

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Allah SWT yang telah memberikan hidayah dan rahmat-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul "Aplikasi Pengamanan Data Berbasis File Menggunakan Triple Des" dengan baik.

Laporan tugas akhir ini dibuat untuk memenuhi persyaratan penilaian sebagai salah satu syarat kelulusan pada program studi (D3) program studi "Akademi Teknik Telekomunikasi Shandy Putra Jakarta".

Semoga laporan ini dapat memberi manfaat kepada pembaca walaupun masih sangat terbatas kemampuan dan ilmu penulis dalam membuat laporan hingga laporan ini masih jauh dari kesempurnaan.

Pada kesempatan kali ini penulis ingin mengucapkan terima kasih sedalam-dalamnya kepada semua pihak yang telah memberi inspirasi, dukungan moril dan do'a bagi penulis hingga selesainya penulis laporan tugas akhir ini. Tidak banyak yang penulis perbuat untuk membalas budi baik selain do'a dan ungkapan terima kasih.

Pada kesempatan ini ungkapan terima kasih penulis sampaikan kepada :

1. Keluarga yang telah memberikan dorongan baik moril maupun materil.
2. H.M.Soleh Hapudin, ST., selaku Dosen Pembimbing I Tugas Akhir Program Studi (D3), Akademi Teknik Telekomunikasi Shandy Putra Jakarta.
3. Teman-teman mahasiswa Akademi Teknik Telekomunikasi Shandy Putra Jakarta, Khususnya angkatan VII, Yang telah membantu dan memberikan dorongan hingga penulis ini dapat diselesaikan.
4. Semua pihak yang tidak dapat penulis sebutkan satu persatu yang telah membantu baik secara langsung maupun tidak langsung.

Penulis menyadari sepenuhnya bahwa laporan tugas akhir ini tidak terlepas dari kesalahan dan kekurangan untuk itu, kritik dan saran yang membangun dalam penulisan ini sangat penulis harapkan. Semoga laporan ini dapat bermanfaat bagi pihak yang membutuhkannya.

Jakarta, 19 Agustus 2011



Budi Irawan Prima Putra

DAFTAR ISI

Halaman Pengesahan	i
Lembar Plagiarisme	ii
Lembar Publikasi	iii
Abstrak	iv
Abstract	v
Kata Pengantar	vi
Daftar Isi	vii
Daftar Gambar	x
Daftar Tabel	xi
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Tujuan Penelitian	2
1.3 Perumusan Masalah	2
1.4 Pembatasan Masalah	2
1.5 Metodologi	2
1.6 Sistematika Penulisan	2
BAB II TRIPLE DES	
2.1 Sejarah Kriptografi	4
2.2 Pengertian dan Tujuan Kriptografi	5
2.3 Keamanan Algoritma Kriptografi	6
2.4 Teknik-Teknik kriptografi	7
2.5 Algoritma Kriptografi	8
2.5.1 Algoritma Simetris	8
2.5.1.1 DES (<i>Data Encryption Standard</i>)	10
2.5.1.2 Triple DES (Tiga Kali DES)	12
2.5.2 Algoritma Asimetris	14
2.6 Enkrip dan Dekripsi	15
2.7 Model Sukensial Linier	17
2.8 Visual Basic NET	18
2.8.1 Sejarah Visual Basic	18
2.8.2 IDE Visual Basic	19
2.8.3 Struktur Project	21

2.8.4	Memahami Istilah Project, Property, Method, dan Event	22
2.9	Diagram Use Case	22
2.10	Diagram Konteks	23
2.11	Kriptografi dalam VB.NET	24
2.11.1	Menggunakan Class-Class Enkripsi.NET	25

BAB III APLIKASI PENGAMANAN DATA BERBASIS FILE MENGGUNAKAN TRIPLE DES

3.1	Proses Aplikasi	27
3.1.1	Algoritma Triple DES	27
3.1.2	Proses Enkripsi	29
3.1.3	Proses Dekripsi	29
3.2	Perancangan Sistem	30
3.2.1	Perancangan Diagram Blok	30
3.2.2	Perancangan Flowchart	31
3.2.2.1	Flowchart Layar Utama	31
3.2.2.2	Flowchart Proses Enkripsi	32
3.2.2.3	Flowchart Proses Dekripsi	33
3.3	Perancangan Aplikasi	35
3.3.1	Rancangan Halaman Utama	36
3.3.2	Rancangan Proses Enkripsi	37
3.3.3	Rancangan Proses Dekripsi	38
3.3.4	Rancangan Halaman About	39

BAB IV PERANCANGAN PENGAMANAN DATA BERBASIS TEKS MENGGUNAKAN TRIPLE DES

4.1	Implementasi	40
4.1.1	Spesifikasi Kebutuhan Sistem	40
4.1.2	Implementasi Kode Program	41
4.1.3	Implementasi Program	45
4.1.3.1	Halaman Menu Utama	46
4.1.3.2	Halaman Proses Enkripsi	47
4.1.3.3	Halaman Proses Dekripsi	48
4.1.3.4	Halaman Untuk mencari atau membuka file	49
4.1.3.5	Halaman Untuk Menyimpan File Terenkripsi	50

DAFTAR GAMBAR

Gambar 2.1 Skema Algoritma Simetris	9
Gambar 2.2 Tabel Pergeseran Caesar key	9
Gambar 2.3 Skema Global DES	10
Gambar 2.4 Jaringan Feistel untuk satu putaran DES	11
Gambar 2.5 Algoritma Enkripsi dengan DES	11
Gambar 2.6 Diagram Enkripsi dan Dekripsi 3DES dengan 2 Buah Kunci	13
Gambar 2.7 Diagram Enkripsi dan Dekripsi 3DES dengan 3 Buah Kunci	13
Gambar 2.8 Skema Algoritma Asimetris	14
Gambar 2.9 Proses Enkripsi dan Dekripsi Sederhana	15
Gambar 2.10 Proses Enkripsi dan Dekripsi dengan Menggunakan Kunci	16
Gambar 2.11 Proses Enkripsi dan Dekripsi dengan Dua Kunci Berbeda	17
Gambar 2.12 Tampilan Halaman Star Page	19
Gambar 2.14 Tampilan Ruang Kerja Visual Basic 2005 Express Edition	20
Gambar 2.15 Notasi diagram use case	23
Gambar 2.16 Contoh diagram use case	23
Gambar 2.17 Contoh diagram Konteks	23
Gambar 3.1 Algoritma Triple DES	29
Gambar 3.2 Diagram Blok Triple DES	30
Gambar 3.3 Flowchart Tampilan Layar Utama	32
Gambar 3.4 Flowchart Tampilan Layar Proses Enkripsi	33
Gambar 3.5 Flowchart Tampilan Layar Proses Dekripsi	34
Gambar 3.6 Desain Antar Muka Halaman Utama	36
Gambar 3.7 Desain Antar Muka Halaman Proses Enkripsi	37
Gambar 3.8 Desain Antar Muka Halaman Proses Dekripsi	38
Gambar 3.9 Desain Antar Muka Halaman About	39
Gambar 4.1 Halaman Menu Utama	46
Gambar 4.2 Halaman Proses Enkripsi	47
Gambar 4.3 Halaman proses Dekripsi	48
Gambar 4.5 Halaman Buka File	49
Gambar 4.6 Halaman Simpan File	50
Gambar 4.7. Proses Enkripsi	57
Gambar 4.8. Hasil Enkripsi	57
Gambar 4.9. Proses Dekripsi	58
Gambar 4.10. Hasil Dekripsi	58

4.2	Pengujian	50
4.2.1	Skenario Pengujian	51
4.2.2	Hasil Pengujian	53
4.2.3	Analisis hasil pengujian	56
4.2.4	Analisa hasil perbandingan	56
BAB V PENUTUP		
5.1	Kesimpulan	59
5.2	Saran	59
DAFTAR PUSTAKA		xii

DAFTAR TABEL

Tabel 2.9 Komponen Kriptografi	24
Tabel 2.9 Tipe-Tipe Enkripsi Dalam.NET	25
Tabel 4.1 Spesifikasi Perangkat Keras	40
Tabel 4.2 Spesifikasi Perangkat Lunak	40
Tabel 4.2.1 Skenario Pengujian	51
Tabel 4.2.2 Hasil Pengujian	53
Tabel 4.2.3 Hasil Pengujian Proses Enkripsi	54
Tabel 4.2.4 Hasil Pengujian proses Dekripsi	55