BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan semakin luasnya penggunaan teknologi informasi diberbagai bidang, tingkat kejahatan digital juga semakin meningkat. Masalah Keamanan digital pun kini menjadi perhatian komunitas teknologi informasi.

Tanda tangan digital adalah serangkaian data string yang menghubungkan pesan dengan pemilik pesan yang asli, dengan menggunakan suatu teknik asimetrik kriptograpy. Tanda tangan digital dapat member sifat-sifat keamanan sebagai berikut :

1. Otentikasi, menjamin keaslian pengirim pesan
2. Akuntabilitas, pesan dengan tanda tangan digitaldapat dipertanggung jawabkan dan tidak dapat disangkal.
3. Tidak dapat dipalsukan.
4. Integritas, menjamin keaslian pesan yang dikirim.
5. Dapat di verifikasi secara independen, public dan pihak ketiga.

Selain itu juga perhitungan pembuatan tanda tangan digital harus mudah dihitung dan tanda tangan harus mudah disimpan.

Fakultas Sains dan Teknologi adalah salah satu fakultas pada perguruan tinggi Universitas Islam Negeri Sunan Gunung Djati Bandung. Yang mengelola data dan informasi yang berkaitan dengan akademik. Untuk menjaga keamanan data tersebut, maka perlu adanya aplikasi yang dapat mencegah pemalsuan tanda tangan atau identitas.

Berdasarkan uraian di atas, akan dilakukan penelitian dan penyusunan tugas akhir yang berjudul “Implementasi Tanda Tangan Digital Pada Transkrip Digital dengan Menggunakan Metode DSA”.

1.2 Identifikasi Masalah

Berdasarkan latar belakang di atas, terdapat beberapa masalah yang dapat diidentifikasi. Diantaranya adalah sebagai berikut :

1. Metode apa yang digunukan untuk membuat tanda tangan digital?
2. Bagaimana menentukan public key dan private key?
3. Bagaimana cara kerja metode DSA pada penggunaan tanda tangan digital?

1.3 Tujuan

Berdasarkan identifikasi masalah di atas, dapat disimpulkan bahwa penelitian ini bertujuan untuk:

1. Untuk otentikasi pada data digital (pesan, dokumen elektronik).
2. Dapat menentukan private key dan public key.
3. Dapat menentukan keabsahan tanda tangan digital.

1.4 Batasan Masalah

Untuk menghindari meluasnya permasalahan, maka permasalahan yang ditemukan selama penelitian ini dibatasi oleh hal-hal yang tercantum sebagai berikut :

1. Pada aplikasi ini format pesan yang dikirim berupa teks.
2. Algoritma yang digunakan untuk tanda tangan digital pada perancangan aplikasi ini adalah algoritma DSA (Digital Signature Algorithm).
3. E-dokumen adalah berupa data digital dengan format biner berupa file dengan ekstensi doc.
4. Pengamanan e-dokumen hanya meliputi : kerahasian meliputi deksripsi terhadap tandatangan digital, autentikasi pengirim dan integritas dan integritas e-dokumen sebagai hasil verifikasi pada pihak penerima.

1.5 Metologi Penelitian

Pada penelitian ini, menggunakan metode penelitian sebagai berikut :

1. Metode pengembangan perangkat lunak

   Dalam proses pengembangan perangkat lunak, metode yang digunakan adalah metode *prototype*. *Prototype* adalah salah satu pendekatan dalam rekayasa perangkat lunak yang secara langsung mendemonstrasikan bagaimana sebuah perangkat lunak atau komponen-komponen perangkat lunak akan bekerja dalam lingkungannya sebelum tahapan konstruksi aktual dilakukan(Howard, 1997).

   Prototype tersebut dievaluasi oleh pelanggan atau pemakai dan dipakai untuk menyaring kebutuhan pengembangan perangkat lunak. Iterasi terjadi pada saat disetel untuk memenuhi kebutuhan pelanggan dan pada saat yang sama memungkinkan pengembang untuk secara lebih baik memahami apa yang harus dilakukan. (Pressman, 2002).

   Tahapan-tahapan pada model *prototype* adalah sebagai berikut:

1) Pengumpulan dan identifikasi kebutuhan :

   Pada tahap ini pelanggan dan pengembang bersama-sama mendefinisikan format seluruh perangkat lunak, mengidentifikasikan semua kebutuhan, dan garis besar sistem yang akan dibuat.

2) Rancang bangun *prototyping* :

   Pada tahap ini dibangun *prototyping* dengan membuat perancangan sementara yang berfokus pada penyajian kepada pelanggan (misalnya dengan membuat input dan format output).

3) Uji *protoptyping* :

Tahap ini dilakukan untuk mengetahui apakah prototyping yang dibangun sudah sesuai dengan keinginan pelanggan atau belum. Jika sudah sesuai maka langkah 4 akan diambil. Jika tidak *prototyping* direvisi dengan mengulangi langkah 1,2,dan 3.

4) Mengkodekan sistem :

Pada tahap ini *prototyping* yang sudah disepakati diterjemahkan atau dikodekan ke dalam bahasa pemrograman yang sesuai.

5) Menguji sistem :

Setelah sistem sudah menjadi suatu perangkat lunak yang siap pakai, harus dites dahulu sebelum digunakan. Pengujian ini dilakukan dengan *White Box, Black Box*, *Basis Path*, pengujian arsitektur dan lain-lain.

6) Evaluasi Sistem :

Pelanggan mengevaluasi apakah sistem yang sudah jadi sudah sesuai dengan yang diharapkan . Jika ya, langkah 7 dilakukan; jika tidak, ulangi langkah 4 dan 5.

7) Penggunaan dan penerapan sistem akhir :

Perangkat lunak yang telah diuji dan diterima pelanggan siap untuk digunakan.

2. Metode pengumpulan data

Dalam penelitian ini, metode pengumpulan data yang dilakukan adalah sebagai berikut :

a) Wawancara

Teknik pengumpulan data dengan mengadakan tanya jawab secara langsung dan bimbingan dari pembimbing.

b) Studi literatur

Pengumpulan data dilakukan dengan cara mempelajari literatur tentang penulisan dan mengenai hal-hal yang mendukung program aplikasi serta mempelajari dari sumber data yang lain.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang, identifikasi masalah yang dihadapi, tujuan penelitian, batasan masalah yang dihadapi, metodologi penelitian, teknik pengumpulan data serta sistematika penulisan.

BAB II LANDASAN TEORI

Menjelaskan tentang teori-teori yang digunakan dalam tugas akhir ini serta untuk menjelaskan dan menyelesaikan permasalahan yang akan dikaji.

BAB III TINJAUAN UMUM INSTITUSI

Bab ini menjelaskan mengenai perusahaan/organisasi/institusi yang menjadi *study* kasus dalam penelitian sebagai bahan dari tugas akhir ini.

BAB IV ANALISIS DAN PERANCANGAN

Bab ini juga membahas tentang rancangan aplikasi yang akan dibangun.

BAB V IMPLEMENTASI DAN PENGUJIAN

Membahas proses implementasi dan pengujian perangkat lunak secara detil. Proses Implementasi meliputi Persiapan software dan hardware, installasi aplikasi, dan tampilan akhir aplikasi.sedangkan pengujian meliputi identifikasi software, rencana pengujian, kasus uji dan hasil uji, evaluasi pengujian.

BAB VI PENUTUP

Membahas tentang kesimpulan dan saran yang diperoleh dari penulisan tugas akhir ini.