

Jurusan Teknik Informatika Program Studi Strata 1
Skripsi Sarjana Komputer dan Sarjana Sains
Semester Ganjil tahun 2007/2008

PERANCANGAN PROGRAM APLIKASI SISTEM
KEAMANAN FILE DATA MENGGUNAKAN
ALGORITMA *BLOWFISH*

Hendrikus Juan Fernando

0700722491

Abstrak

Berbagai macam layanan komunikasi tersedia di internet, diantaranya adalah *web*, *email*, *milis*, *newsgroups*, dan sebagainya. Dengan semakin maraknya orang memanfaatkan layanan komunikasi tersebut, maka permasalahan pun bermunculan, apalagi ditambah dengan adanya *hacker* dan *cracker*. Banyak orang kemudian berusaha menyiasati bagaimana cara mengamankan informasi yang dikomunikasikannya, atau menyiasati bagaimana cara mendeteksi keaslian dari informasi yang diterimanya. Untuk mengamankan data atau *message* diperlukan *cryptography* dengan metode *encryption*. Metode yang digunakan adalah Algoritma *Blowfish*.

Dalam penelitian ini akan disajikan analisis kinerja Algoritma *Blowfish* dan perancangan program aplikasi untuk mengamankan suatu *file* data. Untuk menenkripsi dan mendekripsi suatu *file* data, *user* harus menjalankan program aplikasi tersebut dan juga memberikan *key* sebagai kunci yang digunakan. Hasil penelitian menunjukkan bahwa program dapat digunakan untuk semua tipe *file* data tanpa ada kesalahan.

Kata kunci : data, *cryptography*, *encryption*, Algoritma *Blowfish*, program aplikasi, *file*, dekripsi, *key*.

PRAKATA

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Pengasih dan Penyayang atas anugrah dan kasih-Nya, sehingga penulis dapat menyelesaikan penyusunan skripsi yang berjudul "Perancangan Program Aplikasi Sistem Keamanan File Data Menggunakan Algoritma *Blowfish*" dalam rangka untuk memenuhi persyaratan penyelesaian Program Studi Ganda Jenjang Pendidikan Strata 1 di Universitas Bina Nusantara dengan baik dan tepat waktu.

Pada kesempatan ini penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada :

1. Bapak Prof. Dr. Drs. Gerardus Polla, M.App.Sc., selaku Rektor Universitas Bina Nusantara.
2. Bapak Wikaria Gazali, S.Si., M.T selaku Dekan dan Kajur Fakultas MIPA Universitas Bina Nusantara.
3. Bapak Fredy Purnomo, S.Kom., M.Kom., selaku Ketua Jurusan Teknik Informatika Universitas Bina Nusantara.
4. Bapak Ngarap Imanuel Manik, Drs., M.Kom., yang telah banyak membantu dalam proses pembuatan skripsi ini..
5. Bapak Sangadji, Drs., M.Sc., Ph.D, selaku dosen pembimbing pertama yang telah banyak memberikan saran, petunjuk, bimbingan, dan waktunya kepada penulis sehingga skripsi ini dapat diselesaikan dengan baik dan tepat waktu.

6. Bapak Syaeful Karim, Ir., M.Sc., selaku dosen pembimbing kedua yang telah banyak memberikan saran, petunjuk, bimbingan, dan waktunya kepada penulis sehingga skripsi ini dapat diselesaikan dengan baik dan tepat waktu.
7. Seluruh dosen yang telah meluangkan waktu dan memberikan bantuan kepada penulis dalam penyusunan skripsi ini.
8. Seluruh keluarga yang dengan penuh penuh perhatian dan kasih sayangnya, telah memberikan dorongan dan doa untuk dapat menyelesaikan penyusunan skripsi ini.
9. Rekan – rekan yang telah memberikan bantuan dan dorongan kepada penulis dalam penyusunan skripsi ini.
10. Semua pihak lainnya yang tidak dapat penulis sebutkan satu persatu, yang telah memberikan berbagai nasehat, saran, petunjuk dan dukungan kepada penulis sehingga penulis dapat menyelesaikan penyusunan skripsi ini.

Penulis menyadari bahwa skripsi yang telah dibuat dengan sebaik - sebaiknya ini masih memiliki kekurangan. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang sifatnya membangun untuk dapat menyempurnakan skripsi ini. Penulis juga ingin mengucapkan terima kasih kepada semua pihak yang bersedia meluangkan waktunya untuk membaca skripsi ini. Akhir kata penulis berharap semoga skripsi ini dapat bermanfaat bagi semua pihak yang memerlukannya.

Hendrikus Juan Fernando
0700722491

Jakarta, Januari 2008

DAFTAR ISI

	Halaman
ABSTRAK	iv
PRAKATA	v
DAFTAR ISI	vii
BAB 1 : PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Ruang Lingkup	2
1.4 Tujuan dan Manfaat	3
1.4.1 Tujuan	3
1.4.2 Manfaat	3
1.5 Metodologi	3
1.6 Sistematika Penulisan	4
BAB 2 : LANDASAN TEORI	
2.1 Konsep Dasar Kriptografi	6
2.2 Konsep Matematis dalam Kriptografi	10
2.3 Tujuan Kriptografi	11
2.4 Algoritma Simetrik	13
2.5 Algoritma <i>Public-Key</i>	13

2.6	Algoritma <i>Blowfish</i>	14
2.6.1	Enkripsi Algoritma <i>Blowfish</i>	14
2.6.2	Dekripsi Algoritma <i>Blowfish</i>	17
2.7	Jaringan Feistel	18
2.8	Bidang-Bidang Aplikasi	19
2.9	<i>Platform</i>	19
2.10	Membangkitkan <i>Sub-Key</i>	20
2.11	Kriteria Rancangan Algoritma <i>Blowfish</i>	22

BAB 3 : ANALISIS DAN PERANCANGAN PROGRAM

3.1	Gambaran Umum Perancangan Program	23
3.2	Rancangan Layar Program	24
3.3	Struktur Menu Perancangan Layar	26
3.4	<i>State Transition Diagram</i>	27
3.5	<i>Flowchart</i>	28

BAB 4 : IMPLEMENTASI DAN HASIL PERANCANGAN

4.1	Spesifikasi Kebutuhan Sarana	29
4.1.1	Spesifikasi Perangkat Keras yang Dibutuhkan	29
4.1.2	Spesifikasi Perangkat Lunak yang Dibutuhkan	29
4.2	Persiapan Data	30
4.3	Pengujian Program Aplikasi	30
4.4	Kelebihan dan Kekurangan Program Aplikasi	36

BAB 5 : KESIMPULAN DAN SARAN

5.1 Kesimpulan	37
5.2 Saran	38
DAFTAR PUSTAKA	40
RIWAYAT HIDUP	41
LAMPIRAN	L-1

DAFTAR GAMBAR

2.1 Konsep Kriptografi Secara Umum	7
2.2 Blok Diagram Algoritma Enkripsi <i>Blowfish</i>	15
2.3 Fungsi F	16
2.4 Blok Diagram Dekripsi <i>Blowfish</i>	17
3.1 Rancangan Layar Halaman Pembuka	24
3.2 Rancangan Layar Halaman Utama	25
3.3 Rancangan Layar Halaman Penutup	26
3.4 Struktur Menu	26
3.5 <i>State Transition Diagram</i>	27
3.6 <i>Flowchart</i>	28
4.1 <i>Preview File</i> test1.txt Sebelum Enkripsi	30
4.2 <i>Preview Program</i> Enkripsi test1.txt Menjadi hasil1.txt	31
4.3 <i>Preview</i> hasil1.txt Hasil Enkripsi Dari test1.txt	31
4.4 <i>Preview Program</i> Dekripsi hasil1.txt Menjadi balik1.txt	32
4.5 <i>Preview File</i> balik1.txt Hasil Dekripsi Dari hasil1.txt	32
4.6 <i>Preview File</i> test2.jpg Sebelum Enkripsi	33
4.7 <i>Preview Program</i> Enkripsi test2.jpg Menjadi hasil2.jpg	33
4.8 <i>Preview</i> hasil2.jpg Hasil Enkripsi Dari test2.jpg	34
4.9 <i>Preview Program</i> Dekripsi hasil2.jpg Menjadi balik2.jpg	34
4.10 <i>Preview File</i> balik2.jpg Hasil Dekripsi Dari hasil2.jpg	35