IMPLEMENTASI ALGORITMA CIPHER TRANSPOSISI DAN SECURE HASH ALGORITHM (SHA) DALAM SISTEM PENGAMANAN DATA

SKRIPSI

FERRY ANTONIUS SIMAMORA
061401087

PROGRAM STUDI S1 ILMU KOMPUTER
DEPARTEMEN ILMU KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS SUMATERA UTARA
MEDAN
2010

IMPLEMENTASI ALGORITMA CIPHER TRANSPOSISI DAN SECURE HASH ALGORITHM (SHA) DALAM SISTEM PENGAMANAN DATA

SKRIPSI

Diajukan untuk melengkapi tugas dan memenuhi syarat mencapai gelar
Sarjana Komputer

FERRY ANTONIUS SIMAMORA
061401087

PROGRAM STUDI S1 ILMU KOMPUTER
DEPARTEMEN ILMU KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS SUMATERA UTARA
MEDAN
2010

PERSETUJUAN

Judul	: IMPLEMENTASI ALGORITMA CIPHER TRANSPOSISI DAN SECURE HASH ALGORITHM (SHA) DALAM SISTEM PENGAMANAN DATA
Kategori	: SKRIPSI
Nama	: FERRY ANTONIUS SIMAMORA
Nomor Induk Mahasiswa	: 061401087
Program Studi	: SARJANA (S1) ILMU KOMPUTER
Departemen	: ILMU KOMPUTER
Fakultas	: MATEMATIKA DAN ILMU PENGETAHUAN ALAM (FMIPA) UNIVERSITAS SUMATERA UTARA

Diluluskan di
Medan, 21 Desember 2010

Komisi Pembimbing :

Pembimbing 2	Pembimbing 1
Syahriol Sitorus, S.Si, MIT	Drs. Partano Siagian M.Sc
NIP. 197 103101997031004	NIP. 130 877 994

Diketahui/Disetujui oleh
Program Studi S1 Ilmu Komputer
Ketua,

Prof. Dr. Muhammad Zarlis
NIP 195707011986011003

PERNYATAAN

IMPLEMENTASI ALGORITMA CIPHER TRANSPOSISI
DAN SECURE HASH ALGORITHM (SHA)
DALAM SISTEM PENGAMANAN DATA

SKRIPSI

Saya mengakui bahwa skripsi ini adalah hasil karya saya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya.

Medan, Desember 2010

FERRY ANTONIUS S.
061401087

PENGHARGAAN

Puji dan syukur penulis panjatkan kepada Tuhan Yesus Kristus, dengan limpahan karunia-Nya, sehingga saya dapat menyelesaikan penyusunan tugas akhir ini.

Ucapan terima kasih saya sampaikan kepada Bapak Drs. Partano Siagian M.Sc sebagai Dosen Pembimbing I dan Bapak Syahriol Sitorus, S.Si, MIT sebagai Dosen Pembimbing II pada penyelesain tugas akhir ini yang telah memberikan panduan dan penuh kepercayaan kepada saya untuk menyempurnakan kajian ini. Panduan ringkas, padat dan profesional telah diberikan kepada saya agar dapat menyelesaikan tugas ini. Selanjutnya kepada para Dosen Penguji Bapak Ir. T Ahri Bahriun, M.Sc dan Bapak Ir. Arman Sani, MT atas saran dan kritikan yang sangat berguna bagi saya. Ucapan terima kasih juga ditujukan kepada Ketua Program Studi S1 Ilmu Komputer Bapak Prof. Dr. Muhammad Zarlis, Dekan dan pembantu Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Unversitas Sumatera Utara, semua dosen Program Studi S1 Ilmu Komputer FMIPA USU, dan pegawai di FMIPA USU, angkatan 2004 dan 2005 yaitu Bang Raja Salomo dan Bang Andre Pratama yang menjadi teman diskusi penulis selama menyusun tugas akhir ini, rekan-rekan kuliah angkatan 2006 yaitu Friendly, Kadar, Pangeran, Evin, Rain, dan Handy. Teristimewa Kepada Ayah Daripen Simamora dan Ibu Rukiah Situmorang, abang saya Dantes Simamora yang telah memberikan doa, dorongan dan perhatian kepada saya.

Akhirnya penulis berharap tugas akhir ini bermanfaat kepada penulis maupun para pembaca serta semua pihak yang berhubungan dengan tugas akhir ini. Penulis menyadari bahwa tugas akhir ini jauh dari sempurna. Oleh karena itu saya menerima saran dan kritik demi kesempurnaan tugas akhir ini. Akhir kata penulis mengucapkan Terima Kasih.

ABSTRAK

Keamanan data merupakan salah satu aspek dalam teknologi informasi. Dengan keamanan data, diharapkan informasi dapat terjaga keasliannya. Pada tugas akhir ini, dibentuk suatu sistem pengamanan data dengan menggabungkan dua algoritma kriptografi yaitu algoritma Cipher Transposisi dan *Secure Hash Algortihm* (SHA). Algoritma Cipher Transposisi merupakan algoritma kriptografi klasik yang sederhana, sehingga Algoritma Cipher Transposisi tidak pernah digunakan lagi. Karena kesederhanaan dari Algoritma Cipher Transposisi, timbul ide untuk menggabungkannya dengan SHA yang merupakan algoritma kriptografi modern yang kompleks. Sistem pengamanan data ini dibangun menggunakan bahasa pemograman Borland Delphi 7.0. Penggabungan kedua algoritma ini diharapkan dapat menjamin keamanan data, sehingga tidak dapat dilihat atau diubah orang yang tidak berhak. Implementasi dari penggabungan kedua algoritma ini dapat mengenkripsi *file* biner dan mendekripsi kembali *file* tersebut.

IMPLEMENTATION OF TRANSPOSITION CIPHER ALGORITHM AND SECURE HASH ALGORITHM (SHA) IN SYSTEM SECURITY OF DATA

ABSTRACT

Data security is one of the important aspect in the information technology. With data security, is expected information can be protected authenticity. In this writing, the system security of data is formed by Transposition Cipher algorithm and Secure Hash Algorithm (SHA). The Transposition Cipher algorithm is the classical cryptography that simple, so that Transposition Cipher algorithm has never been used anymore. Because the simplicity of Transposition Cipher algorithm, the idea to combine it with SHA that representing of complex modern cryptography. This system security of data is built by using Borland Delphi 7.0. The combination of that algorithms are expected to make sure of data security, so that the data cannot be viewed or altered by unauthorized user. The implementation form combination of that algorithms can encrypt of biner file and decrypt it back.

DAFTAR ISI

	Halaman
PERSETUJUAN	ii
PERNYATAAN	iii
PENGHARGAAN	iv
ABSTRAK	v
ABSTRACT	vi
DAFTAR ISI	vii
DAFTAR TABEL	ix
DAFTAR GAMBAR	x
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Metode Penelitian	3
1.7 Sistematika Penulisan	4
BAB 2 LANDASAN TEORI	6
2.1 Pengertian Kriptografi	6
2.2 Proses Kriptografi	7
2.3 Algoritma Cipher Transposisi	7
2.3.1 Columnar Transposition	8
2.4 Secure Hash Algorithm (SHA)	9
2.5 Metode Serangan Terhadap Kriptografi	15
2.6 Keamanan Algoritma Kriptografi	16
2.7 Serangan Terhadap Sistem Pengamanan Data	16
BAB 3 ANALISIS DAN PERANCANGAN	19
3.1 Analisis Masalah	19
3.2 Penyelesaian Masalah	20
3.2.1 Proses Enkripsi Columnar Transposition	20
3.2.2 Proses Dekripsi Columnar Transposition	21
3.2.3 Proses Pembentukan Nilai Hash dengan SHA dan otentikasi	22
3.2.4 Arsitektur Sistem Keamanan Data Columnar Transpositon dan SHA	25

3.3 Analisis Kebutuhan Perangkat Lunak 26
3.3.1 Diagram Use Case 27
3.3.1.1 Enkripsi 27
3.3.1.2 Dekripsi 29
3.4 Perancangan 30
3.4.1 Perancangan Struktur Program 31
3.4.2 Perancangan Antar Muka Pemakai 31
3.4.2.1 Rancangan Form Utama 32
3.4.2.2 Rancangan Form Enkripsi 33
3.4.2.3 Rancangan Form Dekripsi 33
3.4.2.4 Rancangan Form Help 34
3.4.3 Perancangan Prosedural 35
3.4.3.1 Algoritma dan Flowchart Proses Enkripsi 35
3.4.3.2 Algoritma dan Flowchart Proses Dekripsi 36
3.4.3.3 Algoritma dan Flowchart Prosesdur SHA-1 38

BAB 4 IMPLEMENTASI DAN PENGUJIAN 42
4.1 Implementasi 42
4.2 Tampilan Menu Utama 42
4.2.1 Tampilan Submenu Enkripsi 43
4.2.2 Tampilan Submenu Dekripsi 45
4.2.3 Tampilan Submenu Help 49
4.3 Pengujian Perangkat Lunak 49
4.3.1 Pengujian Integrasi Perangkat Lunak 50
4.3.1.1 Menu Utama 51
4.3.1.2 Submenu Enkripsi 52
4.3.1.3 Submenu Dekripsi 52
4.3.1.4 Submenu Help 53

BAB 5 KESIMPULAN DAN SARAN 54
5.1 Kesimpulan 54
5.2 Saran 54

DAFTAR PUSTAKA 56

DAFTAR TABEL

	Halaman
Tabel 2.1 Enkripsi *Columnar Transposition*	8
Tabel 2.2 Fungsi logika f_t pada setiap putaran	14
Tabel 3.1 Proses Enkripsi *Columnar Tranposition*	21
Tabel 3.2 Proses Dekripsi *Columnar Transposition*	22
Tabel 4.1 Evaluasi Menu Utama	51
Tabel 4.2 Evaluasi Submenu Enkripsi	52
Tabel 4.3 Evaluasi Submenu Dekripsi	52
Tabel 4.4 Evaluasi Submenu Help	53

DAFTAR GAMBAR

Halaman

Gambar 2.1 Proses Kriptografi 7
Gambar 2.2 Pembuatan *message digest* dengan SHA 10
Gambar 2.3 Pengolahan blok 512 bit 12
Gambar 2.4 Operasi dasar SHA dalam satu putaran (fungsi *f*) 13
Gambar 3.1 Arsitektur Enkripsi Sistem Keamanan Data 25
Gambar 3.2 Arsitektur Dekripsi Sistem Keamanan Data 26
Gambar 3.3 *Use Case* Global 27
Gambar 3.4 *Use Case* Enkripsi Plainteks dan Pembentukan Nilai *hash* 1 28
Gambar 3.5 Diagram Alir Enkripsi 28
Gambar 3.6 *Use Case* Pembuktian Keaslian Cipherteks dan Dekripsi Cipherteks 29
Gambar 3.7 Diagram Alir Dekripsi 30
Gambar 3.8 Struktur Program Kriptografi *Columnar Transposition* dan SHA 31
Gambar 3.9 Rancangan Form Utama 32
Gambar 3.10 Rancangan Form Enkripsi 33
Gambar 3.11 Rancangan Form Dekripsi 34
Gambar 3.12 Rancangan Form Help 34
Gambar 3.13 Flowchart Prosedur Enkripsi 36
Gambar 3.14 Flowchart Prosedur Dekripsi 37
Gambar 3.15 Flowchart Prosedur SHA-1 40
Gambar 3.16 Flowchart Proses fungsi f dan k 41
Gambar 4.1 Tampilan Menu Utama 42
Gambar 4.2 Tampilan Submenu Enkripsi 43
Gambar 4.3 Membuka Gambar1.JPEG 44
Gambar 4.4 Tampilan Submenu Enkripsi setelah membuka *file* 44
Gambar 4.5 Pemberitahuan nama *file* kunci 44
Gambar 4.6 Pemberitahuan proses Enkripsi selesai 45
Gambar 4.7 Tampilan Submenu Dekripsi 45
Gambar 4.8 Membuka Gambar1.JPEG 46
Gambar 4.9 Tampilan Submenu Dekripsi setelah membuka *file* terenkripsi 46
Gambar 4.10 Membuka *file* kunci 47
Gambar 4.11 Pemberitahuan bahwa ekstensi kunci valid 47
Gambar 4.12 Tampilan Submenu Dekripsi setelah membuka kedua *file* 48
Gambar 4.13 Pemberitahuan proses dekripsi berhasil 48
Gambar 4.14 Pemberitahuan kunci tidak cocok 48
Gambar 4.15 Tampilan Submenu Help 49