

PENGAMANAN DATA DENGAN METODA KRIPTOGRAFI IDEA

SKRIPSI

**Disusun Untuk Melengkapi dan Memenuhi Syarat Kelulusan Program Strata 1
Jurusan Teknik Informatika Fakultas Teknik
Universitas Muhammadiyah Jember**



Oleh :
ADITYA PRATAMA 1010652001

**JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER
2013**

HALAMAN PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Laporan Tugas Akhir ini penulis persembahkan untuk:

*Kedua Orangtua dan Saudara-Saudara kami yang
sangat kami sayangi*

*Teman-teman satu angkatan yang selalu memberiku
semangat untuk menyelesaikan tugas akhir ini*

*Almamater Fakultas Teknik Universitas Muhammadiyah
Jember*

PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama : Aditya Pratama

NIM : 1010652001

Menyatakan dengan sesungguhnya bahwa karya Ilmiah yang berjudul “**Pengamanan Data dengan Metoda Kriptografi IDEA**” adalah benar-benar karya sendiri kecuali kutipan yang sudah saya sebutkan sumbernya, belum pernah diajukan pada institusi manapun, dan bukan karya jiplakan. Saya bertanggung jawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus 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, Januari 2013

Aditya Pratama

NIM: 1010652001

HALAMAN PENGESAHAN

PENGAMANAN DATA DENGAN METODA KRIPTOGRAFI IDEA

Oleh :

**ADITYA PRATAMA
1010652001**

**Proyek Akhir Ini Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Komputer (S.Kom)**

*di
Universitas muhammadiyah Jember*

Disetujui oleh :

Tim Penguji

Dosen Pembimbing ,

**1. Zainul Arifin, S.Si
NPK. 12 03 714**

**1. Daryanto, S.Kom
NPK. 11 03 589**

**2. Hardian Oktavanto, S.Si
NPK. 12 03 715**

**2. Lutfi Ali Muharrom, S.Si
NPK. 10 09 550**

Jember, Januari 2013

Mengetahui

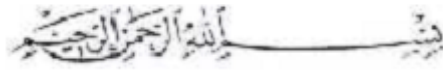
Dekan Fakultas Teknik

Ketua Jurusan Teknik Informatika,

**Ir. Kuswardani, MT
NPK. 93 01 379**

**Taufik Timur Warisaji, S.Kom, M.Kom
NPK. 08 04 846**

KATA PENGANTAR



Puji syukur kita panjatkan kehadiran Allah SWT atas rahmat dan karuniaNya yang telah dilimpahkan sehingga kami bisa menyelesaikan Laporan Tugas Akhir. Penyusunan Laporan Tugas Akhir Disusun Untuk Melengkapi dan Memenuhi Syarat Kelulusan Program Strata 1 Jurusan Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember dan juga sebagai syarat untuk memperoleh Gelar Sarjana Komputer (S.Kom).

Ucapan terima kasih penulis sampaikan kepada pihak-pihak yang telah membantu penulis, baik selama pembuatan aplikasi maupun selama penyusunan Laporan Tugas Akhir, di antaranya :

1. Bapak Daryanto dan Bapak Lutfi dosen pembimbing,
2. Para Dosen Fakultas Teknik Informatika, terima kasih atas semua ilmu yang telah diberikan,
3. Teman-teman yang telah mendukung dan memberi semangat kepada penulis, khususnya Pak Edy, Mas Faiz, dan Mas Afiadi,
4. Keluarga penulis dan La'aliy Afida yang telah memberikan do'a dan juga bantuan secara moril dan materil,
5. Serta pihak-pihak yang telah membantu dan tidak dapat penulis sebutkansatu persatu.

Penulis menyadari bahwa masih banyak kekurangan dan kelemahan dalam penyusunan Laporan Skripsi ini. Oleh karena itu, kami mengharapkan kritik dan saran yang membangun dan menambah wawasan dan wacana ilmu kami. Besar harapan kami laporan ini dapat bermanfaat bagi semua pihak dan dapat dimanfaatkan sebaik-baiknya.

Jember,

Penulis

Pengamanan Data dengan Metoda Kriptografi IDEA

^{1.} *Aditya Pratama (1010652001)*

^{2.} *Daryanto, S.Kom.,*

^{3.} *Lutfi Ali M, S.Si.*

Jurusan Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember

Email : aditya.pratama487@yahoo.co.id

ABSTRAK

Dalam sebuah masalah kerahasiaan data, data yang rahasia harus diamankan terlebih dahulu dengan berbagai macam cara, salah satunya adalah dengan menggunakan metoda kriptografi. Salah satu metoda kriptografi yang dianggap sebagai algoritma block cipher yang terbaik dan teraman yang tersedia untuk publik sampai saat ini adalah metoda kriptografi IDEA (International Data Encryption Algorithm). Metoda ini terdiri dari 8 putaran (round) dan menggunakan 64 bit plaintext dengan panjang kunci sebesar 128 bit. Yang menjadi permasalahan dalam menyusun tugas akhir (skripsi) ini adalah bagaimana merancang perangkat lunak pembelajaran metoda kriptografi IDEA yang telah dikembangkan dengan inputan plaintext lebih kecil dan lebih besar dari 64 bit (32 bit dan 128 bit). Sehingga nantinya menghasilkan sebuah aplikasi metoda kriptografi IDEA yang telah dikembangkan dengan inputan plaintext lebih kecil dan lebih besar dari 64 bit (32 bit dan 128 bit).

Kata kunci : *Kriptografi, IDEA, Plaintext.*

Data Security with Cryptography IDEA Method

^{1.} *Aditya Pratama (1010652001)*

^{2.} *Daryanto, S.Kom.,*

^{3.} *Lutfi Ali M, S.Si.*

Informatics Departement of Engineering Faculty,

Universitas Muhammadiyah Jember

Email : aditya.pratama487@yahoo.co.id

ABSTRACT

In a matter of data secrecy, confidential data should be secured in advance in various ways, one of which is by using cryptographic methods. One of the methods of cryptographic block cipher algorithm is considered as the best and safest available to the public until now is a cryptographic method IDEA (International Data Encryption Algorithm). This method consists of 8 rounds (round) and use the 64 bit plaintext with a key length of 128 bits. The problem in compiling the final project (thesis) is how to design learning software IDEA cryptographic method that has been developed with the input plaintext smaller and larger than 64 bits (32 bits and 128 bits). So will result in an application IDEA cryptographic method that has been developed with the input plaintext smaller and larger than 64 bits (32 bits and 128 bits).

Keywords: Cryptography, IDEA, Plaintext.

DAFTAR ISI

	Halaman
HALAMAN JUDUL.....	i
HALAMAN PERSEMBAHAN	74
PERNYATAAN.....	75
HALAMAN PENGESAHAN.....	76
KATA PENGANTAR	77
ABSTRAK	78
DAFTAR ISI.....	80
DAFTAR TABEL.....	83
DAFTAR GAMBAR	84
BAB I.....	Error! Bookmark not defined.
PENDAHULUAN	Error! Bookmark not defined.
1.1 Latar Belakang Pemilihan Judul	Error! Bookmark not defined.
1.2 Perumusan Masalah	Error! Bookmark not defined.
1.3 Tujuan dan Manfaat	Error! Bookmark not defined.
1.4 Pembatasan Masalah	Error! Bookmark not defined.
1.5 Sistematika Penulisan	Error! Bookmark not defined.
BAB II.....	Error! Bookmark not defined.
TINJAUAN PUSTAKA	Error! Bookmark not defined.
2.1 Definisi Kriptografi.....	Error! Bookmark not defined.
2.2 Tujuan Kriptografi	Error! Bookmark not defined.
2.3 Jenis Sistem Kriptografi.....	Error! Bookmark not defined.
2.3.1 Kriptografi Kunci Rahasia (<i>Secret Key Cryptography</i>).....	Error! Bookmark not defined.
2.3.2 Kriptografi Kunci Publik (<i>Public Key Cryptography</i>).....	Error! Bookmark not defined.
2.4 Landasan Matematis Kriptografi.....	Error! Bookmark not defined.
2.4.1 Aritmatika Modular.....	Error! Bookmark not defined.
2.4.2 Inverse Perkalian.....	Error! Bookmark not defined.

2.4.3 Inverse Penjumlahan	Error! Bookmark not defined.
2.4.4 Operasi XOR.....	Error! Bookmark not defined.
2.4.5 Permutasi (Permutation).....	Error! Bookmark not defined.
2.4.6 Pergeseran Bit (Shift).....	Error! Bookmark not defined.
2.4.7 Rotasi Bit (Rotate)	Error! Bookmark not defined.
2.4.8 Perkalian Modulo	Error! Bookmark not defined.
2.5 Metoda IDEA	Error! Bookmark not defined.
2.5.1 Algoritma	Error! Bookmark not defined.
2.6 Perangkat Lunak Pembelajaran.....	Error! Bookmark not defined.
BAB 3.....	Error! Bookmark not defined.
METODE PENELITIAN	Error! Bookmark not defined.
3.1 Metodologi Penelitian	Error! Bookmark not defined.
3.2 Rancangan Perangkat Lunak Kriptografi IDEA	Error! Bookmark not defined.
defined.	
3.2.1 Proses Pembentukan Kunci.....	Error! Bookmark not defined.
3.2.2 Proses Enkripsi.....	Error! Bookmark not defined.
3.2.3 Proses Dekripsi	Error! Bookmark not defined.
3.3 Perancangan	Error! Bookmark not defined.
3.3.1 Form Main.....	Error! Bookmark not defined.
3.3.2 Form Input Proses Pembentukan Kunci.....	Error! Bookmark not defined.
defined.	
3.3.3 Form Input Proses Enkripsi.....	Error! Bookmark not defined.
3.3.4 Form Input Proses Dekripsi	Error! Bookmark not defined.
3.3.5 Form Proses Pembentukan Kunci	Error! Bookmark not defined.
3.3.6 Form Proses Enkripsi / Dekripsi	Error! Bookmark not defined.
3.3.7 Form Teori	Error! Bookmark not defined.
3.3.8 Form Proses Inverse Penjumlahan	Error! Bookmark not defined.
3.3.9 Form Proses Inverse Perkalian.....	Error! Bookmark not defined.
3.3.9 Form About	Error! Bookmark not defined.
BAB IV	Error! Bookmark not defined.
ALGORITMA DAN IMPLEMENTASI	Error! Bookmark not defined.

4.1	Algoritma	Error! Bookmark not defined.
4.1.1	Algoritma Pembentukan Kunci Enkripsi dan Dekripsi.....	Error! Bookmark not defined.
4.1.2	Algoritma Proses Enkripsi	Error! Bookmark not defined.
4.1.3	Algoritma Proses Dekripsi	Error! Bookmark not defined.
4.1.4	Algoritma Fungsi Pendukung dalam Proses Pembentukan Kunci, Enkripsi dan Dekripsi.....	Error! Bookmark not defined.
4.2	Implementasi Sistem	Error! Bookmark not defined.
4.2.1	Spesifikasi Perangkat Keras dan Perangkat Lunak ...	Error! Bookmark not defined.
4.2.2	Cara Menggunakan Perangkat Lunak ..	Error! Bookmark not defined.
4.2.3	Pengujian Program	Error! Bookmark not defined.
4.2.4	Hasil Pengujian	Error! Bookmark not defined.
	KESIMPULAN DAN SARAN.....	Error! Bookmark not defined.
5.1	KESIMPULAN	Error! Bookmark not defined.
5.2	SARAN	Error! Bookmark not defined.
	DAFTAR PUSTAKA	Error! Bookmark not defined.
	LAMPIRAN.....	Error! Bookmark not defined.
	BIODATA PENULIS	Error! Bookmark not defined.

DAFTAR TABEL

	Halaman
Tabel 2.1 Aturan Operasi XOR24.....	14
Tabel 2.2 Permutasi 16 bit	16
Tabel 2.3 Permutasi 16 bit awal.....	16
Tabel 2.4 Permutasi 16 bit akhir	16
Tabel 2.5 Subkey enkripsi dan dekripsi algoritma IDEA	24
Tabel 4.1 Hasil pengujian Proses Enkripsi diketik secara manual	60
Tabel 4.2 Hasil pengujian Proses Enkripsi secara open file	60
Tabel 4.1 Hasil pengujian Proses Dekripsi diketik secara manual	61
Tabel 4.2 Hasil pengujian Proses Dekripsi secara open file	61

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Ilustrasi kriptografi kunci rahasia.....	10
Gambar 2.2 Ilustrasi Kriptografi Kunci Publik.....	12
Gambar 2.3 Proses Pembentukan Kunci untuk IDEA	22
Gambar 2.4 Proses Enkripsi Algoritma IDEA.....	24
Gambar 3.1 Diagram Proses metode IDEA	28
Gambar 3.2 Diagram Proses Enkripsi IDEA	30
Gambar 3.3 Diagram Proses Dekripsi IDEA	31
Gambar 3.4 Rancangan Form Main	32
Gambar 3.5 Rancangan menu dari perangkat lunak	33
Gambar 3.6 Rancangan Form Input Proses Pembentukan Kunci	33
Gambar 3.7 Rancangan Form Input Proses Enkripsi	34
Gambar 3.8 Rancangan Form Input Proses Dekripsi.....	34
Gambar 3.9 Rancangan Form Proses Pembentukan Kunci	35
Gambar 3.10 Rancangan Form Proses Enkripsi / Dekripsi.....	36
Gambar 3.11 Rancangan Form Teori.....	37
Gambar 3.12 Rancangan Form Proses Inverse Penjumlahan	37
Gambar 3.13 Rancangan Form Proses Inverse Perkalian	37
Gambar 3.14 Rancangan Form Proses Rotasi Kiri	38
Gambar 3.15 Rancangan Form About	38
Gambar 4.1 Langkah-1 untuk proses pembentukan kunci.....	47
Gambar 4.2 Langkah-2 untuk proses pembentukan kunci.....	47
Gambar 4.3 Langkah-3 untuk proses pembentukan kunci.....	48

Gambar 4.4 Langkah-4 untuk proses pembentukan kunci.....	48
Gambar 4.5 Langkah-5 untuk proses pembentukan kunci.....	49
Gambar 4.6 Langkah-1 untuk proses enkripsi	49
Gambar 4.7 Langkah-2 untuk proses enkripsi	50
Gambar 4.8 Langkah-3 untuk proses enkripsi	50
Gambar 4.9 Langkah-4 untuk proses enkripsi	51
Gambar 4.10 Langkah-5 untuk proses enkripsi	51
Gambar 4.11 Langkah-6 untuk proses enkripsi	52
Gambar 4.12 Langkah-1 untuk proses dekripsi	52
Gambar 4.13 Langkah-2 untuk proses dekripsi	53
Gambar 4.14 Langkah-3 untuk proses dekripsi	53
Gambar 4.15 Langkah-4 untuk proses dekripsi	54
Gambar 4.16 Langkah-5 untuk proses dekripsi	54
Gambar 4.17 Langkah-6 untuk proses dekripsi	55
Gambar 4.18 Proses pembentukan kunci enkripsi dan dekripsi untuk kunci = 'indonesiamerdeka'	55
Gambar 4.19 Proses enkripsi.....	56
Gambar 4.20 Proses enkripsi text putaran transformasi output	56
Gambar 4.21 Proses dekripsi.....	57
Gambar 4.22 Proses dekripsi putaran transformasi output	57
Gambar 4.23 Proses dekripsi.....	58
Gambar 4.24 Proses dekripsi putaran transformasi output	59

