

BAB V

IMPLEMENTASI PERANGKAT LUNAK

5.1 Implementasi Secara Umum

Implementasi merupakan tahap dimana sistem siap dioperasikan pada keadaan sebenarnya dari sini akan diketahui apakah sistem yang dibuat benar-benar dapat menghasilkan tujuan yang diinginkan.

Sebelum program diterapkan dan diimplementasikan, maka program harus error free (bebas kesalahan). Kesalahan program yang mungkin terjadi antara lain kesalahan penulisan bahasa, kesalahan waktu proses, atau kesalahan logika. Setelah program bebas dari kesalahan, program ditest dengan memasukkan data yang akan diolah.

5.2 Batasan Implementasi

Pada bagian ini akan menjelaskan apa yang menjadi batasan implementasi perangkat lunak, antara lain; bahasa yang dipakai serta alasan pemilihannya, lingkungan pengembangan perangkat lunak dan batasan-batasan lain yang juga ditemui selama pengembangan.

5.2.1 Bahasa Yang Dipakai

Perangkat lunak yang dipakai untuk program enkripsi RSA adalah Borland Delphi 7 yang merupakan salah satu bahasa komputasi teknis yang sangat populer dan sangat mudah digunakan serta mudah untuk dipahami strukturnya, sehingga tidaklah mengherankan jika diputuskan untuk memilih Borland Delphi

7. Alasan lain menggunakan bahasa ini karena Borland Delphi 7 mempunyai beberapa fasilitas yang dapat mendukung pemrograman yang akan dibuat.

5.2.2 Lingkungan Pengembangan

Implementasi perangkat lunak untuk keamanan dokumen elektronik digunakan dan dikembangkan dan digunakan pada komputer yang memenuhi standar spesifikasi yang disebutkan dibawah ini agar dapat berjalan dengan baik dan sempurna.

Spesifikasi yang perlu diperhatikan dalam pengembangan dan penggunaan perangkat lunak ini adalah

1. Perangkat keras (Hardware) minimal yang digunakan dalam pengembangan sistem ini adalah berupa satu unit komputer/PC dengan prosesor celeron 1GHz dengan RAM 128 MB dan Hardiks 40 GB serta VGA Onboard (8 MB)
2. Spesifikasi perangkat lunak (Software) yang dibutuhkan antara lain Borland Delphi 7 dengan sistem operasi Windows Xp Profesional.

5.2.3 Batasan-batasan yang Digunakan

Karena implementasi program enkripsi menggunakan algoritma RSA ini bersifat studi/pembelajaran sehingga memiliki batasan-batasan implementasi antara lain:

- Untuk enkripsi menggunakan kunci publik yang diperoleh melalui proses pembangkitan kunci yang berupa angka bulat desimal. Dalam pembuatan kunci diperoleh pasangan kunci privat dan publik yang diperoleh dari

bilangan prima yang dipilih secara random dari angka 2 sampai dengan 100000

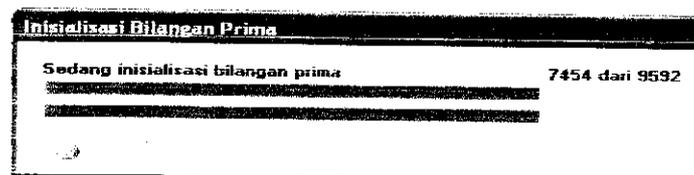
- Kunci yang telah diperoleh bisa disimpan dengan ekstensi *.pub untuk kunci publik dan *.pri untuk kunci privat
- Untuk enkripsi file disini dibatasi samapai file dengan ukuran 50 Mb karena keterbatasan space hardisk dan memori yang ada pada komputer
- File hasil enkripsi berupa bilangan bulat desimal yang tersusun vertikal. File ini berekstensi *.enc

5.3 Implementasi Antarmuka

Pada bagian ini akan digambarkan interface yang akan ditemui selama penggunaan perangkat lunak ini. Antarmuka tersebut antara lain; tampilan menu utama, pembangkitan kunci, enkripsi/dekripsi file, enkripsi/dekripsi teks, dan penjelasan tentang algoritma RSA.

5.3.1 Flash Screen

Sebelum proses aplikasi masuk pada menu utama terlebih dahulu program akan menjalankan proses inialisasi bilangan prima dari 2 sampai dengan 100000. Flash screen akan hilang ketika inisualisai bilangan prima telah selesai. Tampilan formnya dapat dilihat pada pada gambar 5.1.



Gambar 5.1. Proses inisialisai bilangan prima

5.3.2 Interface Menu Utama

Tampilan menu utama pada sistem pengamanan data menggunakan algoritma RSA berisi beberapa tombol yang menggambarkan proses-proses yang bisa dilakukan oleh sistem. Adapun panel-panel tersebut adalah :

- Algoritma RSA

Tombol ini berfungsi untuk menampilkan tentang algoritma RSA dan cara perhitungannya secara singkat.

- Kunci

Tombol ini berfungsi untuk menampilkan form proses pembangkitan kunci.

- File & folder

Tombol ini berfungsi untuk menampilkan form proses enkripsi/dekripsi file dan folder.

- Plain text

Tombol ini berfungsi untuk menampilkan form proses enkripsi/dekripsi teks.

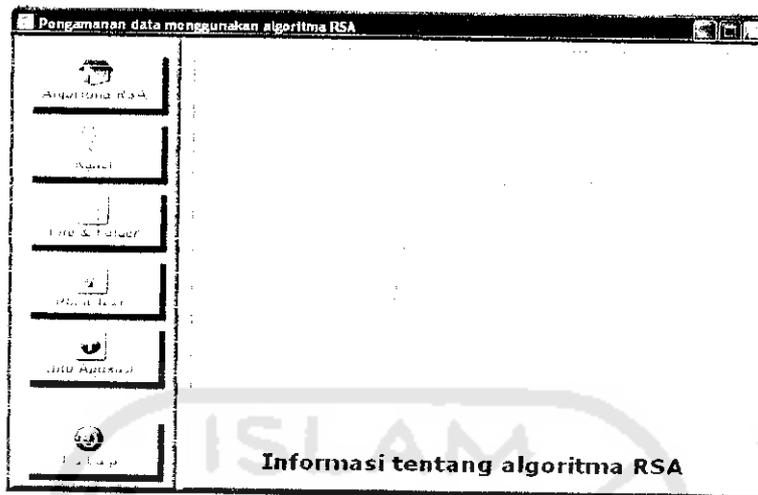
- Info aplikasi

Tombol ini berfungsi untuk menampilkan informasi aplikasi.

- Tutup

Tombol ini berfungsi untuk keluar dari program.

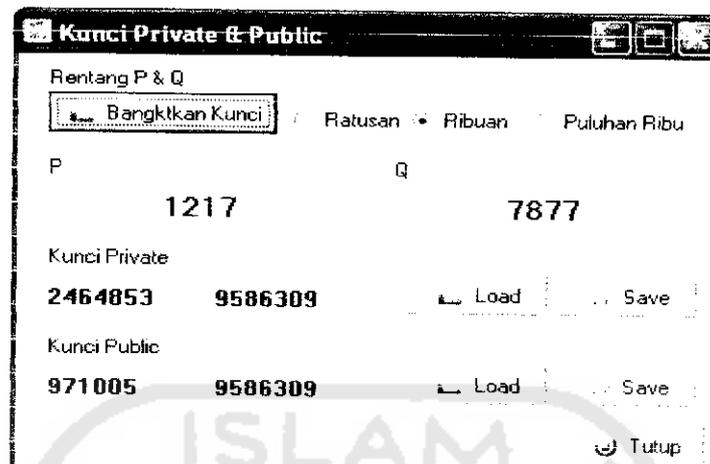
Tampilan menu utama aplikasi dapat dilihat pada gambar 5.2.



Gambar 5.2. Antarmuka menu utama

5.3.3 Interface Pembangkitan Kunci

Tampilan pada pembangkitan kunci berisi tombol bangkitan kunci yang berfungsi untuk memilih bilangan prima (P dan Q) secara random kemudian dari bilangan prima tersebut diperoleh pasangan kunci publik dan kunci privat. Dalam pemilihan bilangan prima disediakan radio button yang berfungsi untuk menentukan besar bilangan prima dari ratusan, ribuan dan puluhan ribu. Setelah diperoleh kunci privat dan kunci publik, kedua pasangan kunci tersebut dapat disimpan dengan menekan tombol save pada setiap kunci. Kunci yang tersimpan nantinya bisa dibuka lagi dengan menekan tombol load. Untuk menuju proses berikutnya form ini harus ditutup terlebih dahulu. Tampilan pembangkitan kunci dapat dilihat pada gambar 5.3.



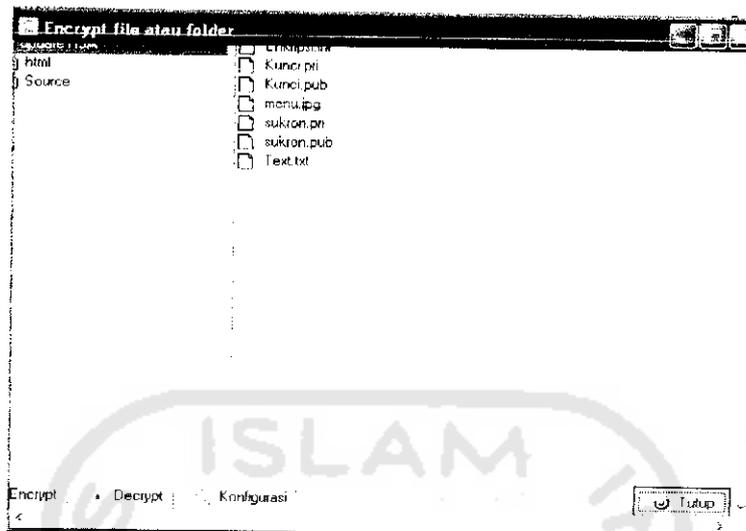
Gambar 5.3. Antarmuka pembangkitan kunci

5.3.4 Interface Enkripsi dan Dekripsi File

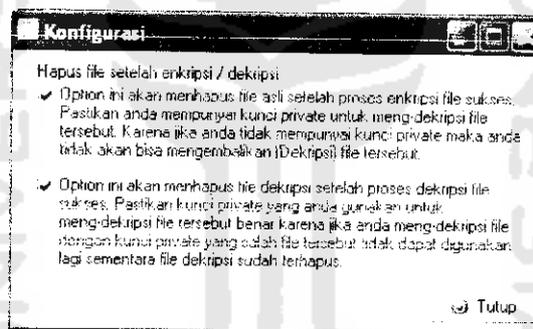
Setelah diperoleh pasangan kunci proses berikutnya adalah enkripsi/ dekripsi. Ada dua jenis enkripsi/dekripsi dalam program ini yaitu enkripsi file atau folder serta enkripsi teks. Pada tampilan enkrip file atau folder terdiri dari:

- Drivecombobox yang berfungsi untuk menampilkan posisi file pada hardisk.
- Directorylistbox untuk menampilkan folder.
- Filelistbox untuk menampilkan file-file yang ada dalam suatu folder.
- Tombol encrypt berfungsi untuk melakukan proses enkripsi.
- Tombol decrypt berfungsi untuk melakukan proses dekripsi.
- Tombol konfigurasi adalah berisi pilihan tindakan user terhadap file atau folder yang akan dienkripsi (apakah file asli akan dihapus atau tidak).
- Tombol tutup adalah untuk menutup form enkrip file.

Tampilan enkripsi file dapat dilihat pada gambar 5.4. Dan tampilan konfigurasi pada gambar 5.5.



Gambar 5.4. Antarmuka enkripsi file atau folder.



Gambar 5.5. Antarmuka konfigurasi.

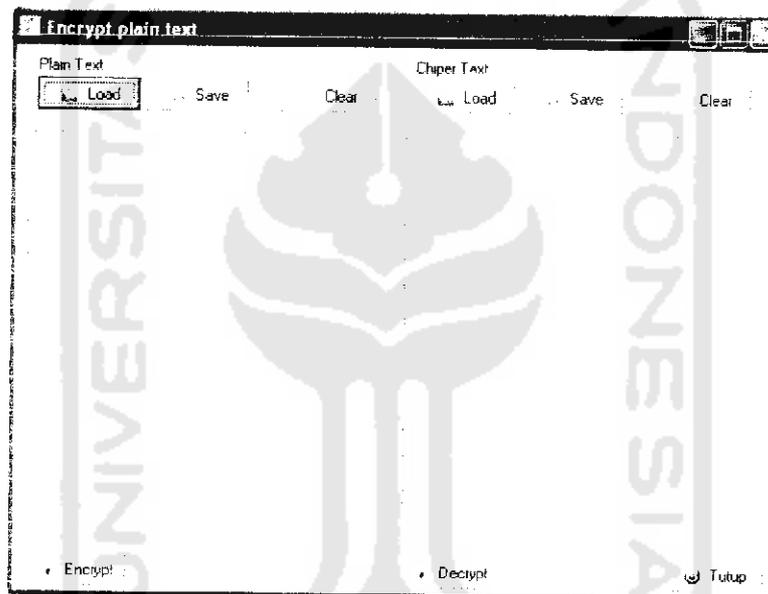
5.3.5 Interface Enkripsi dan Dekripsi Teks

Pada tampilan menu untuk enkripsi/dekripsi teks terdiri dari:

- Memo plain teks berfungsi untuk menampilkan teks yang akan dienkripsi dan teks hasil dekripsi.
- Memo cipher teks berfungsi untuk menampilkan teks hasil enkripsi.
- Tombol load berfungsi untuk mengambil file teks yang akan dienkrip atau didekrip, baik pada plain teks maupun cipher teks.

- Tombol save berfungsi untuk menyimpan teks yang telah ditampilkan pada memo baik untuk plain teks maupun cipher teks.
- Tombol tutup adalah untuk menutup form enkrip file.
- Tombol encrypt berfungsi untuk melakukan proses enkripsi
- Tombol decrypt berfungsi untuk melakukan proses dekripsi

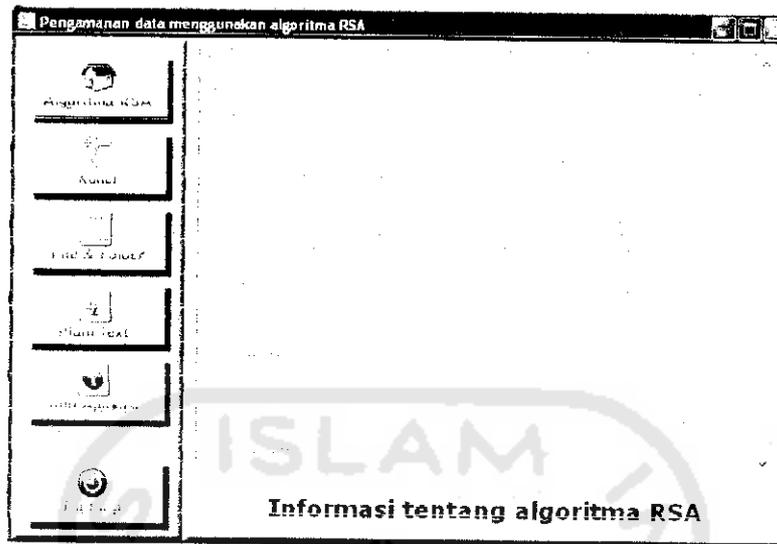
Tampilan menu enkripsi teks dapat dilihat pada gambar 5.6



Gambar 5.6. Antarmuka enkripsi teks

5.3.6 Interface Informasi Tentang Algoritma RSA

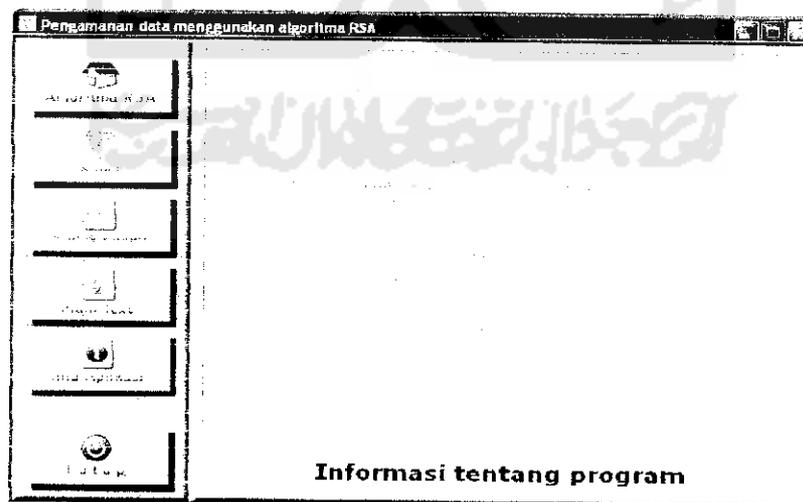
Tampilan menu informasi tentang algoritma RSA berisi penjelasan secara umum algoritma RSA dan cara perhitungan dalam pembuatan kunci, enkripsi dan dekripsi. Tampilan menu informasi tentang algoritma RSA dapat dilihat pada gambar 5.7.



Gambar 5.7. Antarmuka informasi tentang algoritma RSA

5.3.7 Interface Informasi Tentang Program

Tampilan menu informasi tentang program berisi profil dari program yaitu judul program dan profile pembuat. Tampilan menu informasi tentang program dapat dilihat pada gambar 5.8.



Gambar 5.8. Antarmuka informasi tentang program