



**IMPLEMENTASI KRIPTOGRAFI ALGORITMA TRIPLE DES UNTUK
MENGECK KEABSAHAN SUATU IJAZAH**

SKRIPSI

MICHAEL SIRAIT

0910.511.105

**UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI TEKNIK INFORMATIKA
2016**



**IMPLEMENTASI KRIPTOGRAFI ALGORITMA TRIPLE DES UNTUK
MENGECEK KEABSAHAN SUATU IJAZAH**

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Komputer**

MICHAEL SIRAIT

0910.511.105

UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI TEKNIK INFORMATIKA

2016

Pernyataan Orisinalitas

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Michael Sirait

NRP : 0910511105

Tanggal : 22 Februari 2016

Apabila di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 22 Februari 2016

Yang Menyatakan,



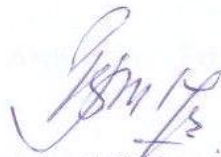
Michael Sirait

Lembar Pengesahan

Skripsi ini diajukan oleh :

Nama : Michael Sirait
NRP : 091051105
Program Studi : Teknik Informatika
Judul Skripsi : Implementasi Kriptografi Algoritma Triple DES
Untuk Mengecek Keabsahan Suatu Ijazah

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jakarta.



Titin Pramiyati, S.Kom, M.Si

Ketua Penguji



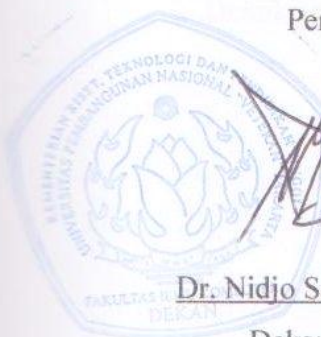
Anita Muliawati, S.Kom, MTI

Penguji I



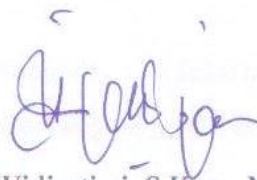
Henki Bayu Seta, S.Kom, MTI

Penguji II (Pembimbing)



Dr. Nidjo Sandjojo, M.Sc

Dekan Fakultas



Yuni Widiastiwi, S.Kom, M.Si

Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Ujian : 12 Februari 2016

Pernyataan Persetujuan Publikasi Skripsi Untuk Kepentingan Akademis

Sebagai civitas akademik Universitas Pembangunan Nasional “Veteran” Jakarta, saya yang bertanda tangan di bawah ini :

Nama : Michael Sirait
NRP : 0910511105
Fakultas : Ilmu Komputer
Program Studi : Teknik Informatika

Demi pengembangan ilmu pengetahuan, telah menyetujui untuk memberikan kepada Universitas Pembangunan Nasional “Veteran” Jakarta yaitu Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul :

Implementasi Kriptografi Algoritma Triple DES Untuk Mengecek Keabsahan Suatu Ijazah

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional “Veteran” Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 22 Februari 2016

Yang Menyatakan,



(Michael Sirait)

IMPLEMENTASI KRIPTOGRAFI ALGORITMA TRIPLE DES UNTUK MENGECEK KEABSAHAN SUATU IJAZAH

Michael Sirait

Abstrak

Tujuan dari penelitian ini adalah untuk membuat suatu sistem yang dapat digunakan untuk mengecek keabsahan suatu ijazah. Penelitian ini menggunakan metode enkripsi dan dekripsi dengan algoritma Triple DES untuk mengubah data asli menjadi data acak sehingga tidak diketahui oleh pihak yang tidak berwenang. Dengan penyusunan tugas akhir ini diharapkan dapat mencegah dan mengurangi pemalsuan ijazah yang saat ini marak terjadi. Berdasarkan hasil analisa, kesimpulan yang dapat diambil yaitu dengan adanya sistem ini maka data-data yang ada pada suatu ijazah menjadi acak dan tidak diketahui oleh pihak yang tidak berwenang sehingga tidak bisa dipalsukan. Saran yang dapat diberikan adalah agar sistem ini bisa lebih dikembangkan sehingga dapat lebih membantu dalam mengecek keabsahan ijazah.

Kata Kunci : Kriptografi, Triple DES, Keabsahan Ijazah

TRIPLE DES CRYPTOGRAPHIC ALGORITHM IMPLEMENTATION FOR CHECK THE VALIDITY OF A DIPLOMA

Michael Sirait

Abstract

The purpose of this research is to create a system that can be used to check the validity of a diploma. This study uses the encryption and decryption with Triple DES algorithm to transform the original data into random data so it is not known by unauthorized parties. With the preparation of this thesis is expected to prevent and reduce forgery diploma that is currently rife. Based on the analysis, the conclusion can be drawn that the presence of this system, the data available to a diploma be random and not known by an unauthorized person that can not be faked. Advice can be given is that this system could be developed so that it can be more helpful in checking the validity of diplomas.

Keywords : cryptography, Triple DES, the validity of diplomas

Kata Pengantar

Puji dan syukur penulis panjatkan kehadiran Tuhan Yang Maha Esa atas segala karunia-Nya sehingga Karya Ilmiah / Skripsi ini dengan judul “**Implementasi Kriptografi Algoritma Triple DES Untuk Mengecek Keabsahan Suatu Ijazah**” dapat diselesaikan.

Skripsi ini disusun untuk memenuhi salah satu syarat dalam meraih gelar Sarjana Komputer di UPN “Veteran” Jakarta. Selain itu penulis berharap apa yang menjadi karya penulis dapat bermanfaat bagi diri sendiri, keluarga, dan masyarakat pada umumnya.

Pada kesempatan ini, penulis ingin menyampaikan penghargaan dan ucapan terima kasih atas bantuan, kerja sama serta bimbingan yang telah diberikan sehingga terselesainya skripsi ini, yaitu kepada:

1. **Tuhan Yang Maha Esa** atas rahmat dan kuasa-Nya serta turut campur tangan-Nya dalam pengerjaan skripsi ini.
2. Kedua Orang Tua, Ayah **Bitner Sirait** dan Ibu **Lustani Samosir**, yang telah mendukung secara do’a, kasih sayang, dan materi selama ini.
3. Kedua saudari, **Escha Natalia Sirait** dan **Fefi Arni Sirait** atas dukungan yang telah diberikan selama ini.
4. Bapak **Dr. Nidjo Sandjojo, M.Sc** selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta.
5. Ibu **Yuni Widiastiwi, S.Kom, M.Si** selaku Ketua Program Studi Teknik Informatika Universitas Pembangunan Nasional “Veteran” Jakarta.
6. Bapak **Henki Bayu Seta, S.Kom., M.TI** selaku dosen pembimbing dalam menyelesaikan skripsi ini.
7. Teman-teman kosan murai yudha, maman, fikri, agung, edward, risky, ali, alek, wanto, ian, babay, uci, sovi, rendy yang selalu menghibur dan member canda tawa.
8. Teman-teman mahasiswa FIK UPN “Veteran” Jakarta khususnya TI-C 2009, yang telah memberikan dukungan hingga penulis bisa menyelesaikan tugas ini.

Tentunya dalam pembuatan skripsi ini masih terdapat banyak kekurangan dan jauh dari kesempurnaan, sehingga penulis mengharapkan kritik dan saran yang membangun dari pembaca.

Akhir kata, penulis mengharapkan agar skripsi ini dapat berguna dan bermanfaat bagi pembaca dan pihak yang membutuhkan.

Jakarta, 3 Januari 2016

Penulis,

DAFTAR ISI

Halaman Judul	
Halaman Pernyataan Orisinalitas	
Halaman Pengesahan	
Halaman Pernyataan Persetujuan Publikasi	
Abstrak	
Abstrack	
Kata Pengantar	i
DAFTAR ISI	iii
DAFTAR GAMBAR	v
DAFTAR TABEL	vi
 BAB I	 PENDAHULUAN
	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	3
1.3 Ruang Lingkup.....	4
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Metode Penelitian	4
1.7 Sistematika Penulisan	5
 BAB II	 TINJAUAN PUSTAKA
	7
2.1 Kriptografi	7
2.2 Algoritma DES.....	19
2.3 Triple DES	25
2.4 Review Penelitian Terdahulu	31
 BAB III	 METODOLOGI PENELITIAN
	33
3.1 Kerangka Berfikir	33
3.2 Tahapan Penelitian.....	33
3.3 Metode Penelitian	35
3.4 Alat Bantu Penelitian	35
3.5 Jadwal Penelitian	36
 BAB IV	 HASIL DAN PEMBAHASAN
	37
4.1 Identifikasi Masalah	37
4.2 DES (Data Encryption Standard)	38
4.3 Triple DES	47
4.4 Perancangan Sistem	48
4.5 Implementasi.....	51
 BAB V	 PENUTUP
	55
5.1 Simpulan	55
5.2 Saran	55

DAFTAR PUSTAKA	56
DAFTAR RIWAYAT HIDUP	

DAFTAR GAMBAR

Gambar 1 Proses Enkripsi dan Dekripsi	11
Gambar 2 Interruption.....	12
Gambar 3 Interception	12
Gambar 4 Modification.....	13
Gambar 5 Fabrication	13
Gambar 6 Skema Enkripsi dan Dekripsi.....	14
Gambar 7 Ilustrasi Enkripsi dan Dekripsi Pesan	15
Gambar 8 Mekanisme Kriptografi Simetrik	16
Gambar 9 Skema Kriptografi Simetrik	16
Gambar 10 Mekanisme Algoritma Asimetri.....	18
Gambar 11 Skema Global Algoritma DES.....	20
Gambar 12 Proses Pembangkitan Kunci-Kunci Internal DES	23
Gambar 13 Proses Enkripsi DES	24
Gambar 14 Skema Triple DES 2 Kunci.....	26
Gambar 15 Skema Triple DES 3 Kunci.....	26
Gambar 16 Algoritma Triple DES.....	27
Gambar 17 Grafik Ukuran File Input Terhadap Kecepatan	30
Gambar 18 Kerangka Berfikir	33
Gambar 19 Desain Input-Output Algoritma DES.....	39
Gambar 20 Skema Enchippering	42
Gambar 21 Proses Dekripsi Setiap Round.....	46
Gambar 22 Diagram Alur / Flowchart	49
Gambar 23 Tampilan Proses Enkripsi (1).....	52
Gambar 24 Tampilan Proses Enkripsi (2).....	52
Gambar 25 Tampilan Proses Dekripsi (1)	53
Gambar 26 Tampilan Proses Dekripsi (2)	53

DAFTAR TABEL

Tabel.1 Serangan Brute Force Pada DES	22
Tabel.2 Cara Pengenkripsian dan Pendekripsian Triple DES	28
Tabel 3 Waktu Proses dan Kecepatan Enkripsi	29
Tabel 4 Waktu Proses dan Kecepatan Dekripsi	30
Tabel 5 Jadwal Penelitian	36
Tabel 6 Initial Permutation	40
Tabel 7 Permutasi Choice One	40
Tabel 8 Rotasi Kiri.....	41
Tabel 9 Permutasi Choice Two.....	41
Tabel 10 Tabel Ekspansi (E).....	42
Tabel 11 Invers Initial Permutation (IP^{-1}).....	45
Tabel 12 Tabel Require Key Pengecekan Pertama.....	50
Tabel 13 Database Ijazah	50
Tabel 14 Database Ijazah Sebelum Ekripsi	51
Tabel 15 Hasil Pengujian	54