

## **TUGAS AKHIR**

# **IMPLEMENTASI PROGRAM ENKRIPSI DESKRIPSI DENGAN MENGGUNAKAN BAHASA PEMROGRAMAN DELPHI**

**Disusun Untuk Memenuhi Syarat  
Mencapai Gelar Kesarjanaan Strata-Satu (S1)**

**DISUSUN OLEH**

**NAMA : HERU WIRANTO  
NIM : 01598-004**



**UNIVERSITAS  
MERCU BUANA**

**JURUSAN TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INDUSTRI  
UNIVERSITAS MERCU BUANA**

**JAKARTA**

**2005**

|                                |                |
|--------------------------------|----------------|
| Yayasan Menara Bhakti          |                |
| <b>UNIVERSITAS MERCU BUANA</b> |                |
| Perpustakaan Pusat             |                |
| Sumbu                          | S              |
| Tanggal                        | " Agt 2005     |
| No Reg                         | STI / 05 / 109 |
|                                | 05 / 5 / 428   |

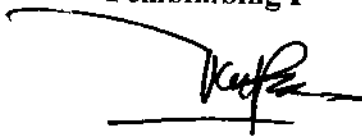
## LEMBAR PENGESAHAN TUGAS AKHIR

Yang bertanda tangan dibawah ini menyatakan bahwa Tugas Akhir dari Mahasiswa berikut ini :

Nama : HERU WIRANTO  
NIM : 01598-004  
Fakultas : Teknologi Industri  
Jurusan : Teknik Informatika  
Judul : " Implementasi Program Enkripsi Dekripsi Dengan  
Menggunakan Bahasa Pemrograman Delphi"

Telah diperiksa dan disetujui untuk disidangkan pada Sidang Tugas Akhir Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Mercu Buana :

Pembimbing I



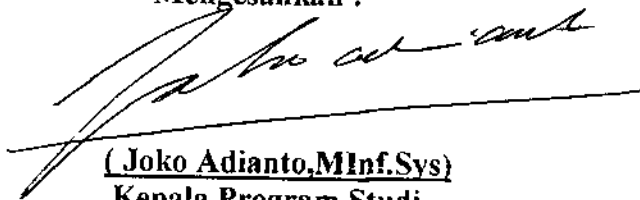
(Ir. Nixon Erzed.MT)

Pembimbing II



( Ratna Mutu Manikam.SKom.MT)

Mengesahkan :



(Joko Adianto,MInf.Sys)  
Kepala Program Studi  
Jurusan Teknik Informatika

Mengetahui :



(Abdusy Syarif.ST)  
Koordinator Tugas Akhir  
Jurusan Teknik Informatika

## SURAT PERNYATAAN

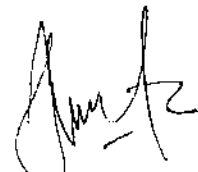
Yang bertanda tangan dibawah ini :

**NAMA : HERU WIRANTO**

**NIM : 01598-004**

Menyatakan bahwa **Tugas Akhir (TA)** ini adalah hasil buatan sendiri bukan hasil jiplakan atau mencontek karya orang lain kecuali yang tercantum dalam daftar pustaka.

Jakarta, 21 Juni 2005



Heru Wiranto

## KATA PENGANTAR

*Assalamua'alaikum Wr.Wb*

Dengan menyebut nama Allah SWT Yang Maha Kuasa dan yang telah memberikan rahmat dan Ridho-Nya hingga penulisan Tugas Akhir ini dapat diselesaikan.

Proses pembuatan pemrograman enkripsi data dan deskripsi data dengan menggunakan bahasa pemrograman Delphi merupakan salah satu cara membuat sistem penyandian data secara sederhana sehingga mudah dipahami untuk dipelajari.

Algoritma DES (Data Encryption Standard) dan Algoritma AES (Advance Data Standard) ini merupakan suatu teknik untuk membuat program sistem penyandian data yang lebih mudah dipahami dan mudah dipelajari oleh penulis.

Pada tahap "*Finishing*" atau tahap penyelesaian, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya atas bimbingan, motivasi dan bantuan yang telah diberikan baik moril maupun materiil. Rasa terima kasih ini saya berikan kepada :

1. Bapak Ir. Nixon Erzed, MT selaku Dosen Pembimbing I
2. Ibu Ratna Mutu Manikam, SKomp.MT sebagai Dosen Pembimbing II
3. Bapak Joko Adiinto, M.Inf.Sys selaku Ketua Jurusan Teknik Informatika
4. Bapak Abdusy Syarif, ST selaku Ketua Koordinator Tugas Akhir Jurusan Teknik Informatika.
5. Bapak Raka Yusuf, ST yang telah memberikan dorongan moril dan motivasinya.
6. Semua Dosen Teknik Informatika yang tidak bisa disebutkan satu persatu, dengan tanpa mengurangi rasa hormat penulis.

7. Kedua Orangtua, Bapak Djumiran Sudwiyanto dan Ibu Parilah yang telah memberikan biaya selama perkuliahan penulis dan saudara-saudari tercinta yang telah banyak membantu baik materil dan maupun doa yang diberikan kepada penulis.
8. Bapak Suhardjo beserta keluarganya yang telah membantu meminjamkan komputernya kepada penulis untuk menyelesaikan Tugas Akhir ini.
9. Ahmad Nur Hidayat, Joehana, Riki Arif Trianto, Triady, M Sofyan, dan Okky Soemirat, Nur Yasin atas bantuan dan motivasi yang diberikan.
10. Teman-teman seperjuangan Himpunan Teknik Informatika yang tak mungkin disebutkan satu-persatu.

Penulis menyadari bahwa dalam penulisan Tugas Akhir ini masih banyak kekurangannya, oleh karena itu kritik dan saran yang membangun serta dorongan agar penulisan Tugas Akhir ini dapat mencapai kesempurnaan sangat penulis harapkan.

Akhir kata mohon maaf yang sebesar-besarnya atas segala kekurangannya dan harapan penulis, semoga Tugas Akhir ini dapat bermanfaat bagi penulis khususnya dan pembaca pada umumnya. *Amin Yaa Robbal A'laamin.*

Jakarta, 2005

Penulis

## DAFTAR ISI

|                                     |      |
|-------------------------------------|------|
| <b>LEMBAR PENGESAHAN</b> .....      | i    |
| <b>SURAT PERNYATAAN</b> .....       | ii   |
| <b>ABSTRAK</b> .....                | iii  |
| <b>ABSTRACT</b> .....               | iv   |
| <b>KATA PENGANTAR</b> .....         | v    |
| <b>DAFTAR ISI</b> .....             | vii  |
| <b>DAFTAR GAMBAR</b> .....          | xi   |
| <b>DAFTAR TABEL</b> .....           | xiii |
| <b>DAFTAR SIMBOL</b> .....          | xiv  |
| <b>BAB I PENDAHULUAN</b>            |      |
| 1.1 Latar Belakang.....             | 1    |
| 1.2 Permasalahan.....               | 1    |
| 1.3 Ruang Lingkup Permasalahan..... | 2    |
| 1.4 Tujuan .....                    | 3    |
| 1.5 Metodologi Perangkat Lunak..... | 3    |
| 1.6 Sistematika Penulisan.....      | 5    |

## **BAB II SISTEM KRIPTOGRAFI**

|                                                     |    |
|-----------------------------------------------------|----|
| 2.1 Pengertian Kriptografi.....                     | 7  |
| 2.2 Mekanisme Sistem Kriptografi.....               | 9  |
| 2.3 Pengenalan Algoritma DES dan Algoritma AES..... | 13 |
| 2.3.1 Algoritma DES.....                            | 13 |
| 2.3.2 Algoritma AES.....                            | 14 |
| 2.4 Sistem Kriptografi.....                         | 15 |
| 2.4.1 Sistem Kriptografi Simetrik.....              | 16 |
| 2.4.2 Sistem Kriptografi Asimetrik.....             | 19 |
| 2.4.3 Sistem Kriptografi Gabungan.....              | 21 |
| 2.5 Protokol Kriptografi.....                       | 23 |
| 2.5.1 Fungsi Sistem Protokol Kriptografi.....       | 24 |
| 2.5.2 Deteksi Penyerangan Terhadap Protokol.....    | 25 |
| 2.5.3 Cryptanalyst Attack.....                      | 26 |
| 2.5.4 Jenis Penyerangan.....                        | 28 |
| 2.6 Tanda Tangan Digital.....                       | 30 |
| 2.7 Sertifikat Digital.....                         | 31 |
| 2.8 Secure Socket Layer (SSL).....                  | 31 |
| 2.9 Public Key Kriptografi.....                     | 32 |

### **BAB III ANALISA DAN PERANCANGAN**

|       |                                                                 |    |
|-------|-----------------------------------------------------------------|----|
| 3.1   | Analisa Permasalahan Dan Alternatif Pemecahan Permasalahan..... | 33 |
| 3.1.1 | Analisa Permasalahan.....                                       | 33 |
| 3.1.2 | Alternatif pemecahan Permasalahan.....                          | 36 |
| 3.2   | Rancangan Tampilan Layar DES.....                               | 37 |
| 3.2.1 | Program HeruMainDlg.....                                        | 41 |
| 3.2.2 | Program HeruUnit.....                                           | 49 |
| 3.2.3 | Program KeyInfoDlg.....                                         | 56 |
| 3.2.4 | Program KeySourceDlg.....                                       | 58 |
| 3.2.5 | Program KeyBoardDlg.....                                        | 62 |
| 3.2.6 | Program KeyFileDlg.....                                         | 65 |
| 3.2.7 | Program Myprogress.....                                         | 67 |

### **BAB IV IMPLEMENTASI PROGRAM ENKRIPSI DESKRIPSI DENGAN MENGUNAKAN BAHASA PEMROGRAMAN DELPHI**

|       |                                                   |    |
|-------|---------------------------------------------------|----|
| 4.1   | Setting Pengimplementasian Program.....           | 68 |
| 4.2   | Langkah Pembuatan Program Enkripsi Deskripsi..... | 69 |
| 4.2.1 | Tampilan Form HeruMainDlg.....                    | 69 |
| 4.2.2 | Tampilan Form KeyInfoDlg.....                     | 71 |
| 4.2.3 | Tampilan Form KeySourceDlg.....                   | 73 |
| 4.2.4 | Tampilan Form KeyBoardDlg.....                    | 75 |

|                                          |    |
|------------------------------------------|----|
| 4.2.5 Tampilan Form KeyFile.....         | 76 |
| 4.2.6 Tampilan Form My Progress Bar..... | 77 |
| 4.2.7 Tampilan Form Heru Unit.....       | 79 |
| 4.3 Tampilan Program Heru Project.....   | 79 |
| 4.3.1 Proses Enkripsi Data.....          | 80 |
| 4.3.2 Proses Deskripsi Data.....         | 82 |
| 4.4 Hasil Pengujian.....                 | 86 |

## **BAB V PENUTUP**

|                     |    |
|---------------------|----|
| 5.1 Kesimpulan..... | 90 |
| 5.2 Saran.....      | 91 |

## **DAFTAR PUSTAKA**

## **LAMPIRAN - LAMPIRAN**

## **LEMBAR ASISTENSI**

## DAFTAR GAMBAR

|             |                                                                |    |
|-------------|----------------------------------------------------------------|----|
| Gambar 1.1  | Daur Hidup Klasik ( <i>Classic Live Cycle</i> ).....           | 3  |
| Gambar 2.1  | Proses Enkripsi Deskripsi Sederhana.....                       | 8  |
| Gambar 2.2  | Mekanisme Proses Sistem Kriptografi.....                       | 11 |
| Gambar 2.3  | Kriptografi Berbasis Kunci ( <i>Key</i> ).....                 | 12 |
| Gambar 2.4  | Penerapan Sistem Kriptografi Secara Real.....                  | 12 |
| Gambar 2.5  | Mekanisme Sistem Kriptografi Simetrik.....                     | 18 |
| Gambar 2.6  | Penggunaan Kunci Asimetrik.....                                | 19 |
| Gambar 2.7  | Mekanisme Sistem Kriptografik Asimetrik.....                   | 20 |
| Gambar 2.8  | Tanda Tangan Digital.....                                      | 30 |
| Gambar 2.9  | Sertifikat Digital.....                                        | 31 |
| Gambar 3.1  | Flowchart Rancangan Algoritma DES.....                         | 37 |
| Gambar 3.2  | Flowchart Tampilan Layar Proses Enkripsi.....                  | 38 |
| Gambar 3.3  | Flowchart Tampilan Layar proses deskripsi.....                 | 39 |
| Gambar 3.4  | Flowchart Program HeruMainDlg.....                             | 42 |
| Gambar 3.5  | Flowchart Procedure Crypton pada Program HeruMainDlg.....      | 43 |
| Gambar 3.5a | Flowchart Proses Enkripsi pada Program HeruMainDlg.....        | 44 |
| Gambar 3.5b | Flowchart Proses Deskripsi pada Program HeruMainDlg.....       | 45 |
| Gambar 3.5c | Flowchart Function.GetKey pada Program HeruMainDlg.....        | 46 |
| Gambar 3.5d | Flowchart Procedure MyBlockWrite pada Program HeruMainDlg..... | 46 |
| Gambar 3.5e | Flowchart Procedure MyBlockRead pada Program HeruMainDlg.....  | 47 |
| Gambar 3.6  | Flowchart Procedure Program HeruUnit.....                      | 50 |

|              |                                                                                |    |
|--------------|--------------------------------------------------------------------------------|----|
| Gambar 3.6.a | Flowchart Procedure dan Function pada Program HeruUnit.....                    | 51 |
| Gambar 3.7   | Flowchart Program KeyInfoDlg.....                                              | 57 |
| Gambar 3.8   | Flowchart Program KeySourceDlg.....                                            | 58 |
| Gambar 3.9   | Flowchart Program KeyInfoDlg.....                                              | 63 |
| Gambar 3.10  | Flowchart Program KeyFileDialog.....                                           | 65 |
| Gambar 4.1   | Form Program HeruMainDlg.....                                                  | 71 |
| Gambar 4.2   | Form Program KeyInformationDlg.....                                            | 73 |
| Gambar 4.3   | Form Program KeySourceDlg.....                                                 | 74 |
| Gambar 4.4   | Form Program KeyBoardDlg.....                                                  | 76 |
| Gambar 4.5   | Form Program KeyFileDialog.....                                                | 77 |
| Gambar 4.6   | Form Program My Progress Bar.....                                              | 78 |
| Gambar 4.7   | Tampilan Program HeruProject pada saat dijalankan.....                         | 79 |
| Gambar 4.8   | Tampilan Proses Penekanan Tombol Enkripsi Data.....                            | 80 |
| Gambar 4.9   | Tampilan Informasi Kunci Yang Akan Digunakan<br>Untuk Enkripsi Data.....       | 81 |
| Gambar 4.10  | Tampilan Proses penekanan tombol Deskripsi Data.....                           | 82 |
| Gambar 4.11  | Tampilan Informasi Kunci yang digunakan untuk Deskripsi Data.....              | 83 |
| Gambar 4.12  | Tampilan KeySourceDlg Pada Saat Dijalankan.....                                | 84 |
| Gambar 4.13  | Tampilan KeyBoard Dlg pada saat dijalankan.....                                | 85 |
| Gambar 4.14  | Tampilan Kotak Open Dialog untuk membuka file yang akan<br>dideskripsikan..... | 85 |
| Gambar 4.15  | Tampilan Proses Hasil File teks ketika dieksekusi programnya.....              | 86 |

## DAFTAR TABEL

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| Tabel 2.1 Nama samaran untuk mempermudah penjelasan kriptografi.....    | 16 |
| Tabel 4.1 Hasil Pengujian dengan menggunakan metode enkripsi data.....  | 87 |
| Tabel 4.2 Ukuran File sebelum dan sesudah di Enkripsi.....              | 88 |
| Tabel 4.3 Hasil Pengujian dengan menggunakan metode Deskripsi data..... | 88 |
| Tabel 4.4 Ukuran sebelum dan sesudah file di Deskripsi.....             | 89 |