

## HALAMAN PENGESAHAN

### Lembar ke-1

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

Nama : Wendy Puspitasari

NIM : J2A 096 064

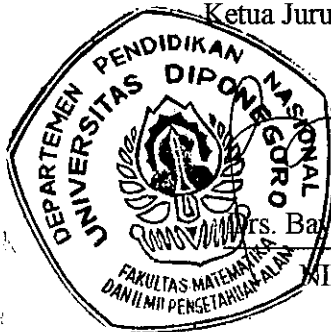
Telah menempuh Ujian Sarjana pada tanggal **28 Juli 2003** dan dinyatakan **LULUS**.


Semarang, Juli 2003

Panitia Ujian Sarjana

Jurusan Matematika Universitas Diponegoro Semarang

Ketua Jurusan Matematika UNDIP



  
Drs. Batu Surarso, MSc. PhD

NIP. 131 764 886

Ketua Tim Penguji

Drs. Kushartantya, MI Komp.

NIP.130 805 062

## HALAMAN PENGESAHAN

### Lembar ke-2

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

Nama : Wendy Puspitasari

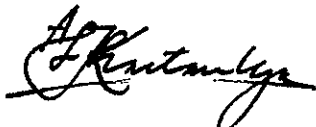
NIM : J2A 096 064

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

Semarang, Juli 2003

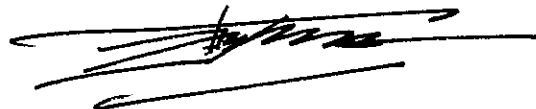
Pembimbing Utama

Pembimbing Anggota



Drs. Kushartantya, MI Komp.

NIP.130 805 062



Drs. Putut Sri Wasito

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 Algorith*m), 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 pencerahan 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 ku persembahkan 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™).**

## DAFTAR ISI

<b>HALAMAN JUDUL</b> .....	i
<b>HALAMAN PENGESAHAN</b> .....	ii
<b>KATA PENGANTAR</b> .....	iv
<b>HALAMAN PERSEMBAHAN</b> .....	vi
<b>ABSTRAK</b> .....	ix
<b>ABSTRACT</b> .....	x
<b>DAFTAR ISI</b> .....	xi
<b>DAFTAR GAMBAR</b> .....	xiv
<b>DAFTAR TABEL</b> .....	xv
<b>DAFTAR LAMPIRAN</b> .....	xvi
<b>DAFTAR SIMBOL</b> .....	xvii
<b>BAB I PENDAHULUAN</b> .....	1
1.1. Latar Belakang.....	1
1.2. Perumusan Masalah.....	2
1.3. Pembatasan Masalah.....	2
1.4. Tujuan.....	3
1.5. Metode Pembahasan.....	3
1.6. Garis Besar Pemecahan Masalah.....	3
1.6.1. Pengantar Kriptografi.....	3
1.6.2. Metode IDEA.....	7
1.7. Sistematika Penulisan.....	8



<b>BAB II MATERI PENUNJANG</b> .....	9
2.1. Konsep Dasar Matematika.....	9
2.1.1. Fungsi.....	9
2.1.1.1. Permutasi .....	14
2.1.1.2. Involusi .....	15
2.1.2. Teori Bilangan .....	16
2.1.2.1. Integer .....	16
2.1.2.2. Integer Modulo $n$ .....	18
2.1.3. Bilangan Biner .....	20
2.1.4. Bilangan Heksadesimal.....	21
2.1.5. Konversi Antar Basis .....	22
2.1.6. Bit (Binary <i>Digit</i> ).....	24
2.1.6.1. Bit Paritas.....	24
2.1.6.2. Paritas Genap Dan Paritas Ganjil .....	25
2.1.7. Ukuran Bilangan .....	27
2.1.8. Operasi Logika.....	28
2.1.9. File .....	30
<b>BAB III PENERAPAN METODE IDEA UNTUK KEAMANAN DATA</b>	
<b>DIGITAL</b> .....	31
3.1. Kriptografi .....	31
3.2. Konsep Dan Terminologi Dasar .....	33
3.2.1. Domain Dan Kodomain Enkripsi.....	33
3.2.2. Transformasi Enkripsi Dan Dekripsi .....	34

3.2.3. Partisipan Dalam Komunikasi .....	37
3.2.4. Keamanan Dalam Kriptografi.....	38
3.2.5. Enkripsi Kunci Simetrik .....	39
3.2.5.1. Sandi Substitusi Sederhana.....	42
3.2.5.2. Sandi Substitusi Polialpabet.....	43
3.2.5.3. Sandi Transposisi.....	44
3.2.6. Panjang Kunci Simetrik.....	45
3.3. Enkripsi Dengan Metode IDEA.....	48
3.3.1 Penjadwalan Kunci Proses Enkripsi ( <i>Encipherment Key Schedule</i> ). 51	
3.3.2 Proses Enkripsi ( <i>Encipherment</i> ).....	53
3.3.3 Penjadwalan Kunci Proses Dekripsi ( <i>Decipherment Key Schedule</i> ). 62	
3.3.4 Proses Dekripsi ( <i>Decipherment</i> ) .....	65
3.4. Desain Program IDEA .....	70
<b>BAB IV KESIMPULAN .....</b>	<b>72</b>
<b>DAFTAR PUSTAKA .....</b>	<b>73</b>
<b>LAMPIRAN.....</b>	<b>74</b>

## DAFTAR GAMBAR

Gambar 1.1. Diagram Alur Proses Enkripsi .....	5
Gambar 1.2. Proses Enkripsi dan Dekripsi dengan Kunci .....	6
Gambar 2.1. Sebuah fungsi dari himpunan $X$ terhadap himpunan $Y$ .....	10
Gambar 2.2. Sebuah fungsi satu-satu $f$ .....	11
Gambar 2.3. Sebuah fungsi onto .....	11
Gambar 2.4. Sebuah fungsi bijeksi $f$ .....	12
Gambar 2.5. Sebuah fungsi bijeksi $f$ dan inversnya $g = f^{-1}$ .....	13
Gambar 2.6. Involusi himpunan $S$ dengan 5 buah elemen.....	16
Gambar 3.1. Enkripsi sederhana .....	35
Gambar 3.2. Skema komunikasi dua pihak dengan menggunakan enkripsi.....	36
Gambar 3.3. Dua pihak yang berkomunikasi menggunakan enkripsi dengan saluran informasi yang aman untuk pertukaran kunci, kunci dekripsi $d$ dapat diperoleh dari kunci enkripsi $e$ .....	41
Gambar 3.4. Diagram Alur Perhitungan IDEA .....	49
Gambar 3.5. Flowchart program enkripsi IDEA .....	71

## DAFTAR TABEL

Tabel 2.1. Konversi desimal, biner dan heksadesimal .....	22
Tabel 2.2. Bit Paritas .....	26
Tabel 2.3. Operasi logika AND.....	29
Tabel 2.4. Operasi logika OR.....	29
Tabel 2.5. Operasi logika NOT .....	29
Tabel 2.6. Operasi logika X-OR.....	29
Tabel 2.7. Operasi logika penambahan modulus $2^{16}$ .....	29
Tabel 2.6. Operasi logika perkalian modulus $2^{16} + 1$ .....	29
Tabel 3.1. Penggunaan Subkunci IDEA Pada Tiap Putaran Untuk Proses Enkripsi.....	52
Tabel 3.2. Hasil Enkripsi untuk Putaran Ketiga Sampai Kedelapan.....	61
Tabel 3.3. Subkunci IDEA Pada Tiap Putaran Proses Dekripsi.....	63
Tabel 3.4. Penggunaan Subkunci IDEA Pada Tiap Putaran Untuk Proses Dekripsi.....	65
Tabel 3.5. Hasil Dekripsi untuk Putaran Kedua Sampai Kedelapan .....	68

## DAFTAR LAMPIRAN

### Lampiran Tampilan Program

Tampilan 1. Menu utama program enkripsi dengan metode IDEA .....	74
Tampilan 2. Tampilan sebelum mengenkripsi tulisan .....	75
Tampilan 3. Tampilan setelah proses mengenkripsi tulisan dijalankan .....	75
Tampilan 4. Tampilan pada saat memasukkan file masukan yang akan dienkripsi .....	76
Tampilan 5. Tampilan setelah memasukkan file masukan yang akan Dienkripsi .....	76
Tampilan 6. Tampilan pada saat memasukkan file keluaran hasil enkripsi .....	77
Tampilan 7. Tampilan setelah memasukkan file keluaran hasil enkripsi .....	77
Tampilan 8. Tampilan setelah proses enkripsi selesai .....	78
Tampilan 9. Tampilan data yang belum dienkripsi .....	79
Tampilan 10. Tampilan data yang telah dienkripsi .....	79

### Listing Program

Listing Program untuk Unit Main .....	80
Listing Program untuk Unit DCPcrypt .....	86
Listing Program untuk Unit IDEA .....	91
Listing Program untuk Unit SHA1 .....	101

## 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
$\mathbb{Z}$	: Himpunan bilangan bulat
$\mathbb{Z}_n$	: Himpunan bilangan bulat 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 alpabet
$\beta$	: 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 )
- $\boxplus$  : Penambahan mod  $2^{16}$
- $\odot$  : Perkalian modulus  $2^{16} + 1$