LEMBAR PENGESAHAN I

Judul	: Enkripsi Data Digital Berupa File Text Menggunakan Metode GOST (*Gosudarstvennyi Standard*) dan Aplikasinya Menggunakan Bahasa Pemrograman Delphi.
Nama	: Gun Maryadi
NIM	: J2A 096 026
Tanggal lulus ujian	: 3 Juli 2003

Semarang, Juli 2003

Ketua Jurusan Matematika	Panitia Ujian Sarjana Jurusan Matematika
(Drs. Bayu Surarso, M.Sc, PhD)	(Drs. Suhartono, MI Komp)
NIP. 131 764 886	NIP. 131 285 523

LEMBAR PENGESAHAN II

Enkripsi Data Digital Berupa File Text

Menggunakan Metode GOST (*Gosudarstvennyi Standard*)

Dan Aplikasinya Menggunakan Bahasa Pemrograman Delphi

Nama : Gun Maryadi

NIM : J2A 096 026

Telah diujikan pada ujian sarjana tanggal **3 Juli 2003** dan telah dinyatakan **LULUS**

Semarang, Juli 2003

Pembimbing Utama	Pembimbing Anggota
(Drs. Suhartono, MI Komp)	(Drs. Bambang Yismianto)
NIP. 131 285 523	NIP. 131 626 757

KATA PENGANTAR

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

Penulisan Tugas Akhir dengan judul : Enkripsi Data Digital Berupa File Text Menggunakan Metode GOST (*Gosudarstvennyi Standard*) Dan Aplikasinya Menggunakan Bahasa Pemrograman Delphi, 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 berbagai 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. Suhartono, MIKomp. Selaku Dosen Pembimbing I yang telah memberikan pengarahan hingga selesainya Tugas Akhir ini.
3. Bapak Drs. Bambang Yismianto. Selaku Pembimbing II yang telah banyak membantu meluangkan waktunya hingga penulis dapat menyusun Tugas Akhir ini.
4. Ibu Dra. Dwi Ispriyanti, M.Si. Selaku Dosen Wali yang dengan sabar dan nasehatnya telah mengantar penulis hingga selesai kuliah.
5. Seluruh staf pengajar Jurusan Matematika FMIPA UNDIP yang telah memberikan arahan dan ilmunya bagi penulis.

6. Ayah dan Ibuku tercinta, serta Kakak-kakakku tersayang yang telah memberikan dorongan baik secara materiil maupun spirituil kepada penulis.
7. Untuk teman-temanku angkatan 96 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 manfaatnya.

Semarang, 3 Juli 2003

Penulis

DAFTAR ISI

DAFTAR GAMBAR

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
$\mathrm{Im}(f)$	: Image atau bayangan dari f
$g = f^{-1}$	: 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
$\mathbb{Z}$	: Integer atau bilangan bulat
$\mathbb{Z}_n$	: Bilangan Integer modulo n
$a \mid b$	: 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
gcd(a,b)	: Faktor persekutuan terbesar dari integer a dan integer b
lcm(a,b)	: Kelipatan persekutuan terkecil
$\equiv$	: Kongruen
A	: Definisi alpabet
β	: Sistem bilangan yang mempunyai basis atau radix dua
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	: Subkunci enkripsi dengan indeks-i
d_i	: Subkunci 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_r : Data bagian kiri dengan indeks *r*

R_r : Data bagian kanan dengan indeks *r*

DAFTAR TABEL