BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Didirikan sejak tahun 1965, LEN (Lembaga Elektronika Nasional) kemudian bertransformasi menjadi sebuah Badan Usaha Milik Negara (BUMN) pada tahun 1991. Sejak saat itu, Len bukan lagi merupakan kepanjangan dari Lembaga Elektronika Nasional (LEN), tetapi telah menjadi sebuah entitas bisnis profesional dengan nama PT Len Industri. Saat ini Len berada di bawah koordinasi Kementrian Negara BUMN. Len telah mengembangkan bisnis dan produk-produk dalam bidang elektronika untuk industri dan prasarana, serta telah menunjukkan pengalaman dalam berbagai bidang yaitu bidang Broadcasting selama lebih dari 30 tahun dengan ratusan Pemancar TV dan Radio yang telah terpasang di berbagai wilayah di Indonesia. Jaringan infrastruktur telekomunikasi yang telah terentang baik di kota besar maupun daerah terpencil. Elektronika untuk pertahanan, baik darat, laut, maupun udara. Sistem Persinyalan Kereta Api di berbagai jalur kereta api di Pulau Jawa dan Sumatera. Sistem Elektronika Daya untuk kereta api listrik. Pembangkit Listrik Tenaga Surya.

Saat ini dokumen seperti sertifikat bppt dan dokumen tender bisa diunduh oleh semua unit kerja di lingkungan internal perusahaan melalui web internal perusahaan. Tapi yang menjadi kendala adalah legalisasi siapa yang mengeluarkan dokumen tersebut. Selain itu hanya unit kerja terkait yang boleh mengakses dan memiliki dokumen terutama dokumen yang bersifat rahasia seperti dokumen keuangan, dokumen hukum, desain produk, dokumen strategi marketing dan dokumen rahasia lainnya. Untuk mengatasi hal tersebut dilakukan pertukaran dokumen antar bagian unit kerja di PT Len Industri terutama dokumen yang terkait dengan unit kerja yang bersangkutan. Penyerahan dokumen terkait secara langsung antar unit kerja akan memakan waktu yang cukup lama mengingat jumlah unit kerja yang banyak, selain itu integritas (keutuhan) isi dokumen tidak terjamin.

Dokumen berbasis komputer dan didistribusikan menggunakan jaringan komputer disebut dengan dokumen digital atau dokumen elektronik (e-dokumen). Di PT Len Industri e-dokumen biasanya disebarkan melalui media jaringan di lingkungan internal perusahaan, sehingga aspek keamanannya harus dipertimbangkan. Penyebaran informasi melalui jaringan komputer rentan terhadap serangan. Informasi rahasia dapat diungkap atau dirubah oleh pihak yang tidak berwenang.

Pada beberapa kasus, yang diperlukan hanya otentikasi, tetapi kerahasiaan data tidak. Maksudnya, data tidak dienkripsi, sebab yang dibutuhkan hanya otentikasi saja. *Digital signature* merupakan mekanisme dalam kriptografi dimana pengirim e-dokumen dapat menandatangani secara elektronik sebuah e-dokumen dan penerima dapat memverifikasi tanda tangan tersebut untuk mengetahui keaslian pengirim. *Digital signature* hanya bisa menyelesaikan masalah otentikasi dan anti-penyangkalan tetapi tidak dapat menjamin kerahasiaan e-dokumen yang disebarkan melalui jaringan. Sementara e-dokumen yang terdapat di PT Len Industri sendiri dibagi dua yaitu, e-dokumen yang boleh diketahui oleh pihak internal perusahaan dan e-dokumen yang bersifat rahasia seperti dokumen keuangan, dokumen hukum, desain produk, dokumen strategi marketing dan dokumen rahasia lainya. Untuk menghindari terjadinya pengungkapan isi e-dokumen oleh pihak yang tidak berwenang, penggunaan *digital signature* saja tidak cukup maka diperlukan mekanisme lain untuk menjamin kerahasiaan e-dokumen yaitu dengan teknik enkripsi. enkripsi merupakan mekanisme penyandian/ pengacakan isi e-dokumen dari e-dokumen yang memiliki informasi penting menjadi e-dokumen yang tidak memiliki informasi apa-apa.

Sistem yang akan dibangun adalah aplikasi *digital signauture* dan enkripsi. Dengan penggabungan *digital signauture* dan enkripsi ini diharapkan dapat menutupi kelemahan-kelemahan baik dari segi *digital signauture* dan enkripsi. Sehingga e-dokumen yang disebarkan dilingkungan PT Len Industri dapat menjamin otentikasi, anti-penyangkalan dan kerahasian e-dokumen.

1.2 Rumusan Masalah

Berdasarkan uraian di latar belakang, maka rumusan masalahnya adalah bagaimana membangun Aplikasi *Digital Signature* dan Enkripsi Untuk Keamanan E-dokumen di PT Len Industri.

1.3 Maksud dan Tujuan

Berdasarkan permasalahan yang diteliti, maka maksud dari penulisan tugas akhir ini.

1.3.1 Maksud

Maksud dari penulisan tugas akhir ini adalah untuk membangun Aplikasi *Digital signature* dan enkripsi untuk keamanan e-dokumen di PT Len Industri.

1.3.2 Tujuan

Tujuan yang akan dicapai dalam penelitian ini adalah :

1. Mempermudah masing-masing unit kerja di PT Len Industri untuk mengetahui legalisasi (otentikasi/ keaslian) pengirim e-dokumen yang dikirimkan melalui jaringan memang benar berasal dari unit kerja yang terkait dengan dokumen tersebut.
2. Membantu menjamin kerahasian e-dokumen yang bersifat rahasia seperti dokumen keuangan, dokumen hukum, dokumen tender dan alur pertukarannya hanya dikalangan tertentu misalnya hanya diantara dua unit kerja.

1.4 Batasan Masalah

Batasan masalah pada penelitian ini yaitu :

1. Masukan dari aplikasi ini adalah e-dokumen dalam bentuk extensi .pdf, .doc, .xls, .xlsx.
2. Panjang kunci yang digunakan 160 bit.
3. Aplikasi ini menyediakan fitur yaitu halaman utama, kirim pesan, pesan masuk, pesan keluar, kontak (alamat), *generate* (pembuatan) kunci.
4. Ruang lingkup pertukaran e-dokumen ini hanya pada jaringan lokal (LAN) PT Len Industri (Persero). Berikut penjelasan pemetaan jaringan komputer PT Len Industri:

a. Terdapat sepuluh gedung pada komplek bangunan PT Len Industri, terdiri dari Gedung A (gedung utama tempat semua kegiatan korporasi). Gedung B, P, Q,

E, U, Gedung C (merupakan gedung anak perusahaan yaitu SEI dan Eltran), Gedung D (merupakan kantor dari bagian SDM), Gedung T merupakan gedung anak perusahaan LRS.

b. Topologi jaringan yang digunakan yaitu topologi *tree.*

c. Sistem jaringan yang sekarang berjalan pengelompokan jaringan bukan berdasarkan per bagian unit kerja. Jadi dalam satu jaringan LAN bisa saja terdapat lebih dari satu bagian unit kerja.

5. Algoritma *digital signature* yang digunakan yaitu ECDSA (*Eliptik Curve Digital Signature Algorithm*).
6. Algoritma enkripsi yang digunakan pada aplikasi ini yaitu ElGamal berbasis kurva eliptik.
7. Aplikasi berbasis *Client-Server*.
8. Permodelan sistem yang digunakan adalah permodelan berorientasi objek.
9. Bahasa pemrograman yang digunakan dalam pembuatan aplikasi ini adalah bahasa pemrograman *Java*.
10. Perangkat lunak yang digunakan untuk membuat aplikasi ini yaitu Netbeans IDE 7.1.

1.5 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut :

1. Tahap Pengumpulan Data

Tahap pengumpulan data yang digunakan dalam penelitian ini adalah sebagai berikut :

a. Studi Literatur.

Pengumpulan data dengan cara mengumpulkan literatur, jurnal, *paper* dan bacaan-bacaan mengenai kriptografi dan *digital signature* yang ada kaitannya dengan topik penelitian.

b. Observasi.

Teknik pengumpulan data dengan mengadakan penelitian dan tinjauan langsung ke PT Len Industri untuk mengumpulkan data dari beberapa bagian diantaranya bagian umun Sisfo (bagian khusus yang mengatur dan memelihara

jaringan komputer perusahaan dan sebagian anak perusahaan) dan menentukan berbagai hal yang menjadi masalah di dalamnya.

c. Interview.

Teknik pengumpulan data dengan tanya jawab secara langsung dengan beberapa bagian diantaranya bagian umum Sisfo dan bagian Hukum di PT Len Industri yang ada kaitannya dengan judul penelitian.

2. Metode Pembangunan Perangkat Lunak

Tahap yang digunakan dalam pembangunan perangkat lunak ini menggunakan pendekatan model *waterfall*, model ini melingkupi aktivitas-aktivitas dibawah ini:

a. Communication

Tahap *communication* merupakan analisis terhadap kebutuhan aplikasi, dan tahap pengumpulan data dengan melakukan pertemuan dengan *user* di PT Len Industri, maupun mengumpulkan data-data tambahan baik yang terdapat pada jurnal ilmiah, artikel, buku, dan referensi lainnya.

b. Planning

Tahap *planning* merupakan lanjutan dari tahap *communication.* Tahapan ini akan menghasilkan dokumen *user requirement* atau bisa dikatakan sebagai data yang berhubungan dengan keinginan *user* dalam pembuatan aplikasi dan rencana yang akan dilakukan.

c. Modelling

Proses *modelling* ini akan menerjemahkan syarat kebutuhan ke dalam sebuah perancangan aplikasi yang dapat diperkirakan sebelum dibuat pengkodean (*coding*). Proses ini berfokus pada arsitektur aplikasi, tampilan antarmuka, dan detil algoritma yang digunakan. Tahapan ini akan menghasilkan dokumen yang disebut *software requirment*

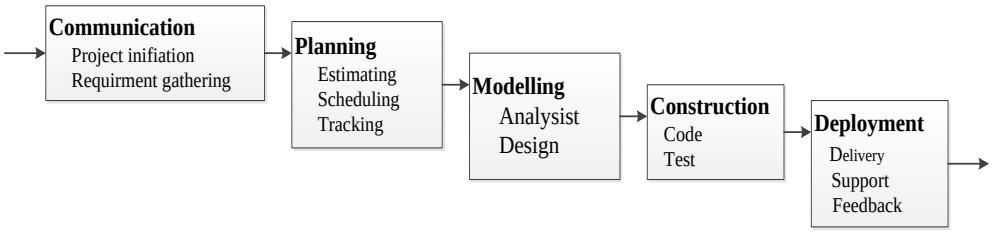
d. Construction

Construction merupakan proses pengkodean. Pengkodean merupakan penterjemahan desain kedalam bahasa yang bisa dimengerti oleh komputer. Setelah tahap pengkodean telah selesai maka akan dilakukan proses *testing* adalah

menemukan kesalahan-kesalahan pada sistem untuk kemudian bisa ditentukan perbaikannya.

e. Deployment

Tahapan ini merupakan tahap akhir dalam pembangunan sebuah aplikasi atau sistem. Setelah melakukan analisis, desain, dan pengkodean maka sistem yang sudah dibuat bisa digunakan oleh *user*. Kemudian setelah aplikasi jadi harus dilakukan pemeliharaan.



Gambar 1.1 Model Waterfall [1]

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Menguraikan tentang latar belakang masalah, rumusan masalah, maksud dan tujuan penelitian, batasan masalah, metodologi penelitian dan sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Bab ini membahas tentang tinjauan instansi seperti profil instansi, visi dan misi, struktur organisasi serta teori-teori pendukung yang menunjang dalam perancangan dan pembangunan apaliaksi *digital signature* dan enkripsi untuk keamanan e-dokumen.

BAB III. ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi analisis pada sistem yang sedang berjalan di PT Len Industri yang sedang di teliti, analisis kebutuhan non fungsional dan analisis kebutuhan

fungsional dalam pembangunan sistem serta perancangan sistem yang dikembangkan.

BAB IV. IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini berisi implementasi sistem yang dibangun, spesifikasi perangkat lunak dan perangkat keras, ujicoba program dan hasil pengujian.

BAB V. KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang diperoleh dari hasil pengujian sistem, serta saran perbaikan dan pengembangan sistem ke depan.