

**SIMULASI PROSES ENKRIPSI-DESKRIPSI DENGAN
MENGUNAKAN METODE KRIPTOGRAFI WAKE
(*WORD AUTO KEY ENCRYPTION*)**

TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Persyaratan

Menyelesaikan Program Studi Strata Satu (S1)

Program Studi Teknik Informatika



Disusun Oleh :

Nama : Nurul Amri

Nim : 41505010011

**JURUSAN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
2011**



**SIMULASI PROSES ENKRIPSI-DESKRIPSI DENGAN
MENGUNAKAN METODE KRIPTOGRAFI WAKE
(*WORD AUTO KEY ENCRYPTION*)**

Oleh:

Nurul Amri

41505010011

**JURUSAN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA**

2011

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41505010011
Nama : Nurul Amri
Fakultas : Ilmu Komputer
Program Studi : Teknik Informatika
Judul Skripsi : **SIMULASI PROSES ENKRIPSI-DESKRIPSI
DENGAN MENGGUNAKAN METODE WAKE
(WORD AUTO KEY ENCRYPTION)**

Menyatakan bahwa skripsi ini tersebut diatas adalah hasil karya saya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 2011

(Nurul Amri)

LEMBAR PENGESAHAN

NIM : 41505010011
Nama : Nurul Amri
Judul Skripsi : **SIMULASI PROSES ENKRIPSI-DESKRIPSI
DENGAN MENGGUNAKAN METODE WAKE
(WORD AUTO KEY ENCRYPTION)**

Skripsi ini telah diperiksa dan disetujui.

Jakarta, 2011

Raka Yusuf, ST.,MT

Pembimbing

Ida Nurhaida, ST.,MTI

Koord. Tugas Akhir Teknik Informatika

Devi Fitriyah, S.KOM.,MTI

Kaprodi Teknik Informatika

KATA PENGANTAR

Terima kasih kepada Tuhan yang Maha Esa, karena berkat rahmat dan karunia-Nya lah penulis dapat menyelesaikan penulisan tugas akhir ini. Penulisan tugas akhir ini dimaksudkan untuk memenuhi sebagian syarat-syarat dalam menyelesaikan Program Strata Satu (S1) pada program Studi Teknik Informatika Universitas Mercu Buana.

Penulis menyadari penulisan tugas akhir ini tidak lepas dari bantuan berbagai pihak, baik dari segi material maupun spiritual. Atas segala bimbingan, dorongan, dan bantuan baik secara langsung maupun tidak langsung yang telah diberikan, maka penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Kedua orang tuaku yang telah banyak mendidik, memberikan kasih sayang, mendoakan serta yang selalu memberi dorongan baik materi maupun moral, sehingga aku merasa bersyukur dan bangga memiliki orang tua seperti mereka.
2. Ibu Devi Fitriyah, S.KOM.,MTI., selaku Ketua Program Studi Teknik Informatika, Universitas Mercu Buana.
3. Ibu Nurhaida, ST.,MTI., selaku Koordinator Tugas Akhir Jurusan Teknik Informatika, Universitas Mercu Buana.
4. Bapak Raka Yusuf, ST.,MT., Dosen Pembimbing tugas akhir penulis, yang telah berkenan meluangkan waktunya serta memberi dukungan dan pengarahan hingga laporan tugas akhir ini selesai.
5. Kedua kakak tersayang Reni Wahyuni, Fitriyah dan juga kedua orang tua Bapak H. Maman Sutarnan dan Hj. Tati Maryati atas segala Doa, kesabaran, dan motivasinya sehingga penulis selalu mempunyai semangat dalam menyelesaikan tugas akhir ini.
6. Keluarga besar tercinta yang telah memberi banyak semangat dan dorongan baik moral maupun materi.
7. Sahabat-sahabatku angkatan 2005 di Mercu Buana khususnya Jurusan Teknik Informatika yang telah rela dalam membagi pengalaman dan ilmu kepada penulis.
8. Semua pihak yang telah memberikan dorongan dan membantu serta memberikan saran kepada penulis sehingga laporan ini dapat terselesaikan.

Akhir kata dengan segala kerendahan hati penulis memohon maaf yang sebesar-besarnya atas kekurangan dan keterbatasan yang terdapat dalam laporan tugas akhir ini dan untuk itu semua saran dan kritik yang sifatnya membangun sangat diharapkan demi kesempurnaan tugas akhir ini serta besar harapan penulis semoga laporan tugas akhir ini dapat bermanfaat bagi pihak-pihak yang membutuhkan.

Jakarta, 2011

Penulis

DAFTAR ISI

	Halaman
LEMBAR PERNYATAAN	i
LEMBAR PENGESAHAN.....	ii
KATA PENGANTAR.....	iii
ABSTRAK.....	v
ABSTRACT	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xii
BAB I PENDAHULUAN	
1.1. Latar Belakang	1
1.2. Perumusan Masalah.....	3
1.3. Batasan Masalah.....	3
1.4. Tujuan Penelitian.....	4
1.5. Manfaat Penelitian.....	4
1.6. Metode Penelitian.....	4
1.7. Sistematika Penulisan	5
BAB II LANDASAN TEORI	
2.1 Teknik Simulasi.....	7
2.1.1 Kelebihan Dan Kekurangan Model Simulasi	10
2.1.2 Tipe Model Simulasi	11
2.1.2.1 Statis Vs Dinamis	11
2.1.2.2 Stokastik Vs Deterministik	11
2.1.2.3 Kontinu Vs Diskrit	11

2.2	Teori Kriptografi	12
2.3	Sistem Kriptografi	14
2.3.1	Algoritma Simetris	14
2.3.2	Algoritma Asimetris	15
2.4	Matematika Kriptografi	16
2.4.1	AND	16
2.4.2	OR	17
2.4.3	XOR.....	17
2.4.4	Penjumlahan Modulo.....	18
2.4.5	Pergeseran Bit (Shift)	18
2.4.6	Konversi Bilangan Berbasis.....	19
2.4.7	Konversi Bilangan Biner ke Bilangan Heksadesimal	19
2.4.8	Konversi Bilangan Heksadesimal ke Bilangan Biner	20
2.5	WAKE (Word Auto Key Encryption).....	20
2.5.1	Proses Pembentukan Tabel S-Box	21
2.5.2	Proses Pembentukan Kunci.....	21
2.5.3	Proses Enkripsi dan Dekripsi	21
2.6	Visual Basic Programming	22
2.7	Metodologi Rekayasa Perangkat Lunak	24
2.7.1	Diagram Use Case	25
2.7.2	Diagram Aktifitas	27
2.8	Pengujian	28
2.8.1	Pengujian BlackBox	29
2.8.2	Pengujian WhiteBox.....	29

BAB III ANALISA DAN PERANCANGAN SISTEM

3.1	Metode Analisis.....	31
3.1.1	Analisis Kebutuhan	32
3.1.2	Kebutuhan Antar Muka	33
3.1.3	Pembentukan Tabel S-Box	33
3.2	Metode Perancangan	36
3.2.1	Proses Pembentukan Tabel S-Box	37
3.2.2	Proses Pembentukan Kunci.....	37
3.2.3	Proses Enkripsi.....	37
3.2.4	Proses Dekripsi.....	38
3.3	Analisis Pemodelan Sistem.....	39
3.3.1	Diagram Use Case.....	39
3.3.2	Diagram Aktifitas	42
3.4	Perancangan Antar Muka (Interface)	43

BAB IV IMPLEMENTASI DAN PENGUJIAN

4.1	Implementasi.....	45
4.1.1	Implementasi Aplikasi.....	45
4.1.1.1	Pengkodean.....	45
4.1.1.2	Tampilan Layar	55
4.2	Pengujian	56
4.2.1	Lingkungan Pengujian.....	56
4.2.2	Pengujian BlackBox	57
4.2.3	Pengujian WhiteBox.....	59
4.2.4	Analisis Hasil Pengujian.....	60

BAB V PENUTUP	
5.1 Kesimpulan	61
5.2 Saran	62
DAFTAR PUSTAKA	63
LAMPIRAN	64

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Posisi Simulasi Dalam Studi Sistem.....	8
Gambar 2.2 Hubungan Simulasi dengan Pemodelan.....	9
Gambar 2.3 Diagram Proses Enkripsi Dan Dekripsi	13
Gambar 2.4 Model Sederhana Sistem Kriptografi Simetris.....	15
Gambar 2.5 Model Sederhana Sistem Kriptografi Asimetris	16
Gambar 3.1 Flowchart Enkripsi.....	38
Gambar 3.2 Flowchart Dekripsi	39
Gambar 3.3 Diagram Use Case	40
Gambar 3.4 Diagram Aktifitas Simulasi Kriptografi WAKE	43
Gambar 3.5 Interface Simulasi Kriptografi WAKE	44
Gambar 4.1 Tampilan Simulasi Kriptografi WAKE	55
Gambar 4.2 Pengujian WhiteBox Kriptografi WAKE	59

DAFTAR TABEL

	Halaman
Tabel 2.1 Aturan Operasi AND	16
Tabel 2.2. Aturan Operasi OR.....	17
Tabel 2.3 Aturan Operasi XOR	17
Tabel 2.4 Jenis Diagram Resmi UML	24
Tabel 2.5 Notasi Pemodelan Diagram Use Case.....	26
Tabel 2.6 Simbol-Simbol Pada Diagram Aktifitas	28
Tabel 4.1 Skenario Pengujian BlackBox	57
Tabel 4.2 Hasil Pengujian BlackBox	58
Tabel 4.3 Tabel Matrix Pengujian Whitebox	60