal untuk keamanan pengiriman email	Error! Bookmark not defined.
2.6.5	Studi dan Implementasi Algoritma RSA untuk Pengamanan Data Transkrip Akademik Mahasiswa	Error! Bookmark not defined.
2.6.6	Penerapan Algoritma Kriptografi Asimetris RSA untuk Keamanan Data di Oracle	Error! Bookmark not defined.
2.6.7	Implementasi <i>Bluetooth Instant Messaging</i> Pada Perangkat <i>Seluler</i> ..	Error! Bookmark not defined.
2.6.8	Perbandingan Dengan Metode Enkripsi Lainnya	Error! Bookmark not defined.
BAB III.....		Error! Bookmark not defined.
PERANCANGAN SISTEM.....		Error! Bookmark not defined.
3.1	Perancangan Sistem	Error! Bookmark not defined.
3.2	Garis Besar Sistem	Error! Bookmark not defined.

3.3 Sistem Utama	Error! Bookmark not defined.
3.4 Algoritma RSA	Error! Bookmark not defined.
3.4.1 Proses Enkripsi Menggunakan RSA	Error! Bookmark not defined.
3.4.2 Proses Dekripsi Menggunakan RSA.....	Error! Bookmark not defined.
3.4.3 Contoh Sederhana Perhitungan Kata RSA.....	Error! Bookmark not defined.
BAB IV	Error! Bookmark not defined.
IMPLEMENTASI	Error! Bookmark not defined.
4.1 Platform	Error! Bookmark not defined.
4.2 Perangkat Keras	Error! Bookmark not defined.
4.3 Perangkat Lunak ...	Error! Bookmark not defined.
4.3.1 MENGINSTAL PLUGIN ADT .	Error! Bookmark not defined.
4.3.2 KONFIGURASI SDK.....	Error! Bookmark not defined.
4.3.3 Update Pacakge SDK (Optional)	Error! Bookmark not defined.
4.3.4 Membuat Android Virtual Device (AVD)	Error! Bookmark not defined.
4.4 Pengujian Program	Error! Bookmark not defined.
4.4.1 Tampilan tombol menu	Error! Bookmark not defined.
4.4.2 Aplikasi Lain	Error! Bookmark not defined.
4.4.3 Pengujian antara pengirim dan penerima	Error! Bookmark not defined.

- 4.4.4 Hasil Uji Jarak Bluetooth **Error! Bookmark not defined.**
- 4.4.5 Tampilan awal**Error! Bookmark not defined.**
- 4.4.6 Tampilan tombol *help* **Error! Bookmark not defined.**
- 4.4.7 Pengujian Halaman Setelah *Bluetooth* Tersambung
Error! Bookmark not defined.
- 4.4.8 Pengujian Proses *Chatting* ... **Error! Bookmark not defined.**
- 4.4.9 Pengujian Enkripsi **Error! Bookmark not defined.**
- 4.4.10 Pengujian Dekripsi **Error! Bookmark not defined.**
- 4.5 Hasil Kuisisioner Uji Aplikasi **Error! Bookmark not defined.**
 - 4.5.1. Kecepatan Menginstal..... **Error! Bookmark not defined.**
 - 4.5.2. Kemudahan Tombol **Error! Bookmark not defined.**
 - 4.5.3. Kemudahan Petunjuk..... **Error! Bookmark not defined.**
 - 4.5.4. Kemudahan Pengoprasian... **Error! Bookmark not defined.**
 - 4.5.5. Kecepatan Penyampaian Data ... **Error! Bookmark not defined.**
 - 4.5.6. Keamanan Teks**Error! Bookmark not defined.**
 - 4.5.7. Tidak Adanya Biaya **Error! Bookmark not defined.**
 - 4.5.8. Manfaat Aplikasi ..**Error! Bookmark not defined.**

4.5.9. Kenyamanan Penggunaan Aplikasi	Error!
Bookmark not defined.	
4.5.10. Tampilan Aplikasi	Error! Bookmark not defined.
4.6 Penjelasan Format <i>Message</i>	Error! Bookmark not defined.
defined.	
BAB V	Error! Bookmark not defined.
PENUTUP	Error! Bookmark not defined.
5.1. Kesimpulan	Error! Bookmark not defined.
3.1. Saran	Error! Bookmark not defined.
DAFTAR PUSTAKA.....	Error! Bookmark not defined.
LAMPIRAN - LAMPIRAN	Error! Bookmark not defined.
DAFTAR RIWAYAT HIDUP	Error! Bookmark not defined.

DAFTAR GAMBAR

Gambar 2.1 Proses <i>Bluetooth</i>	9
Gambar 3.1 Garis Besar Sistem.....	19
Gambar 3.2 <i>Flowchart</i> Sistem Utama	21
Gambar 3.3 <i>Flowchart</i> pembangkitan kunci RSA	22
Gambar 3.4 Proses Enkripsi RSA	23
Gambar 3.5 Proses Dekripsi RSA	24
Gambar 4.1 Proses Eclipse	30
Gambar 4.2 Dialog add <i>repository</i>	31
Gambar 4.3 <i>Developer Tools</i>	31
Gambar 4.4 Lokasi direktori.....	32
Gambar 4.5 Kotak <i>Available software</i>	33
Gambar 4.6 <i>Interface</i>	34
Gambar 4.7 Proses Update SDK	35
Gambar 4.8 Available packages SDK	35
Gambar 4.9 Android <i>Repostory</i> SDK.....	36
Gambar 4.10 Pilihan Packages	36
Gambar 4.11 Proses Instalng	37
Gambar 4.12 Kotak Dialog AVD	37
Gambar 4.13 Pemilihan Memori	38
Gambar 4.14 Emulator Android	38
Gambar 4.15 Tampilan Tombol Menu.....	39
Gambar 4.16 <i>Software RSA</i>	40
Gambar 4.17 <i>Website RSA</i>	41
Gambar 4.18 Pengujian <i>Software</i>	41
Gambar 4.19 Tampilan Awal	43
Gambar 4.20 Tampilan <i>Help</i>	45
Gambar 4.21 Belum Tersambung.....	46
Gambar 4.22 Sudah tersambung.....	46
Gambar 4.23 Pengujian Proses <i>Chatting</i>	47
Gambar 4.24 Untuk memilih enkripsi atau tidak.....	48
Gambar 4.25 Setelah enkripsi.....	49
Gambar 4.26 Tombol pilihan Dekripsi	50
Gambar 4.27 Hasil dari Dekripsi	50

(Halaman ini Sengaja dikosongkan)

DAFTAR TABEL

Tabel 4.1. Pengujian Jarak *Bluetooth* 42

Tabel 4.2. Pengujian Aplikasi.....54

DAFTAR ISTILAH

- Chatting* : Merupakan aktivitas antara dua *user* melakukan percakapan dalam hal ini adalah obrolan melalui jaringan Internet.
- Kriptografi*: Sebuah cara atau metode untuk menjadikan informasi asli menjadi informasi yang tidak dapat dibaca
- Enkripsi* : Proses untuk menjadikan informasi asli menjadi informasi yang tidak dapat diartikan dalam proses kriptografi.
- Dekripsi* : Proses pengembalian dari informasi yang terenkripsi menjadi informasi asli.
- Chypertext* : Informasi yang telah disandikan atau informasi yang tidak dapat dibaca karena telah dienkripsi menggunakan metode kriptografi tertentu.
- Emulator* : Suatu perangkat lunak yang memungkinkan kita untuk menjalankan suatu program komputer di dalam sistem komputer lain yang berbeda.
- Smartphone* : Telepon cerdas adalah telepon genggam yang mempunyai kemampuan tingkat tinggi, Terkadang dengan fungsi menyerupai computer
- Plainteks* : Suatu jenis berkas komputer yang berupa teks tidak terformat

DAFTAR LAMPIRAN

Lampiran 1. <u>Hasil Uji Kuisisioner</u>	59
Lampiran 2. <u>Pengujian Enkripsi</u>	63
Lampiran 3. <u>Perhitungan Manual</u>	67
Lampiran 4. <u>Penjelasan Coding Program</u>	85

(Halaman ini Sengaja dikosongkan)