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 اللهِ الرَّحْمٰنِ الرَّحِيْمِ

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 :

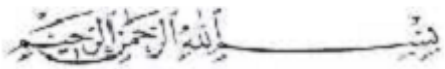
Tim Penguji	*Dosen Pembimbing ,*
1. Zainul Arifin, S.Si	**1. Daryanto, S.Kom**
NPK. 12 03 714	**NPK. 11 03 589**
2. Hardian Oktavanto, S.Si	**2. Lutfi Ali Muharrom, S.Si**
NPK. 12 03 715	**NPK. 10 09 550**

Jember, Januari 2013

Mengetahui

Dekan Fakultas Teknik	Ketua Jurusan Teknik Informatika,
Ir. Kuswardani, MT	**Taufik Timur Warisaji, S.Kom, M.Kom**
NPK. 93 01 379	**NPK. 08 04 846**

KATA PENGANTAR



Puji syukur kita panjatkan kehadirat 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 kerahasian 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

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman