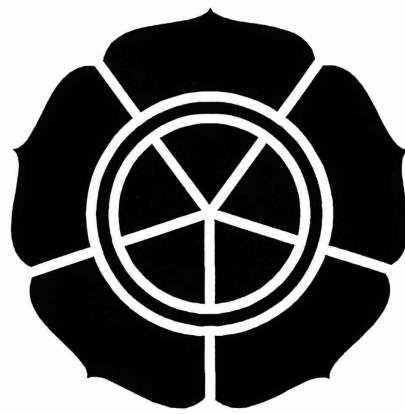


**IMPLEMENTASI PENGENKRIPSAN DATA NILAI SISWA DENGAN
MENGUNAKAN ALGORITMA
DES (*Data Encryption Standard*) BERBASIS WEB**

SKRIPSI



disusun oleh
Pramulyandi
04.11.0476

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2012**

PERSETUJUAN

SKRIPSI

Implementasi Pengenkripsian Data Nilai Siswa Dengan Menggunakan
Algoritma
DES (*Data Encryption Standard*) Berbasis Web

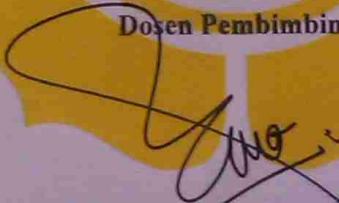
yang dipersiapkan dan disusun oleh

Pramulyandi

04.11.0476

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 14 Juni 2012

Dosen Pembimbing,



Ema Utami, Dr., S.Si, M.Kom
NK. 190302037

PENGESAHAN

SKRIPSI

**Implementasi Pengenkripsian Data Nilai Siswa Dengan Menggunakan
Algoritma
DES (Data Encryption Standard) Berbasis Web**

yang dipersiapkan dan disusun oleh

Pranudyandi

04.11.0476

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

**Sudarmawan, MT
NIK. 190302035**



**M. Rudyanto Arief, MT
NIK. 190302098**



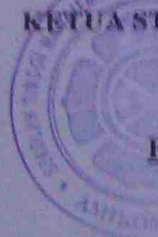
**Bambang Sudaryatno, Drs, MM
NIK. 190302029**



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer

Tanggal 28 Mei 2017

KETUA STMIK AMIKOM YOGYAKARTA



**Prof. Dr. M. Suyanto, M.M.
NIK. 190302001**

iii

PERNYATAAN

Saya yang bertanda tangan di bawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta 1 Juni 2012

Pramulyandi

Kata Pengantar

Puji Syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi.

Adapun penyusunan skripsi ini dimaksudkan untuk memenuhi persyaratan kelulusan Program Sarjana Srata-1 di Sekolah Tinggi Manajemen Informatika dan Komputer STMIK “AMIKOM” Yogyakarta.

Terselesainya skripsi ini tidak terlepas dari dukungan berbagai pihak yang telah memberikan dukungan moral maupun spiritual dan juga bimbingan ilmu pengetahuan, oleh karena itu pada kesempatan yang sangat berharga ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Dr. Ema Utami, Si, M.Kom. selaku dosen pembimbing yang telah meluangkan waktunya untuk membimbing dan mengarahkan penulis dalam menyusun skripsi ini.
2. Dewan Penguji Skripsi.
3. Kepada teman-teman dan semua pihak yang telah memberikan dukungan dan membantu saya hingga selesainya penyusunan laporan skripsi ini dengan lancar.

Penulis menyadari sebagaimana kodratnya sebagai manusia yang tidak luput dari kesalahan dan kekurangan dalam penyusunan skripsi ini dan masih jauh dari kesempurnaan. Oleh karena itu penulis mengharapkan kritik dan saran yang bersifat membangun dari pembaca yang budiman.

Demikian Laporan skripsi ini disusun, semoga dapat bermanfaat bagi pembaca dan lembaga STMIK AMIKOM Yogyakarta. Akhir kata penulis mengucapkan banyak terima kasih dan mengharapkan kerjasamanya.

Yogyakarta, 1 Juni 2012

Penulis

Daftar Isi

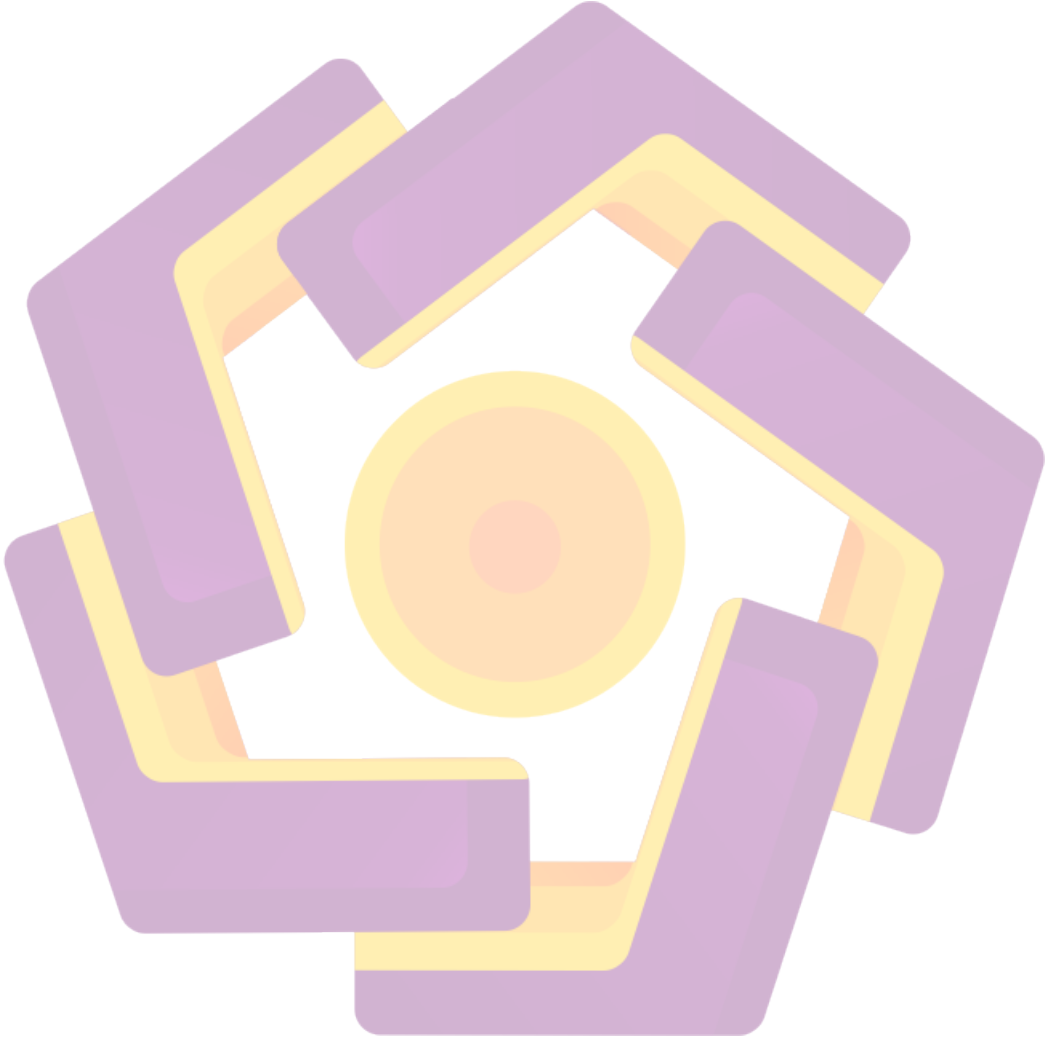
COVER	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
PERNYATAAN	iv
KATA PENGANTAR	v
DAFTAR ISI	vii
DAFTAR TABEL	x
DAFTAR GAMBAR	xii
INTISARI	xiii
ABSTRACT	xiv
BAB I PENDAHULUAN	
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	5
1.6 Metode Penelitian.....	5
1.7 Jadwal Penelitian.....	7
1.8 Sistematika Penelitian.....	8
BAB II LANDASAN TEORI	
2.1 Pengertian Keamanan Komputer.....	10
2.2 Keamanan Data.....	10
2.3 Kriptografi.....	12
2.3.1 Algoritma Kriptografi.....	12
2.3.2 Macam Algoritma Kriptografi.....	13
2.3.3 Kriptografi Klasik.....	18
2.3.4 kriptografi Modern.....	19
2.4 Database.....	19

2.5	Sql 2005 Express Edition	19
2.6	Microsoft Web Development 2005 Express Edition	22
2.7	Kerangka Berfikir	24
BAB III ANALISA DAN PERANCANGAN SISTEM		
3.1	Analisa Sistem	26
3.1.1	Analisa Kebutuhan Sistem	26
3.1.2	Arsitektur Sistem	26
3.2	Perancangan Proses	28
3.2	Perancangan Database	29
3.2.1	Pembuatan Struktur Tabel-tabel yang Digunakan	29
3.2.2	Hubungan Antar Tabel	35
3.3	Struktur Program	37
3.4	Desain Antar Muka	38
BAB IV IMPLEMENTASI PROGRAM		
4.1	Implementasi Basis Data	42
4.1.1	Struktur Tabel Tahun	42
4.1.2	Struktur Tabel Kelas	42
4.1.3	Struktur Tabel Matapelajaran	43
4.1.4	Struktur Tabel Guru	43
4.1.5	Struktur Tabel Nilai	43
4.1.6	Struktur Tabel Detil Nilai	44
4.2	Antarmuka Program	44
4.2.1	Tampilan Sebelum Login	46
4.2.2	Tampilan Utama Setelah Login	46
4.2.3	Tampilan Tahun Ajaran	47
4.2.4	Tampilan Data Kelas	48
4.2.5	Tampilan Matapelajaran	49
4.2.6	Tampilan Guru	50
4.2.7	Tampilan Siswa	51
4.2.8	Tampilan Data Admin	52
4.2.9	Tampilan Daftar Siswa	53
4.2.10	Tampilan Input Kelas	54
4.2.11	Input Nilai	56
4.2.12	Lihat Nilai	57

BAB V PENUTUP

5.1 Kesimpulan 59
5.2 Saran 60

DAFTAR PUSTAKA



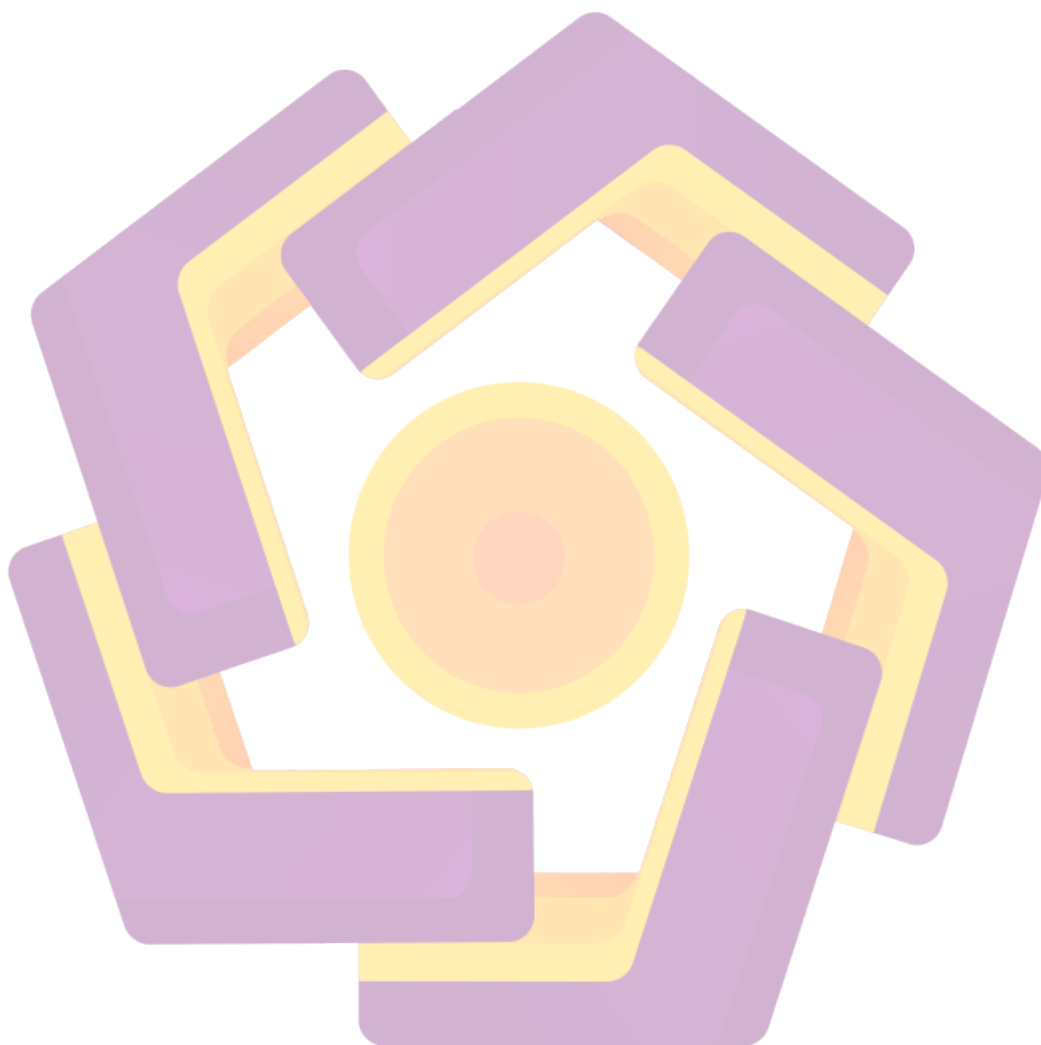
Daftar Tabel

Tabel 1.1	Tabel Jadwal Kegiatan.....	7
Tabel 3.1	Tabel Pengguna	30
Tabel 3.2	Tabel Guru	30
Tabel 3.3	Tabel Siswa	31
Tabel 3.4	Tabel Tahun Ajaran	31
Tabel 3.5	Tabel Extra Kulikuler.....	32
Tabel 3.6	Tabel Kelas	32
Tabel 3.7	Tabel Matapelajaran.....	32
Tabel 3.8	Tabel Nilai Raport	33
Tabel 3.9	Tabel Detil Raport	33
Tabel 3.10	Tabel Extrakulikuler Siswa.....	34

Daftar Gambar

Gambar 2.1.	Konsep Keamanan Data.....	11
Gambar 2.2.	Jaringan Feistel untuk satu putaran DES.....	15
Gambar 2.3.	Algoritma Enkripsi dengan DES.....	16
Gambar 2.4.	Kerangka Berfikir.....	24
Gambar 3.1.	Arsitektur Sistem Pengenkripsian Data.....	26
Gambar 3.2.	Hubungan Antar Tabel.....	35
Gambar 3.3.	Alur Program.....	37
Gambar 3.4.	Tampilan Page Master.....	38
Gambar 3.5.	Tampilan Login.....	39
Gambar 3.6.	Tampilan Untuk Input Tahun.....	39
Gambar 3.7.	Tampilan Anggota.....	39
Gambar 3.8.	Tampilan Kelas.....	40
Gambar 3.9.	Tampilan Extrakurikuler.....	40
Gambar 3.10.	Tampilan Matapelajaran.....	40
Gambar 3.11.	Tampilan Siswa.....	41
Gambar 4.1.	Struktur Tabel Tahun Ajaran.....	42
Gambar 4.2.	Struktur Tabel Kelas.....	42
Gambar 4.3.	Struktur Tabel Matapelajaran.....	43
Gambar 4.4.	Struktur Tabel Guru.....	43
Gambar 4.5.	Struktur Tabel Nilai.....	43
Gambar 4.6.	Struktur Tabel Detil Nilai.....	44
Gambar 4.7.	Tampilan Menu Sebelum Login.....	44
Gambar 4.8.	Tampilan Menu.....	46
Gambar 4.9.	Tampilan Tahun Ajaran.....	47
Gambar 4.10.	Tampilan Data Kelas.....	48
Gambar 4.11.	Tampilan Mata Pelajaran.....	49
Gambar 4.12.	Tampilan Guru.....	50
Gambar 4.13.	Tampilan Data Siswa.....	51
Gambar 4.14.	Data Admin.....	52
Gambar 4.15.	Tampilan Data siswa.....	53

Gambar 4.16	Tampilan Input Kelas	54
Gambar 4.17	Tampilan Input Nilai	56
Gambar 4.18	Tampilan Input Nilai	57



Intisari

Masalah keamanan adalah salah satu aspek yang paling penting dari sebuah sistem informasi. Salah satu cara untuk membatasi akses data bagi mereka yang tidak berhak adalah dengan enkripsi. Proses enkripsi adalah proses untuk menyandikan data dalam bentuk yang hanya dapat dibaca oleh sistem yang memiliki kunci untuk membaca data.

Metode enkripsi tidak satu-satunya solusi terbaik untuk keamanan jaringan seperti yang kadang-kadang enkripsi juga dapat dipecahkan. Pada sistem unix, biasanya digunakan enkripsi standar DES atau ruang bawah tanah. Data Encryption Standard (DES) adalah sebuah teknik enkripsi modern yang secara resmi digunakan oleh Amerika Serikat pada 1977. Sementara crypt berdasarkan teknik enkripsi me sin Enigma Jerman (Perang Dunia II). DES lebih baik dari keduanya.

Studi ini memberikan bagaimana menerapkan enkripsi dan dekripsi data di dalam sistem lembaga pendidikan menggunakan DES (Data Encryption Standard) algoritma dengan berbasis web. Hal ini memberikan keamanan lebih untuk data di dalam sistem database. Dengan ini penulis studi telah berhasil merancang dan membangun sistem yang dapat mengamankan nilai data dari sebuah lembaga pendidikan siswa yang lebih baik.

Kata-kunci : Sistem Informasi, *Encryption, Description*

Abstract

Security problem is one of the most important aspect of an information system. One way of limiting data access to those who are not entitled is with encryption. Encryption process is a process to encode the data in a form that can only be read by a system that has the key to read data.

The encryption method is not the only best solution for network security as it is sometimes encryption can also be solved. On unix systems, commonly used encryption standard or DES crypt. Data Encryption Standard (DES) is a modern encryption techniques are officially used by the United States in 1977. While crypt based on the German Enigma encryption techniques (World War II). DES is better than both.

This study provides how to implement encryption and decryption the data within the system of educational institutions using DES (Data Encryption Standard) algorithm with web-based. This gives more security to the data inside the database system. With this study author has succeeded designing and building a system that can secure the data value from an educational institution the student better.

Key-word : Information system, Encryption, Description