HALAMAN PENGESAHAN

Lembar ke-1

Judul Skripsi : **Enkripsi Data Digital Menggunakan IDEA (*International Data Encryption Algorithm*)**

Nama : Wendy Puspitasari

NIM : J2A 096 064

Telah menempuh Ujian Sarjana pada tanggal **28 Juli 2003** dan dinyatakan **LULUS**.

Semarang, Juli 2003

Panitia Ujian Sarjana

Jurusan Matematika Universitas Diponegoro Semarang

Ketua Jurusan Matematika UNDIP	Ketua Tim Penguji
Drs. Bayu Surarso, MSc. PhD	Drs. Kushartantya, MI Komp.
NIP. 131 764 886	NIP.130 805 062

HALAMAN PENGESAHAN

Lembar ke-2

Judul Skripsi : **Enkripsi Data Digital Menggunakan IDEA (*International Data Encryption Algorithm*)**

Nama : Wendy Puspitasari

NIM : J2A 096 064

Telah menempuh Ujian Sarjana pada tanggal **28 Juli 2003** dan dinyatakan **LULUS**.

Semarang, Juli 2003

Pembimbing Utama	Pembimbing Anggota
Drs. Kushartantya, MI Komp.	Drs. Putut Sri Wasito
NIP.130 805 062	NIP 130 877 410

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 Menggunakan Metode IDEA (*International Data Encryption Algorthm*), 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. Kushartantya, MIKomp. Selaku Dosen Pembimbing I yang telah memberikan pengerahan hingga selesainya Tugas Akhir ini.
3. Bapak Drs. Putut Sri Wasito. Selaku Pembimbing II yang telah banyak membantu meluangkan waktunya hingga penulis dapat menyusun Tugas Akhir ini.
4. Ibu Dra. Suparti, 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, Juli 2003

Penulis

HALAMAN PERSEMBAHAN

... seluruh keberhasilan kupersembahkan untuk ...

Allah SWT, Tuhan Yang Maha Pengasih dan Penyayang

... untuk janji-Mu yang tak pernah ingkar ...

Mama dan Ayah

... untuk kasih sayang dan cinta yang sesungguhnya ...

... untuk kasih sepanjang masa ...

Mbak Uly dan Bang Dendy

... untuk semangatnya ...

The One, My Love and My Soul

... untuk perjalanannya ...

TERIMA KASIH

... hanya di lembar ini sajalah bisa kubalas kebaikan kalian ...

Igun, **The Thinker**, terima kasih untuk pemikiran dan semangatnya, juga komputer dan printernya.

Juliana dan Teguh (terima kasih hem putihnya, ya Li`!) ... dimanapun kamu, teman melampaui ruang dan waktu.

Etin dan Nur, untuk dukungannya.

Winda, Leny, Antin, dan teman-teman Kost Tunjungsari 7A untuk support-nya.

Anjar, FX Ari, Anam, Imunk, Laily, Henry, Titik, Farid dan teman-teman Matematika Angkatan 96 ... terima kasih untuk support-nya, terima kasih bantuannya ... **Seto, Woho, Arifin, Prilu** ... **AYO KAMU BISA !!!**

Prambors Semarang 102,3 FM *and all of The Wadya Bala, especially* ***Ari Bule and Diaz****, nice to hear your crazy jokes*

My Children at Permata Internusa School*, thanks for all joyfull moments! Love You All.*

Honda Supra V, AD 3367 AR dan Yamaha Jupiter, AD 4817 YG, tak pernah kau mengeluh, hanya bensin dan oli yang kamu minta.

My computer and my printer, kalau kamu mau coklat, berikan aku *dialog box.*

BARIS PENCERAH

... di baris-baris ini kutemukan sinaran ...

demi masa. sesungguhnya manusia benar-benar berada dalam kerugian. kecuali orang-orang yang beriman dan mengerjakan amal saleh dan nasehat menasehati supaya menaati kebenaran dan nasehat menasehati supaya menetapi kesabaran.
(Qur`an:103 Al `Ashr)

one moment lost and passing by - fielding me from my own destiny – taking away my pride cracking me into pieces – making me like a fool - - so now I stand here with this conviction – reaching out for perfection – I put my life at stake for any reason – and it`s time for turning back
although I`ve been hurt and things are fallen – shattering before my eyes – I know I have something inside of me – and that makes me strong
from this moment on I`ll live, I`ll stand, and I`ll be the best I can be – cause I am work of heaven.
(padi, song of 2002 fifa world cup[tm]).

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

Lampiran Tampilan Program

Listing Program

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
$\mathbb{Z}$	: Himpunan bilangan bulat
$\mathbb{Z}_n$	: Himpunan bilangan bulat 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)

$\boxplus$: Penambahan mod 2^{16}

$\odot$: Perkalian modulus $2^{16} + 1$