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

(Drs. Bayu 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)	(Drs. Putut Sri Wasito)
NIP. 130 805 062	NIP. 130 877 410

HALAMAN PERSEMBAHAN

Tugas Akhir ini Saya persembahakan

Sebagai tanda bakti dan terima kasihku

Serta rasa cinta yang dalam kepada

Ayah Bunda Ku Tercinta

Dan Adik-adikku Tersayang

KATA PENGATAR

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 mengantar 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 spriritуil 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 kesempuranaan 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

DAFTAR GAMBAR

DAFTAR TABEL

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,...}	: a, b, c, ... 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
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
≥	: Lebih besar sama dengan
≤	: Kurang dari sama dengan
<	: Kurang dari
>	: Lebih dari
≠	: 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
≡	: 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
$\oplus$	:	Ekslusif-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