BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi komputer yang sangat pesat membawa perubahan yang signifikan bagi kehidupan manusia. Dengan semakin berkembangnya teknologi komputer, semakin banyak aktivitas manusia yang sebelumnya harus dilakukan secara manual, sekarang dapat dilakukan dengan bantuan komputer sehingga dapat menghemat waktu terutama dalam melakukan pertukaran informasi. Namun, hal ini masih sangat membutuhkan sistem keamanan dalam pengirimannya sehingga tidak bisa digunakan oleh pihak lain yang tidak berhak yang bisa merugikan pemilik informasi baik secara material maupun immaterial. Salah satunya digunakan untuk tanda tangan dokumen elektronik yang lebih dikenal dengan nama *digital signature.*

Digital signature ini merupakan tanda tangan pada data digital berupa nilai kriptografis yang berfungsi untuk mengotensifikasi keaslian suatu dokumen digital. Autentifikasi penting untuk memastikan keaslian dokumen sehingga dapat diketahui apabila data masih terjaga keasliannya atau sudah disalahgunakan oleh pihak yang berwenang.

Namun, permasalahannya sekarang adalah proses verifikasi tanda tangan tersebut, dimana sering terjadi tanda tangan digital yang diverifikasi oleh pihak lain yang tidak berhak atau adanya penyangkalan dari pihak yang melakukan tanda tangan dengan tidak mau melakukan autentifikasi terhadap dokumen asli. Oleh karena itu diperlukan suatu sistem tanda tangan digital yang hanya dapat diverifikasi dengan persetujuan pihak penandatangan *(non-self authenticating).* Tanda tangan digital dengan sistem ini sering disebut dengan *undeniable signature scheme.*

Undeniable signature scheme ini dapat dirancang menggunakan algoritma *Chaum's Blind Siganture,* di mana algoritma ini menggunakan sebuah bilangan prima yang cukup besar sebagai parameter sekuriti dengan menggunakan kunci publik dan kunci privat. Verifikasi tanda tangan hanya dapat dilakukan oleh pemilik tanda tangan karena hanya pemilik tanda tangan yang mengetahui kunci privatnya, sehingga pihak yang menerima dokumen tidak menunjukkan keaslian dokumen kepada pihak ketiga tanpa melibatkan si pemilik tanda tangan. Hal ini digunakan untuk mengantisipasi kemungkinan terjadinya penyalahgunaan dokumen oleh penerima, sehingga ada tuntutan dari pihak lain yang merasa dirugikan dengan isi dokumen tersebut, namun tidak bisa melibatkan pihak penanda tangan dokumen tersebut.

Berdasarkan uraian di atas, maka penulis tertarik untuk menuangkannya dalan tugas akhir yang berjudul "**Perancangan Aplikasi Dokumen Undeniable Digital Signature Dengan Algoritma Chaum's Blind Signature".**

1.2 Rumusan Masalah

Perumusan masalah dalam penulisan tugas akhir ini adalah :

a. Bagaimana proses kerja *Undeniable digital signature* dalam melakukan verifikasi terhadap suatu dokumen elektronik dengan algoritma *Chaum's Blind Signature.*
b. Bagaimana cara merancang dan membuat aplikasi kriptografi *Undeniable digital signature* dengan algoritma *Chaum's Blind Signature*.
c. Apa kelebihan dan kekurangan kriptografi *Undeniable digital signature* dengan algoritma *Chaum's Blind Signature*.

1.3 Batasan Masalah

Batasan masalah dalam penulisan tugas akhir ini adalah sebagai berikut :

a. Algoritma yang digunakan adalah *Chaum's Blind Siganture.*
b. Panjang bit tanda tangan digital yang digunakan adalah 16 bit.
c. Verifikasi tanda tangan yang digunakan adalah satu arah.
d. Bahasa pemrograman yang digunakan adalah *Microsoft Visual Basic 6.0*

1.4 Tujuan Penelitian

Adapun tujuan dari penulisan tugas akhir ini adalah :

a. Mengetahui proses kerja *undeniable digital signature* dalam melakukan verifikasi terhadap suatu dokumen elektronik dengan algoritma *Chaum's Blind Signature.*
b. Mengetahui cara merancang dan membuat aplikasi kriptografi *Undeniable digital signature* dengan algoritma *Chaum's Blind Signature*.
c. Mengetahui kelebihan dan kekurangan kriptografi *Undeniable digital signature* dengan algoritma *Chaum's Blind Signature*.

1.5 Manfaat Penelitian

Manfaat yang diambil dari penulisan tugas akhir ini adalah :

a. Menambah wawasan dan pengetahuan penulis dalam bidang analisa dan perancangan aplikasi dokumen *Undeniable digital signature* dengan algoritma *Chaum's Blind Signature.*
b. Membantu pengguna dalam menandatangani dokumen digital tanpa menunjukkan siapa yang melakukan autentifikasi atas keaslian dokumen tersebut, sehingga penyalahgunaannya tidak akan bisa melibatkan pihak yang memverifikasi.

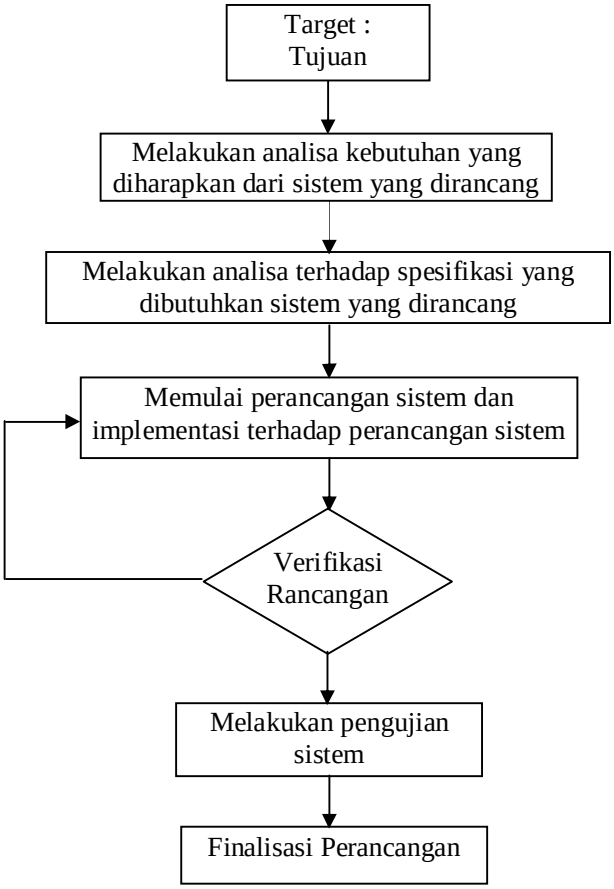
c. Sebagai referensi bagi pengguna yang ingin mengetahui mengenai cara kriptografi *Undeniable digital signature* dengan algoritma *Chaum's Blind Signature* pada dokumen elektronik.

1.6 Metodologi Penelitian

Dalam penulisan skripsi ini, penulis menggunakan metodologi penelitian yang terdiri dari :

a. Prosedur Perancangan

Adapun tata cara yang penulis lakukan dalam prosedur perancangan aplikasi dokumen *Undeniable digital signature* dengan algoritma *Chaum's Blind Signature* ini sebagaimana terlihat pada Gambar 1.1.



Gambar 1.1 Prosedur Perancangan

b. Analisa Kebutuhan

Adapun analisa yang penulis lakukan terhadap kebutuhan yang diharapkan dari sistem yang dirancang adalah sebagai berikut :

1. Sistem harus dapat digunakan untuk kriptografi *Undeniable digital signature* dengan algoritma *Chaum's Blind Signature*.
2. Sistem harus dapat menunjukkan kelebihan dan kekurangan kriptografi *Undeniable digital signature* dengan algoritma *Chaum's Blind Signature*.
3. Sistem harus dapat memberikan saran pengembangan kriptografi *Undeniable digital signature* dengan algoritma *Chaum's Blind Signature* berdasarkan perkembangan teknologi informasi.

c. Spesifikasi dan Desain

Adapun spesifikasi dari sistem yang dirancang ini adalah sebagai berikut :

1. Sistem membutuhkan sistem operasi *Windows XP* agar dapat berjalan dengan baik.
2. Sistem membutuhkan memori minimal 512 MB agar dapat berjalan dengan baik.
3. Sistem hanya dapat digunakan untuk kriptografi *Undeniable digital signature* dengan algoritma *Chaum's Blind Signature*.
4. Sistem membutuhkan dokumen dalam format teks agar *Undeniable digital signature* bisa dilaksanakan.

Sedangkan desain sistem yang penulis rancang agar pengguna dapat berinteraksi dengan perangkat lunak yang dirancang adalah sebagai berikut :

1. Form Signature

   Berfungsi sebagai form yang berisi menu-menu dan tombol-tombol yang dapat dipilih *user* untuk melakukan *Undeniable digital signature.*

2. Form Verifikasi

   Berfungsi sebagai form yang berisi menu-menu dan tombol-tombol yang dapat dipilih *user* untuk melakukan verifikasi untuk *Undeniable digital signature*.

3. Form About

   Berfungsi untuk menampilkan data penulis selaku perancang perangkat lunak.

d. Implementasi dan Verifikasi

Tahapan implementasi yang penulis lakukan terhadap perancangan aplikasi dokumen *Undeniable digital signature* dengan algoritma *Chaum's Blind Signature* ini adalah sebagai berikut :

1. Melakukan implementasi desain form

   Pada tahapan ini, penulis melakukan implementasi desain *form* dengan cara membuat *form-form* sesuai dengan desain yang dirancang pada bahasa pemrograman *Visual Basic 6.0*.

2. Melakukan *Coding Program*

   Pada tahapan ini, penulis menuliskan *coding-coding* yang dibutuhkan agar aplikasi kriptografi *Undeniable digital signature* dengan algoritma *Chaum's Blind Signature.*

3. Melakukan pengujian sistem

   Pada tahapan ini, penulis melakukan pengujian pada setiap form yang dihasilkan. Pengujian dilakukan untuk mengetahui apakah ada kesalahan (*error*) pada setiap form untuk melakukan perbaikan.

e. Validasi

Validasi sistem yang penulis lakukan adalah melakukan pengujian sistem secara keseluruhan. Validasi ini dilakukan agar sistem yang dirancang telah sesuai dengan kebutuhan awal, yaitu dapat digunakan untuk kriptografi *Undeniable digital signature* dengan algoritma *Chaum's Blind Signature* tersebut.

1.7 Sistematika Penulisan

Langkah-langkah atau tahapan-tahapan yang ditempuh dalam menyelesaikan penelitian ini adalah :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan tentang teori dasar yang berhubungan dengan program yang dirancang, serta bahasa pemograman yang digunakan.

BAB III : ANALISA DAN PERANCANGAN SISTEM

Pada bab ini mengemukakan tentang analisa masalah program yang akan dirancang dan perancangan program yang digunakan dalam penulisan tugas akhir ini.

BAB IV : IMPLEMENTASI SISTEM

Pada bab ini mengemukakan tentang hasil implementasi sistem yang dirancang mencakup uji coba sistem, tampilan, serta perangkat yang dibutuhkan, serta analisa sistem yang dirancang untuk mengetahui kelebihan dan kelemahan sistem yang dibuat.

BAB V : PENUTUP

Pada bab ini berisi kesimpulan penelitian dan saran dari peneliti sebagai perbaikan di masa yang akan datang.