

**ENKRIPSI DATA DIGITAL MENGGUNAKAN METODE DES
(DATA ENCRYPTION STANDARD)**

SYARIF TAUCHID

J2A 096 061

Skripsi

**Sebagai salah satu syarat untuk memperoleh gelar
Sarjana Sains pada Jurusan Matematika FMIPA
Universitas Diponegoro**

**JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS DIPONEGORO
SEMARANG**

2003

LEMBAR PENGESAHAN I

Judul : “Enkripsi Data Digital Menggunakan Metode DES
(Data Encryption Standard)”

Nama : Syarif Tauchid

Nim : J2A 096 061

Tanggal lulus ujian : 29 Januari 2003

Semarang, Februari 2003

Ketua Jurusan Matematika



(Signature)
(Drs. Bawo Surarso, M.Sc, PhD)
NIP. 131 764 886

Panitia Ujian Sarjana Jurusan

Matematika

(Drs. Kushartantya, MI Komp)
NIP. 130 805 062

LEMBAR PENGESAHAN II

ENKRIPSI DATA DIGITAL MENGGUNAKAN METODE DES (DATA ENCRYPTION STANDARD)

Nama : Syarif Tauchid

Nim : J2A 096 061

Telah diujikan pada ujian sarjana tanggal 29 Januari 2003 dan telah dinyatakan **LULUS**

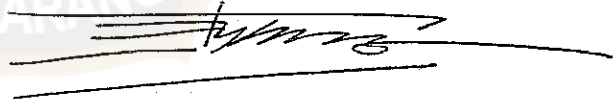
Semarang, Februari 2003

Pembimbing Utama

Pembimbing Anggota



(Drs. Kushartantya, MI Komp)
NIP. 130 805 062



(Drs. Putut Sri Wasito)
NIP. 130 877 410

HALAMAN PERSEMBAHAN

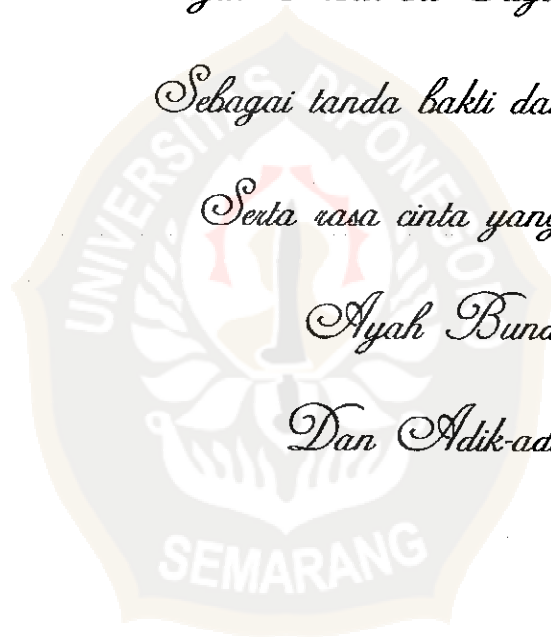
Tugas Akhir ini Saya persembahkan

Sebagai tanda bakti dan terima kasihku

Serta rasa cinta yang dalam kepada

Ayah Bunda Ku Tercinta

Dan Adik-adikku Tersayang



KATA PENGANTAR

Alhamdulillah, segala puji syukur penulis panjatkan kehadirat Allah Ta'ala yang telah melimpahkan rahmat dan petunjuk-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir ini.

Penulisan Tugas Akhir dengan judul “ Enkripsi Data Digital Menggunakan Metode DES (Data Encryption Standard)” ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu (S1) pada Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Diponegoro Semarang.

Penulis menyadari bahwa selesainya Tugas Akhir ini adalah tidak lepas dari bantuan beberapa pihak, oleh karena itu pada kesempatan ini penulis ingin menyampaikan terima kasih kepada:

1. Bapak Drs. Bayu Surarso, MSc. PhD. Selaku Ketua Jurusan Matematika.
2. Bapak Drs. Kushartantya, MI Komp. Selaku Dosen Pembimbing I yang telah memberikan pengarahan hingga selesainya Tugas Akhir ini.
3. Bapak Drs. Putut Sri Wasito selaku Dosen Pembimbing II yang telah banyak membantu dan meluangkan waktunya hingga penulis dapat menyusun Tugas Akhir ini.
4. Ibu Dra. Suparti, MSi. Selaku Dosen Wali yang dengan sabar dan nasehatnya telah mengantarkan penulis hingga selesai kuliah.
5. Seluruh staf pengajar Jurusan Matematika FMIPA yang telah memberikan arahan dan ilmunya bagi penulis

6. Ayah dan Ibuku tercinta, serta Adik-adikku tersayang yang telah memberikan dorongan baik secara materil maupun sprirituil kepada penulis.
7. Untuk teman-temanku Adi, Ari, Fath, Ismail, Igun, Izza (Panda.Com), Umi, Ari N, Sulardi, Nanang dan konco'96 lainnya, serta ikhwan Nurussunnah dan lainnya yang belum tersebut disini.

Mengingat terbatasnya kemampuan dan pengetahuan yang dimiliki penulis, maka tentunya masih banyak kekurangan-kekurangan dalam penulisan Tugas Akhir ini. Penulis mengharapkan kritikan dan saran yang bersifat membangun demi kesempurnaan Tugas Akhir ini. Semoga Tugas Akhir ini dapat bermanfaat bagi penulis dan siapa saja yang dapat mengambil manfaat darinya.

Semarang, Februari 2003

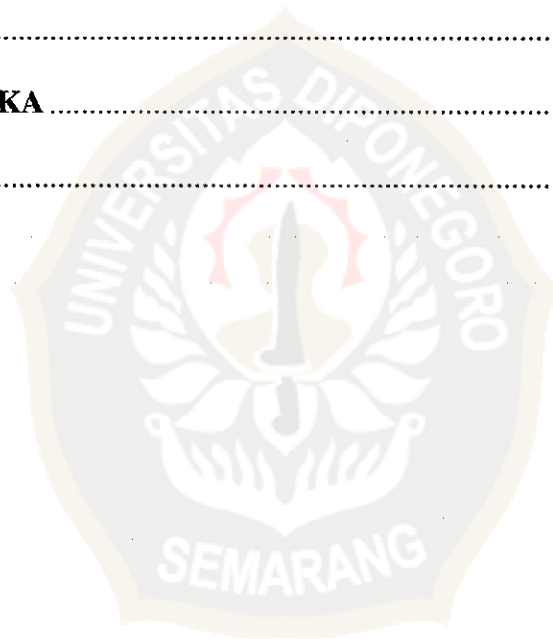
Penulis

DAFTAR ISI

HALAMAN JUDUL	i
LEMBAR PENGESAHAN	ii
HALAMAN PERSEMBAHAN	iv
KATA PENGANTAR	v
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiii
DAFTAR SIMBOL	xiv
BAB I PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Perumusan Dan Pembatasan Masalah.....	2
1.3. Tujuan.....	3
1.4. Sistematika penulisan.....	3
BAB II MATERI PENUNJANG	5
2.1. Konsep Dasar Matematika.....	5
2.1.1. Fungsi.....	5
2.1.1.1. Permutasi.....	11
2.1.1.2. Involusi.....	12
2.1.2. Teori Bilangan.....	13
2.1.2.1. Integer.....	13

2.1.2.2. Integer Modulo n.....	15
2.1.3. Bilangan Biner	17
2.1.4. Bilangan Heksadesimal.....	18
2.1.5. Konversi antar Basis	20
2.1.6. Bit (Binary digit).....	21
2.1.6.1. Bit Paritas	21
2.1.6.1.1. Bit Paritas Genap dan Ganjil.....	22
2.1.7. Ukuran Bilangan	25
2.1.3. Operasi Logika.....	26
2.2. File.....	28
2.3. Pengantar Kriptografi.....	28
BAB III PENERAPAN KRIPTOGRAFI UNTUK KEAMANAN DATA	32
3.1. Kriptografi.....	32
3.2. Metode Enkripsi Des.....	34
3.3. Konsep Dan Terminologi Dasar.....	36
3.3.1. Domain Dan Kodomain Enkripsi.....	36
3.3.2. Transformasi Enkripsi Dan Dekripsi	37
3.3.3. Partisipan Dalam Komunikasi	40
3.3.4. Keamanan dalam Kriptografi.....	41
3.3.5 Enkripsi Kunci Simetrik.....	42
3.3.5.1. Sandi Substitusi Sederhana	45
3.3.5.2. Sandi Substitusi Polialpabet.....	46
3.3.5.3. Sandi Transposisi	47

3.3.9. Panjang Kunci Simetrik	48
3.4. Penerapan Metode DES untuk Keamanan Data Digital.....	51
3.4.1 Penjadwalan Kunci (<i>Key Schedule</i>).....	57
3.4.2. Proses Penyandian (<i>Enchiperment</i>)	59
3.4.3. Proses Dekripsi (<i>Dechiperment</i>).....	68
3.4.4. Desain Program.....	72
PENUTUP	74
DAFTAR PUSTAKA	75
LAMPIRAN	76



DAFTAR GAMBAR

Gambar 2.1	Sebuah fungsi dari himpunan X terhadap himpunan Y.....	6
Gambar 2.2	Sebuah fungsi satu-satu f	7
Gambar 2.3	Sebuah fungsi onto f	7
Gambar 2.4	Sebuah fungsi bijeksi f	8
Gambar 2.5	Sebuah fungsi bijeksi f dan inversnya $g = f^{-1}$	9
Gambar 2.6	Involusi himpunan S dengan 5 buah elemen	12
Gambar 2.7	Proses Enkripsi dan Dekripsi dengan Kunci.....	30
Gambar 3.1.	Proses input-output DES.....	34
Gambar 3.2	Enkripsi sederhana.....	38
Gambar 3.3	Skema komunikasi dua pihak dengan menggunakan enkripsi ...	39
Gambar 3.4	Dua pihak yang berkomunikasi menggunakan enkripsi dengan saluran informasi yang aman untuk pertukaran kunci.....	44
Gambar 3.5	Alur skema enkripsi DES	55
Gambar 3.6	Satu putaran dari DES	56
Gambar 3.7	Flowchart program enkripsi.....	73
Tampilan 1.	Menu utama program enkripsi dengan metode DES.....	101
Tampilan 2.	Tampilan pada saat button atau menu enkripsi/dekripsi dipilih.	101
Tampilan 3.	Tampilan pada saat menu acknowledge dipilih dari menu help.	102
Tampilan 4.	Tampilan pada saat button atau menu exit dipilih dari menu file	102

DAFTAR TABEL

Tabel 2.1	Konversi desimal, biner dan heksadesimal	19
Tabel 2.2	Bit paritas.....	24
Tabel 2.3.	Ukuran Bilangan.....	26
Tabel 2.4.	Operasi logika AND.....	27
Tabel 2.5.	Operasi logika OR.....	27
Tabel 2.6.	Operasi logika NOT.....	27
Tabel 2.7.	Operasi logika X-OR.....	27
Tabel 3.1.	Permuted Choice 1 (PC-1).....	57
Tabel 3.2.	Shift Schedule for Encipherment.....	58
Tabel 3.3.	Permuted Choice 2 (PC-2).....	58
Tabel 3.4.	Initial Permutation (IP).....	60
Tabel 3.5.	<i>E</i> bit Selection.....	61
Tabel 3.6.	Primitive S-Box Function.....	62
Tabel 3.7.	Permutation Function (P)	65
Tabel 3.8.	Inverse of Initial Permutation (IP^{-1}).....	67

DAFTAR SIMBOL

X, Y, S	: Himpunan
$x \in X$: x merupakan elemen himpunan X
$y \in Y$: y merupakan elemen himpunan Y
$\{a, b, c, \dots\}$: a, b, c, \dots merupakan elemen atau objek dari suatu himpunan
f	: Fungsi
$f(x)$: Fungsi dengan argumen x
$f(y)$: Fungsi dengan argumen y
$f : X \rightarrow Y$: Notasi untuk pemetaan X terhadap Y oleh fungsi f
$\text{Im}(f)$: Image atau bayangan dari f
r_x	: Remainder atau sisa dari suatu operasi yang didefinisikan oleh $f(x)$
$g = f^{-1}$: Fungsi invers dari f
n	: Nilai integer atau bilangan bulat
p	: Permutasi
$p : S \rightarrow S$: Pemetaan bijeksi fungsi permutasi
p^{-1}	: Invers fungsi permutasi
$f = g = f^{-1}$: Involusi yaitu suatu fungsi yang memiliki invers dirinya sendiri
\mathbb{Z}	: Integer atau bilangan bulat
\mathbb{Z}_n	: Bilangan Integer modulo n
$a b$: Integer a membagi integer b
$=$: Sama dengan
$+$: Tambah

/	: Bagi
-	: Kurang
\geq	: Lebih besar sama dengan
\leq	: Kurang dari sama dengan
<	: Kurang dari
>	: Lebih dari
\neq	: Tidak sama dengan
mod	: Sisa pembagian
div	: Hasil pembagian
$\lfloor a/b \rfloor$: Integer terbesar yang kurang dari atau sama dengan a/b
gcd(a,b)	: Faktor persekutuan terbesar dari integer a dan integer b
lcm(a,b)	: Kelipatan persekutuan terkecil
\equiv	: Kongruen
A	: Definisi alpabet
M	: Ruang pesan (message)
C	: Ruang Sandi (ciphertext)
K	: Ruang Kunci
$e \in K$: e adalah kunci enkripsi dan elemen dari K
$d \in K$: d adalah kunci dekripsi dan elemen dari K
$m \in M$: m adalah pesan dan elemen dari M
$c \in C$: c adalah sandi dan elemen dari C
m_i	: Message dengan indeks-i
e_i	: Kunci enkripsi dengan indeks-i

- d_i : Kunci dekripsi dengan indeks-i
- c_i : Sandi atau cipher dengan indeks-i
- E_e : Fungsi enkripsi dengan kunci e
- D_d : Fungsi dekripsi dengan kunci d
- E_i : Fungsi enkripsi dengan indeks-i
- \oplus : Eksklusif-OR (XOR)
- L_i : Bagian kiri
- R_i : Bagian kanan
- Γ_i : Fungsi XOR ekspansi R_i dengan kunci K_i
- $E(R_i)$: Ekspansi R_i
- $P(R_i)$: Permutasi R_i
- $S(B_i)$: Substitusi B_i

