# APLIKASI KRIPTOSISTEM RSA PADA PROSES PENGKODEAN PESAN DENGAN URUTAN ABJAD TERBALIK

**SKRIPSI**


Oleh

**Muhammad Syirojul Mustaqiim**
**NIM 031810101042**



**JURUSAN MATEMATIKA**
**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM**
**UNIVERSITAS JEMBER**


**2011**

# APLIKASI KRIPTOSISTEM RSA PADA PROSES PENGKODEAN PESAN DENGAN URUTAN ABJAD TERBALIK

**SKRIPSI**

diajukan guna melengkapi tugas akhir dan memenuhi salah satu syarat
untuk menyelesaikan Program Studi Matematika (S1)
dan mencapai gelar Sarjana Sains


Oleh

**Muhammad Syirojul Mustaqiim**
**NIM 031810101042**



**JURUSAN MATEMATIKA**
**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM**
**UNIVERSITAS JEMBER**

**2011**

## PERSEMBAHAN

Dengan menyebut nama Allah Yang Maha Pengasih dan Maha Penyayang serta sholawat kepada Nabi Muhammad SAW, dengan setulus hati skripsi ini saya persembahkan kepada :

1. Kedua orang tua tercinta, Bapak Masturi dan Ibu Sukasih, yang telah memberikan segala cinta, kasih sayang, perhatian dan pengorbanan yang tiada henti, serta doa yang tak pernah putus dalam setiap langkah hidup ini;
2. Adik-adik tercinta, Dwi Esti dan Roufiq Azmy yang selalu memberi semangat, motivasi dan keceriaan dalam menuntut ilmu;
3. Guru-guru sejak Taman Kanak-kanak hingga Perguruan Tinggi, yang telah memberikan ilmu dan membimbing dengan penuh kesabaran;
4. Bapak Bambang Widarbo, yang telah mengenalkan matematika sebagai suatu seni yang memiliki keindahan untuk dipelajari;
5. Guru tercinta, K.H. Iqbal Ridwan yang telah memberi petunjuk, motivasi dan cahaya ilmu sebagai bekal menjalani kehidupan;
6. Ngalim, Edy, Wenang dan Dony serta rekan-rekan mahasiswa yang telah membantu dalam terselesaikannya skripsi;
7. Almamater Jurusan Matematika Fakultas MIPA Universitas Jember.

## MOTTO

Apabila di dalam diri seseorang masih ada rasa malu dan takut untuk berbuat suatu kebaikan, maka jaminan bagi orang tersebut adalah tidak akan bertemunya ia dengan kemajuan selangkah pun.
(Soekarno)

Tugas kita bukanlah untuk berhasil.
Tugas kita adalah untuk mencoba, karena didalam mencoba itulah kita menemukan dan belajar membangun kesempatan untuk berhasil.
(Mario Teguh)

## PERNYATAAN

Saya yang bertanda tangan dibawah ini :

nama : Muhammad Syirojul Mustaqiim

NIM : 031810101042

menyatakan dengan sesungguhnya bahwa skripsi yang berjudul "Aplikasi Kriptosistem RSA Pada Proses Pengkodean Pesan Dengan Urutan Abjad Terbalik" adalah benar-benar hasil karya sendiri, kecuali jika disebutkan sumbernya dan belum pernah diajukan pada institusi manapun, serta bukan karya jiplakan. Saya bertanggungjawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenarnya, tanpa adanya tekanan dan paksaan dari pihak manapun serta bersedia mendapat sanksi akademik jika ternyata di kemudian hari pernyataan ini tidak benar.

Jember, 10 Oktober 2011
Yang menyatakan,

Muhammad Syirojul Mustaqiim
NIM. 031810101042

**SKRIPSI**

# APLIKASI KRIPTOSISTEM RSA PADA PROSES PENGKODEAN PESAN DENGAN URUTAN ABJAD TERBALIK


Oleh :

Muhammad Syirojul Mustaqiim
NIM 031810101042


Pembimbing

Dosen Pembimbing Utama : Kiswara Agung Santoso, S.Si., M.Kom.

Dosen Pembimbing Anggota : Ahmad Kamsyakawuni, S.Si.

**PENGESAHAN**

Skripsi berjudul "Aplikasi Kriptosistem RSA Pada Proses Pengkodean Pesan dengan Urutan Abjad Terbalik" telah diuji dan disahkan pada :

hari, tanggal :

tempat : Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember

Tim Penguji:

| Ketua, | Sekretaris, |
|---|---|
| (Dosen Pembimbing Utama) | (Dosen Pembimbing Anggota) |
| Kiswara Agung Santoso, S.Si., M.Kom. | Ahmad Kamsyakawuni, S.Si. |
| NIP 197209071998031003 | NIP 197211291998021001 |
| Anggota I, | Anggota II, |
| Kosala Dwidja Purnomo, S.Si., M.Si. | Kusbudiono, S.Si., M.Si. |
| NIP 196908281998021001 | NIP 197704302005011001 |

Mengesahkan
Dekan,

Prof. Drs. Kusno, DEA., Ph.D.
NIP 196101081986021001

## RINGKASAN

**Aplikasi Kriptosistem RSA Pada Proses Pengkodean Pesan Dengan Urutan Abjad Terbalik;** Muhammad Syirojul Mustaqiim, 031810101042, 2011: 35 halaman; Jurusan Matematika FMIPA Universitas Jember.

Kemajuan teknologi komputer membantu semua aspek kehidupan manusia, dari hal yang kecil sampai ke berbagai hal yang sangat rumit sekalipun. Jaringan komputer seperti LAN dan internet memungkinkan tersedianya informasi secara cepat. Masalah keamanan dan kerahasiaan data merupakan hal yang sangat penting dalam suatu organisasi maupun pribadi. Oleh karena itu untuk mengatasi masalah ini dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi. Salah satu metode kriptografi yang digunakan adalah RSA. Nama RSA diambil dari nama penemunya yaitu Ron Rivest, Adi Shamir dan Leonard Adleman.

Masalah yang dikaji dalam skripsi ini adalah bagaimana mengaplikasikan kriptosistem RSA untuk mengkodekan pesan. RSA dipilih karena sebagai salah satu algoritma kunci publik yang terkenal aman. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor primanya yang dipakai sebagai dasar pembuatan algoritmanya. Sedangkan untuk data yang diolah adalah karakter berupa kombinasi abjad, angka dan tanda baca sebanyak 80 karakter yang dibangkitkan sendiri dan disusun secara unik, dimana penyusunan abjad dengan cara urutan terbalik

Tujuan dari penulisan skripsi ini adalah mengaplikasikan kriptosistem RSA untuk mengkodekan pesan dengan sistem pengkodean yang unik tetapi memiliki tingkat kerahasiaan yang tinggi, sehingga akan mempersulit proses pembacaan pesan yang dilakukan oleh pihak yang tidak berwenang.

Untuk mendapatkan hasil yang diinginkan maka dilakukan langkah-langkah penyelesaian masalah sebagai berikut: melakukan penyusunan karakter abjad terbalik, membuat rancangan aplikasi pengkodean RSA urutan abjad terbalik dan terakhir membuat program simulasi pengkodean pesan kriptosistem RSA urutan abjad terbalik. Program aplikasi disimulasikan menggunakan *software MATLAB 7.8.0 (R2009a)*.

Hasil dari kajian RSA dapat disimpulkan sebagai berikut, pemilihan dua bilangan prima sembarang pada proses awal pembentukan kunci harus memiliki hasil kali yang lebih besar dari nilai terbesar konversi karakter yang dibangkitkan, hal ini bertujuan untuk menjamin nilai konversi karakter cipherteks juga termuat pada karakter yang dibangkitkan. Pemilihan dua bilangan prima sembarang yang sangat besar juga akan menambah proses faktorisasi pada enkripsi dan dekripsi pesan, sehingga pesan lebih sulit dipecahkan dalam waktu yang singkat.

Dengan melakukan pembalikan urutan abjad, angka dan tanda baca yang tidak seperti penyusunan secara umumnya akan menghasilkan nilai cipherteks yang unik. Kriptosistem RSA dengan urutan abjad terbalik ini mengkodekan karakter abjad, angka dan tanda baca menjadi suatu nilai bilangan. Keamanan pesan akan tetap terjaga karena pembobol pesan tidak mengetahui sistem penyusunan karakter yang dibangkitkan secara unik dan jumlah karakter yang dipakai.

## PRAKATA

Puji syukur kehadirat Allah SWT atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Aplikasi Kriptosistem RSA Pada Proses Pengkodean Pesan Dengan Urutan Abjad Terbalik". Skripsi ini disusun untuk memenuhi salah satu syarat untuk menyelesaikan pendidikan strata satu (S1) pada Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

Penyusunan skripsi ini tidak lepas dari bantuan berbagai pihak, oleh karena itu penulis ingin menyampaikan terima kasih kepada :

1. Bapak Kiswara Agung Santoso, S.Si., M.Kom. dan Bapak Ahmad Kamsyakawuni, S.Si. selaku Dosen Pembimbing yang telah meluangkan waktu, pikiran, dan perhatian dalam penulisan skripsi ini;
2. Bapak Kosala Dwidja Purnomo, S.Si., M.Si., dan Bapak Kusbudiono, S.Si, M.Si. selaku Dosen Penguji yang telah memberikan segala masukan dan motivasi buat terselesaikannya skripsi ini;
3. Bapak Prof. Drs. Kusno, DEA., Ph.D. selaku Dekan Fakultas MIPA, yang telah memberikan pelajaran berharga akan pentingnya manajemen waktu, energi dan filosofi kehidupan;
4. Bapak Drs. Moh. Hasan, M.Sc, Ph.D. selaku Pembantu Dekan bidang Akademik yang telah membimbing dan memberi solusi serta motivasi bagi terselesaikannya studi ini;

Penulis juga menerima segala kritik dan saran dari semua pihak demi kesempurnaan skripsi ini. Akhirnya penulis berharap, semoga skripsi ini dapat bermanfaat.

Jember, Oktober 2011 Penulis

## DAFTAR ISI

Halaman

## DAFTAR LAMPIRAN

Halaman

# DAFTAR TABEL

Halaman

## DAFTAR GAMBAR

Halaman