

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)

NIP. 131 764 886

(Drs. Suhartono, MI Komp)

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

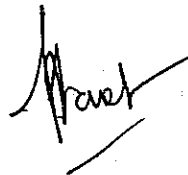
NIM : J2A 096 026

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

Semarang, Juli 2003

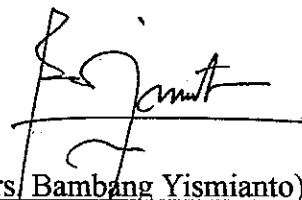
Pembimbing Utama

Pembimbing Anggota



(Drs. Suhartono, MI Komp)

NIP. 131 285 523



(Drs. Bambang Yismianto)

NIP. 131 626 757

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 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.

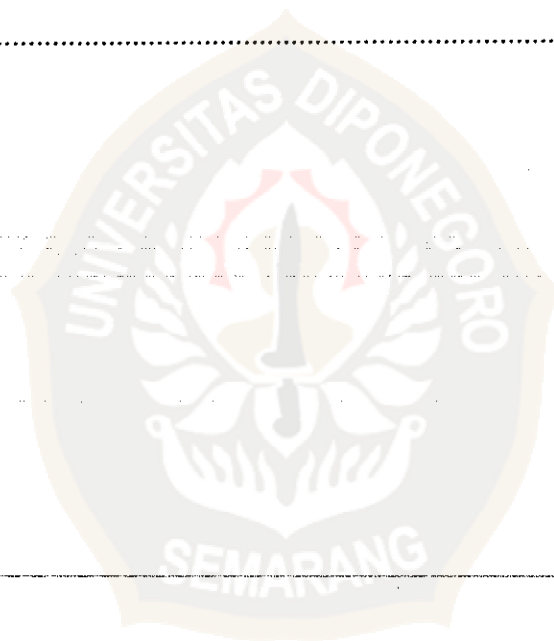
Penulis

DAFTAR ISI

HALAMAN JUDUL	i
LEMBAR PENGESAHAN	ii
KATA PENGANTAR	iv
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR SIMBOL	xii
DAFTAR TABEL	xvi
BAB I PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Perumusan Masalah.....	2
1.3. Pembatasan Masalah.....	3
1.4. Tujuan.....	3
1.5. Sistematika Penulisan.....	3
BAB II MATERI PENUNJANG	5
2.1. Teori Fungsi.....	5
2.1.1. Fungsi.....	5
2.1.2. Permutasi.....	7
2.2. Teori Bilangan.....	8
2.2.1. Integer.....	8

2.2.2. Integer Modulo n	9
2.2.3. Bilangan Biner	10
2.2.4. Bilangan Heksadesimal.....	12
2.2.5. Konversi Antar Basis	13
2.2.6. Bit (<i>Binary Digit</i>).....	14
2.2.7. Ukuran Bilangan	17
2.3. Operasi Logika.....	18
2.4. File	19
BAB III ENKRIPSI DENGAN METODE GOST	22
3.1. Kriptografi.....	22
3.2. Istilah Dasar dan Konsep Dasar.....	23
3.2.1. Domain Dan Kodomain Enkripsi.....	23
3.2.2. Transformasi Enkripsi Dan Transformasi Dekripsi.....	24
3.2.3. Partisipan Dalam Komunikasi	27
3.2.4. Saluran Komunikasi	27
3.2.5. Keamanan Dalam Kriptografi.....	28
3.2.6. Enkripsi Kunci Simetrik.	29
3.2.6.1. Sandi Substitusi Sederhana	32
3.2.6.2. Sandi Substitusi Homophonik	33
3.2.6.3. Sandi Substitusi Polialpabet.....	34
3.2.6.4. Sandi Transposisi	35
3.2.7. Panjang Kunci Simetrik	36
3.3. Enkripsi Dengan Metode GOST.....	37

3.3.1 Penjadwalan Kunci (<i>Key Schedule</i>).....	41
3.3.2. Proses Penyandian (<i>Encipherment</i>).....	43
3.3.3. Proses Dekripsi (<i>Decipherment</i>).....	48
3.4. Desain Program.....	53
BAB IV KESIMPULAN	56
DAFTAR PUSTAKA	57
LAMPIRAN	58



DAFTAR GAMBAR

Gambar 2.1. Sebuah fungsi dari himpunan X terhadap himpunan Y	5
Gambar 2.2. Sebuah fungsi bijeksi dari himpunan X terhadap himpunan Y	6
Gambar 2.3. Sebuah fungsi bijeksi f dan inversnya $g = f^{-1}$	7
Gambar 2.4. Aliran data antara memori internal dengan media penyimpanan eksternal	21
Gambar 3.1. Skema enkripsi sederhana	25
Gambar 3.2. Skema komunikasi dua pihak dengan menggunakan enkripsi....	26
Gambar 3.3. Dua pihak yang berkomunikasi menggunakan enkripsi.....	31
Gambar 3.4. Satu putaran GOST.....	39
Gambar 3.5. Flowchart program enkripsi	54
Tampilan 1. Menu utama program enkripsi dengan metode GOST	59
Tampilan 2. Tampilan pada saat mengklik tombol keterangan.....	59
Tampilan 3. Tampilan pada saat memasukkan file masukan yang akan dienkripsi.....	60
Tampilan 4. Tampilan setelah memasukkan file masukan yang akan dienkripsi.....	60
Tampilan 5. Tampilan pada saat memasukkan file keluaran hasil enkripsi.....	61
Tampilan 6. Tampilan setelah memasukkan file keluaran hasil enkripsi.....	61
Tampilan 7. Tampilan ketika memasukkan password	62
Tampilan 8. Tampilan setelah proses enkripsi selesai	62
Tampilan 9. Tampilan data yang belum dienkripsi.....	63
Tampilan 10. Tampilan data yang telah dienkripsi	63

Tampilan 11. Tampilan sebelum mengenkripsi string (tulisan)..... 64

Tampilan 12. Tampilan setelah proses mengenkripsi string dijalankan 64

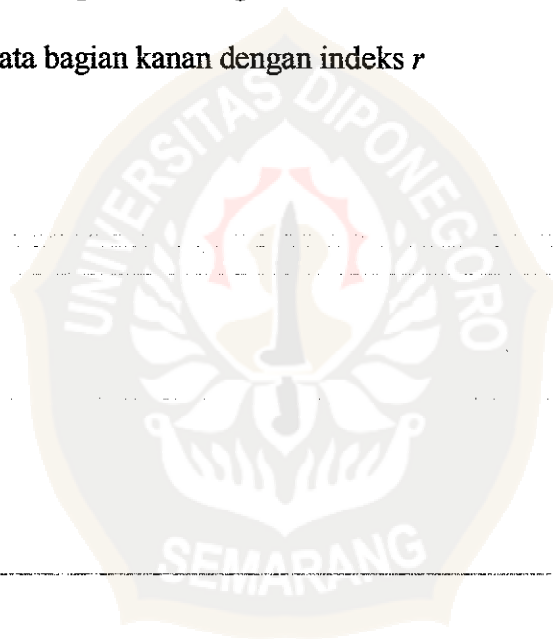


DAFTAR SIMBOL

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
$g = f^{-1}$: 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
Z	: Integer atau bilangan bulat
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
$\gcd(a,b)$: Faktor persekutuan terbesar dari integer a dan integer b
$\text{lcm}(a,b)$: Kelipatan persekutuan terkecil
\equiv	: Kongruen
A	: Definisi alfabet
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 : Eksklusif-OR (XOR)
- L_r : Data bagian kiri dengan indeks r
- R_r : Data bagian kanan dengan indeks r



DAFTAR TABEL

Tabel 2.1. Konversi desimal, biner dan heksadesimal	13
Tabel 2.2. Bit Paritas	16
Tabel 2.3. Operasi logika AND.....	19
Tabel 2.4. Operasi logika OR.....	19
Tabel 2.5. Operasi logika NOT	19
Tabel 2.6. Operasi logika X-OR.....	19
Tabel 3.1. Penggunaan Subkunci GOST Pada Tiap Putaran Untuk Proses Enkripsi.....	41
Tabel 3.2. Penggunaan Subkunci GOST Pada Tiap Putaran Untuk Proses Dekripsi.....	49

