PENGEMBANGAN *PROTOTYPE* SISTEM KRIPTOGRAFI UNTUK ENKRIPSI DAN DEKRIPSI DATA *OFFICE* MENGGUNAKAN METODE BLOWFISH DENGAN BAHASA PEMROGRAMAN JAVA

TESIS

Oleh:
Mohamad Natsir
1111601520

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

JAKARTA
2014

PENGEMBANGAN *PROTOTYPE* SISTEM KRIPTOGRAFI UNTUK ENKRIPSI DAN DEKRIPSI DATA *OFFICE* MENGGUNAKAN METODE BLOWFISH DENGAN BAHASA PEMROGRAMAN JAVA

TESIS

Diajukan sebagai salah satu persyaratan
untuk mendapatkan gelar Magister Ilmu Komputer (MKOM)

Oleh:
Mohamad Natsir
1111601520

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

JAKARTA
2014

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini,

Nama Mahasiswa : MOHAMAD NATSIR
Nomor Induk Mahasiswa : 1111601520
Program Studi : MAGISTER ILMU KOMPUTER
Konsentrasi : REKAYASA KOMPUTASI TERAPAN
Fakultas/Program : PASCASARJANA

menyatakan bahwa **TESIS** yang berjudul :
PENGEMBANGAN PROTOTYPE SISTEM KRIPTOGRAFI UNTUK ENKRIPSI DAN DEKRIPSI DATA OFFICE MENGGUNAKAN METODE BLOWFISH DENGAN BAHASA PEMROGRAMAN JAVA

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain,
2. Saya ijinkan untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan apabila di kemudian pernyataan ini tidak benar.

Jakarta, 03 Maret 2014

(MOHAMAD NATSIR)

PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : Mohamad Natsir
Nomor Induk Mahasiswa : 1111601520
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Strata 2
Juduk Tesis : Pengembangan *Prototype* Sistem Kriptografi untuk Enkripsi dan Dekripsi Data *Office* Menggunakan Metode *Blowfish* dengan Bahasa Pemrograman JAVA

Jakarta, 03 Maret 2014

Tim Penguji: Tanda Tangan:

Ketua,
Ir. Wendi Usino, M.M.,M.Sc., Ph.D .....

Anggota,
Hadi Syahrial, M.M.,M.Kom .....

Pembimbing,
Dr. Ir. Nazori Az, M.T .....

Ketua Program Studi

Dr. Ir. Nazori Az, M.T

ABSTRAK

Perkembangan teknologi komputer yang semakin pesat menjadikan komputer banyak dijumpai mulai dari instansi pemerintahan, perumahan, sekolah-sekolah, warung internet, rumah tangga, bahkan personal atau yang disebut dengan laptop menjadikan komputer sebagai kebutuhan untuk semua kalangan. Pekerjaan-pekerjaan yang dahulunya manualpun kini mulai banyak yang terkomputerisasi mulai dari pekerjaan rumah dari sekolah hingga perusahaan-perusahaan bertaraf internasional dan semua pekerjaan-pekerjaan itu adalah sebuah informasi penting. Layaknya informasi penting, sistem pengamanan adalah bagian krusial dari suatu aplikasi komputer dan salah satu cara untuk melindungi data kita dari pihak-pihak tidak bertanggung jawab adalah dengan melakukan kriptografi seperti yang akan penyusun pakai yaitu menggunakan algoritma *blowfish*. *Blowfish* atau *OpenPGP.Cipher.4* merupakan enkripsi yang termasuk dalam golongan *Symmetric Cryptosystem*, metode enkripsinya mirip dengan Data Enkripsi Standar (DES-like-Cipher). Dibuat untuk digunakan pada komputer yang mempunyai *microprossesor* besar (32-bit keatas dengan cache data yang besar). *Blowfish* dikembangkan untuk memenuhi kriteria desain yang cepat dalam implementasinya dimana pada keadaan optimal dapat mencapai 26 *clock cycle* perbyte, kompak dimana dapat berjalan pada memori kurang dari 5 KB, sederhana dalam algoritmanya sehingga mudah diketahui kesalahannya, dan keamanan yang variable dimana panjang kunci bervariasi (minimum 32 bit, maksimum 448 bit, Multiple 8 bit, *default* 128 bit).

Kata kunci: *kriptografi, key simetrik, algoritma blowfish, enkripsi, dekripsi*

ABSTRACT

The development of computer technology that makes computers much more rapidly found from government agencies, housing, schools, internet cafes , household , personal or even called to make a laptop computer as a requirement for all circles . The works were formerly manual now vastly computerized ranging from homework from school to international companies and all the jobs it is an important information. Like the important information , the security system is a crucial part of a computer application and one way to protect our data from the parties is irresponsible to perform cryptographic would like to use that compiler uses blowfish algorithm. Blowfish or OpenPGP.Cipher.4 is included in the class encryption Symmetric Cryptosystem, the encryption method is similar to the Data Encryption Standard (DES - like - Cipher). Created for use on computers that have a large microprossesor (32 - bit or more with large data caches) . Blowfish was developed to meet the design criteria allows the implementation where the optimal state can reach 26 clock cycles perbyte compact, which can run on less than 5 KB of memory , the simple algorithm so easy to determine guilt, and the security which the variable key length varies (minimum 32 bits, 448 bits maximum, Multiple 8 bits, 128 bits default).

Key words : cryptography,symmetric key, blowfish algorithm, encryption, decryption

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Dengan kerendahan hati penulis panjatkan puji dan syukur yang sedalam-dalamnya kepada Allah SWT Sang Pencipta semesta alam, karena hanya dengan rahmat dan karunia-Nya-lah naskah akhir tesis yang berjudul "PENGEMBANGAN *PROTOTYPE* SISTEM KRIPTOGRAFI UNTUK ENKRIPSI DAN DEKRIPSI DATA *OFFICE* MENGGUNAKAN METODE BLOWFISH DENGAN BAHASA PEMROGRAMAN JAVA" ini dapat diselesaikan. Shalawat serta salam senantiasa tercurahkan kepada Rasulullah yang telah membawa risalah dan Qalam-Nya sehingga penulis dapat memahami dan melaksanakan kewajiban menuntut ilmu. Dalam penyusunan naskah akhir tesis ini, penulis ingin menyampaikan ucapan terimakasih kepada:

1. Allah SWT, atas segala rahmat dan ridho-Nya yang selalu menyertai seluruh aktivitas penulis;
2. Ibuku, Ka Ely, Ka Zainal, Ka Zul, yang senantiasa memberikan kasih sayang, nasihat, dukungan semangat, pengorbanan yang tiada tara serta doa yang tak pernah berhenti mengalir.
3. Istriku Roswita dan kedua anak saya Rizky dan Nazwa, yang selalu memberikan kebahagiaan dan keceriaan.
4. Bapak Dr. Ir. Nazori AZ, MT, selaku pembimbing yang telah memberikan saran dan masukan dalam penyusunan naskah akhir tesis ini;
5. Bapak Dr. Moedjiono, M.Sc, selaku Direktur Program Pascasarjana yang telah memberikan saran dan masukan dalam penyusunan naskah akhir tesis ini;
6. Serta semua pihak yang tidak dapat dituliskan.

Sebagai seorang manusia yang selalu memiliki kekurangan, penulis menyadari bahwa naskah akhir tesis ini masih banyak kekurangan. Oleh karena itu demi menyempurnakan naskah tesis ini, segala bentuk saran dan kritik mohon dapat dikirimkan melalui *e-mail* ke alamat mohnatsir2011@yahoo.co.id.

Wassalamu'alaikum. Wr. Wb.

Jakarta, Januari 2014

M. Natsir

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Gambar Halaman

DAFTAR TABEL

DAFTAR PUSTAKA

[Andriyansah 2005] Andriyansyah. Perangkat Lunak Keamanan Data menggunakan metode Blowfish dan metode RC4, Jakarta,2005.

[Ariyus 2006] Ariyus, Dony. Computer Security, Yogyakarta : 2006.

[Ariyus 2008] Ariyus, Dony. Pengantar Ilmu Kriptografi : Teori, Analisis, dan Implementasi. Andi, Yogyakarta, 2008.

[Ariyus 2009] Ariyus. Keamanan Data dan Komunikasi. Penerbit Graha ilmu, Yogyakarta:2009 [Diakses 08 November 2013].

[Asep 2010] Asep, Herman, Suyanto. Pemograman Java:Konsep Pemrograman Berorientasi Objek.< http://www.bambutechno.com> (Diakses 22 Januari 2014).

[Aziz 2013] Abdul Aziz. Implementasi Setganografi Teknik LSB (Least Significant Bit) dengan Algoritma Kriptografi Blowfish dan Fungsi Hash SHA-1: 2013.

[Burnett 2004] Burnett, Steve and Raine, Stephen. RSA Security's Official Guide to Cryptography. Mc Graw Hill Osborn, California: 2004.

[Christian 2009] Christian ,W.Dawson, Projects in Computing and Information Systems. < www.pearsoned.co.uk> England.First published : 2005 (Diakses 13 Maret 2013).