PENERAPAN ALGORITMA TWOFISH UNTUK MEMBANGUN MODEL KRIPTOSISTEM

Skripsi

Diajukan sebagai syarat kelulusan jenjang Strata -1

Disusun oleh :

RETNO AJI WULANDARI

05.11.0936

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

STMIK AMIKOM YOGYAKARTA

2009

PENERAPAN ALGORITMA TWOFISH UNTUK MEMBANGUN MODEL KRIPTOSISTEM

SKRIPSI

Diajukan untuk memenuhi salah satu syarat dalam mencapai gelar Sarjana Strata Satu Teknik Informatika (S.Kom.)
pada Sekolah Tinggi Manajemen Informatika dan Komputer " AMIKOM " Yogyakarta

Oleh:

Retno Aji Wulandari

05.11.0936

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
"AMIKOM"
YOGYAKARTA
2009

HALAMAN PENGESAHAN

PENERAPAN ALGORITMA TWOFISH UNTUK MEMBANGUN MODEL KRIPTOSISTEM

Laporan Skripsi ini guna memenuhi syarat kelulusan pada program studi Strata Satu Teknik Informatika di Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM" Yogyakarta

Disahkan dan disetujui oleh :

Ketua STMIK "AMIKOM" Yogyakarta	Dosen Pembimbing
(Prof. Dr. M. Suyanto, MM)	(Emma Utami, S.Si, M.Kom)

PENGESAHAN SKRIPSI

Berjudul

PENERAPAN ALGORITMA TWOFISH UNTUK MEMBANGUN KRIPTOSISTEM

Oleh:

Retno Aji Wulandari

05.11.0936

Dipertahankan di hadapan Panitia Penguji Skripsi Jurusan Teknik Informatika AMIKOM Pada Tanggal : 20 Februari 2009

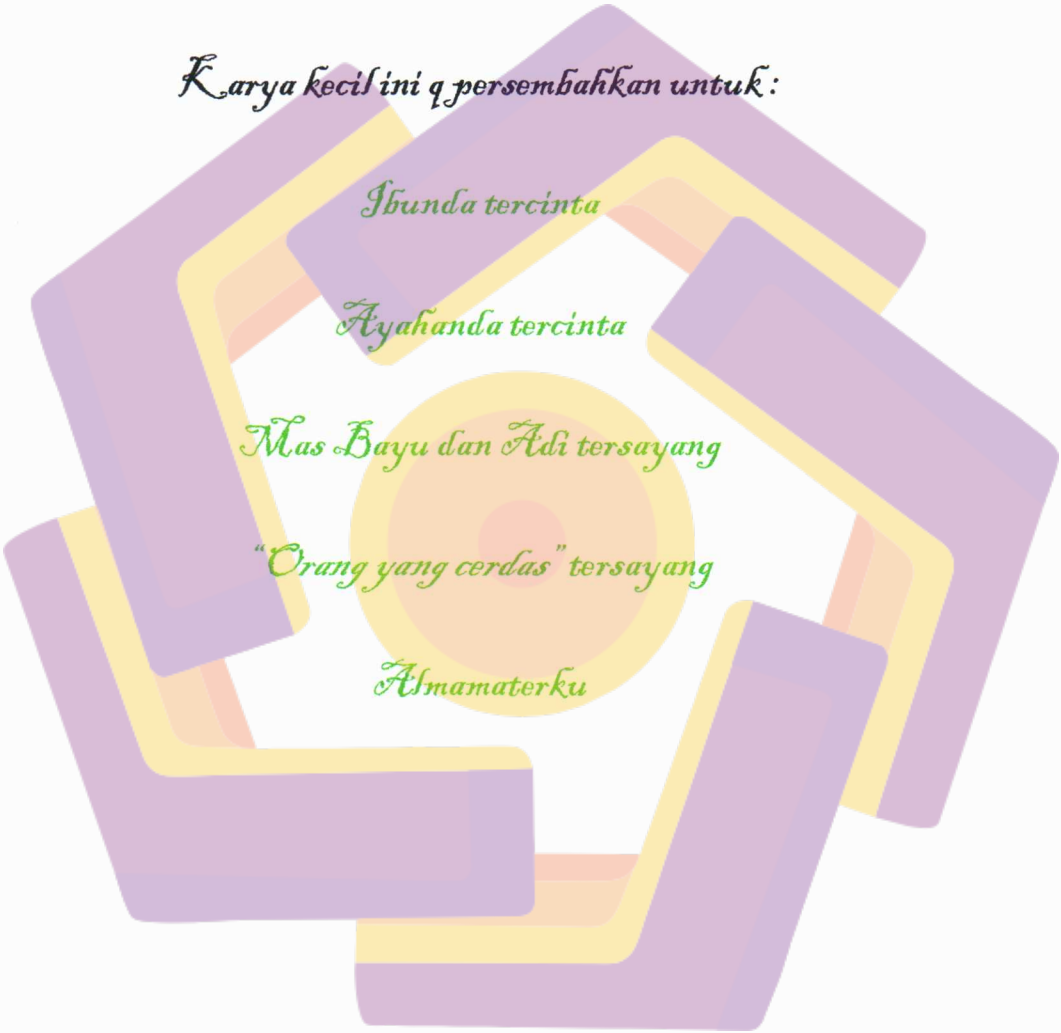
Pembimbing,

Emma Utami, S.Si, M.Kom.

Penguji I	Penguji II
M. Rudyanto Arief, ST, MT	Kusrini, M.Kom

Allah tidak mengabulkan doa dari hati yang lengah dan ragu

-(Muhammad SAW)-



KATA PENGANTAR

Alhamdulillah, puji syukur kehadirat Allah SWT atas limpahan rahmat dan kemudahan-Nya sehingga penulis dapat menyelesaikan laporan skripsi dengan judul Penerapan Algoritma Twofish Untuk Membangun Model Kriptosistem.

Penulisan Laporan ini dimaksudkan untuk melengkapi salah satu syarat dalam menyelesaikan studi di Jurusan Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM" Yogyakarta.

Penulis mengambil judul ini mengingat pesatnya perkembangan teknologi sehingga menuntut munculnya sebuah system pengamanan data yang dapat bekerja cepat. Penulis menggunakan algoritma Twofish dalam membangun model kriptosistem karena tingkat keamanan algoritma yang masih belum mampu diserang oleh *cryptanalis*.

Skripsi ini tidak akan terwujud tanpa bantuan dari berbagai pihak baik moral maupun material. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Mohammad Suyanto, MM selaku ketua Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM" Yogyakarta.
2. Bapak Ir. Abbas Ali Pangera, M.Kom, selaku ketua jurusan S1 Teknik Informatika STMIK "AMIKOM" Yogyakarta.

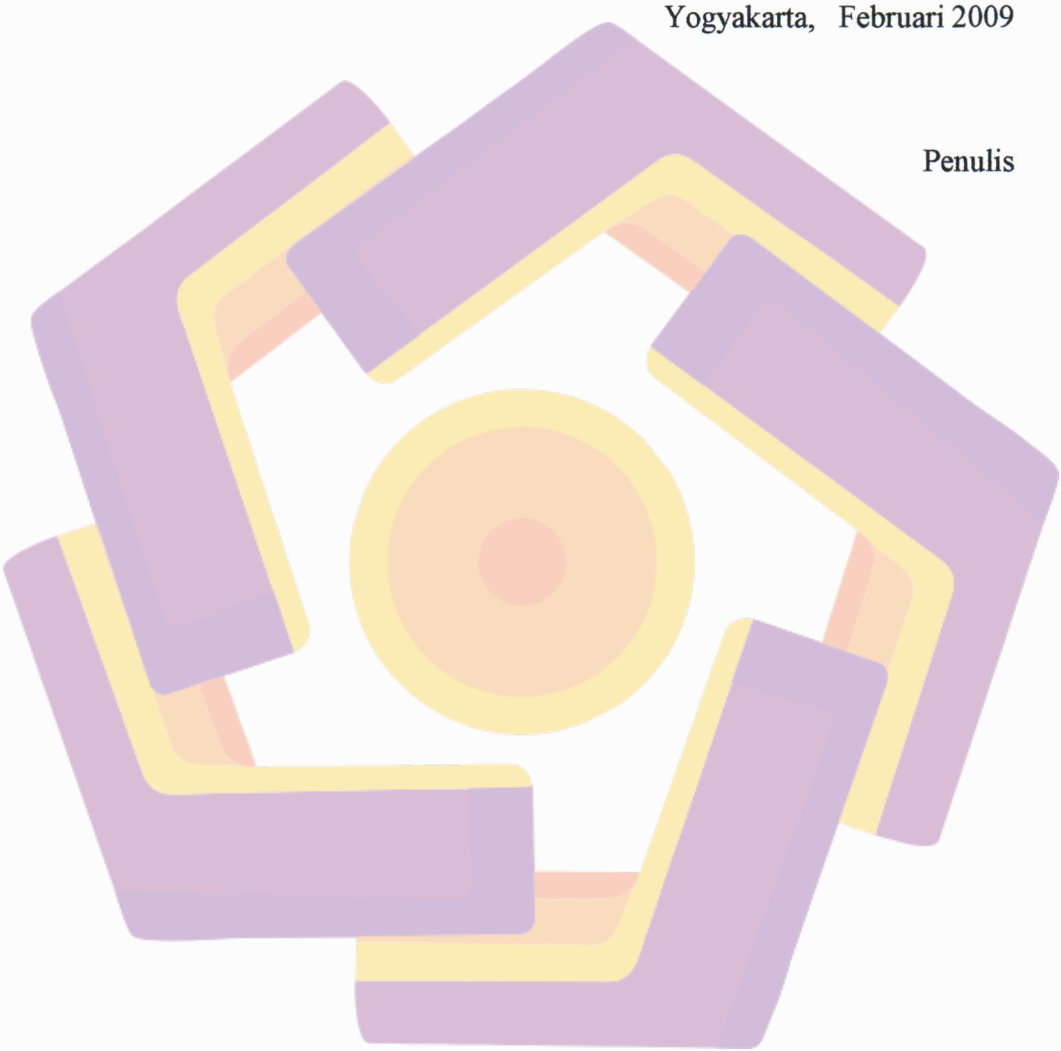
3. Ibu Emma Utami, S.Si, M.Kom, selaku dosen pembimbing yang senantiasa memberikan arahan, bimbingan, dan meluangkan waktu hingga penyusunan skripsi ini selesai.
4. Keluarga di rumah atas doa dan dukungan yang tak pernah putus.
5. "*Orang Yang Cerdas*", atas segala pengertian dan kasih sayangnya serta tuntutan sehingga penulis berhasil mengatur waktu dalam hidup ini. Tanpa-nya penulis akan tetap menjadi orang yang pemalas. Thanks for my sweetheart ☺
6. Keluarga besar Pondok Biru (*boloters*) atas segala pengertian dan semangat dari kalian semua. Mb Adis (kamar *refreshing*), Lili (kamar pengalaman pembantaian), Bela (kamar kerja dan inspirasi), Rida (kamar *sharing*), Icha (kamar perlengkapan IT), Anis (kamar kumpulan lagu jadul penambah semangat), Silvi (teman setia penghilang kepenatan), serta para leluhur pondok biru penulis belajar dari semangat kalian ☺
7. Teman seperjuangan : Even, Wafa, Arif, Robi, Desi.
8. Para penulis artikel tentang Twofish, Mas Deny (JUG), Mas Eko (eecchhoo), terimakasih untuk sharing ilmunya.
9. Teman-teman yang turut berperan dan senantiasa selalu memberi semangat hingga terselesaikannya skripsi ini.

Penulis sadar bahwa dalam penyusunan laporan skripsi ini masih banyak yang perlu dikoreksi lebih lanjut, maka penulis dengan senang hati menerima kritik dan

saran demi perubahan ke arah yang lebih baik. Semoga laporan ini dapat berperan sebagaimana mestinya, terutama bagi pembaca yang

Yogyakarta, Februari 2009

Penulis



DAFTAR ISI

Halaman

Halaman Judul ii

Halaman Persetujuan Dosen Pembimbing iii

Halaman Pengesahan iv

Halaman Persembahan v

Kata Pengantar vi

Daftar Isi vii

Daftar Gambar xi

Daftar Tabel xiii

BAB I PENDAHULUAN 1

1.1 Latar Belakang Masalah 1

1.2 Rumusan Masalah 3

1.3 Batasan Masalah 4

1.4 Tujuan Penelitian 5

1.5 Manfaat Penelitian 5

1.6 Metode Penelitian 5

1.7 Sistematika Penulisan 6

BAB II DASAR TEORI 8

2.1 Konsep Dasar Sistem Kriptografi 8

2.1.1 Enkripsi dan Dekripsi 9
2.1.2 Algoritma Kunci Simetrik 10
2.2 Chiper Blok 11
2.3 Algoritma Twofish 12
2.3.1 Dekripsi Twofish 12
2.3.2 Algoritma Twofish 13
2.3.2.1 Fungsi f 15
2.3.2.2 Fungi g 15
2.3.2.3 Penjadwalan Kunci 16
2.3.3 Kinerja Twofish 17
2.3.4 Keamanan Twofish 18
2.3.5 Kecepatan Kinerja Twofish 19
2.4 Perangkat Lunak Yang Digunakan 19
2.4.1 J2SE (Java Standart Edition) 20
2.4.2 Netbeans 6.5 20

BAB III PERANCANGAN DAN IMPLEMENTASI SISTEM 21
3.1 Analisa Perancangan Sistem 21
3.1.1 Kebutuhan Perangkat Lunak 21
3.1.2 Strategi Perancangan Perangkat Lunak 22
3.1.3 Deskripsi Perangkat Lunak 23
3.2 Perancangan Sistem 24

3.2.1 Flowchart Sistem 24
3.2.1.1 Bagan Alir Sistem 24
3.2.1.2 Bagan Alir Program 25
3.3 Perancangan Antar Muka 29
3.3.1 Halaman Utama 29
3.3.2 Halaman About 30
3.4 Implementasi Sistem 30

BAB IV UJI COBA SISTEM 35
4.1 Tujuan Uji Coba Sistem 35
4.1.1 Pengujian Key 36
4.1.2 Pengujian Enkripsi Terhadap Beberapa Tipe File 39
4.1.3 Pengujian Enkripsi Terhadap Beberapa Ukuran File 45
4.2 Pembahasan Masalah 47
4.2.1 Kecepatan Sistem 47
4.2.2 Kinerja Sistem 48
4.2.2.1 Cara Kerja Sistem 48
4.2.2.2 Kinerja Sistem 49
4.2.2.3 Kelebihan dan Kekurangan Sistem 51

BAB V PENUTUP 52
5.1 Kesimpulan 52

5.2 Saran 53

DAFTAR PUSTAKA 55