BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Internet merupakan salah satu media untuk bertukar informasi atau berkomunikasi. Hampir semua orang menggunakan internet karena sudah menjadi kebutuhan utama dalam kehidupan mereka sehari-hari, baik untuk keperluan pendidikan, bisnis, hiburan, dan lain-lain. Namun, seiring dengan pesatnya perkembangan internet, masalah keamanan juga semakin kompleks.

Ketika saling berkomunikasi tidak menutup kemungkinan untuk mengirim informasi yang berbentuk file berjenis text, suara, gambar, dan video atau yang disebut juga dokumen elektronik (e-dokumen). E-dokumen atau dokumen elektronik adalah informasi yang direkam atau disimpan dengan cara yang memerlukan perangkat komputer atau perangkat elektronik lain untuk menampilkan, menafsirkan atau memprosesnya. Berbeda dengan dokumen kertas, dokumen elektronik/*digital* memiliki kelebihan dalam hal duplikasi atau regenerasi. Data digital dapat diduplikasi seperti aslinya tanpa mengurangi kualitas data asilnya. Hal ini sulit dilakukan dalam teknologi analog, dimana kualitas data asli lebih baik dari duplikatnya, sehingga seseorang dengan mudah dapat memverifikasi keaslian sebuah dokumen. Tetepi e-dokumen memiliki kelemahan yaitu sangat mudah untuk diduplikasikan sehingga tidak diketahui lagi data mana yang asli. E-dokumen sebagai alat bukti dikhawatirkan dapat dipalsukan dan nantinya akan muncul masalah tentang keaslian dokumen elektronik tersebut.

Salah satu masalah keamanan tersebut adalah pencurian dan pemalsuan data. Data yang dikirim lewat internet dapat diambil dan diubah oleh orang yang tidak bertanggung jawab. Salah satu cara untuk mencegahnya adalah dengan membuat suatu tanda khusus yang memastikan bahwa data tersebut adalah data yang benar/*valid*.

Tanda tangan merupakan salah satu bukti untuk membenarkan atau mengesahkan suatu dokumen, dikarenakan keaslian dokumen yang memiliki

tanda tangan menjadi aset yang sangat berharga baik dari suatu organisasi, perusahaan, pemerintah maupun pribadi. Hal ini menyebabkan keaslian (*autentifikasi)* tanda tangan menjadi sangat penting untuk dilindungi dari orang-orang yang tidak bertanggung jawab yang akan memanipulasi tanda tangan untuk kepentingannya yang dapat merugikan orang lain.

Untuk itu dapat digunakan salah satu teknologi keamanan jaringan yang disebut tanda tangan digital atau *digital signature*. Salah satu algoritma kriptografi untuk membuat *digital signature* adalah algoritma RSA.

Penggabungan metode RSA dengan tanda tangan manual untuk pengamanan e-dokumen dapat dilakukan karena tanda tangan manual disini berfungsi untuk membangkitkan parameter dan sepasang kunci secara dinamis.

1.2 Identifikasi Masalah

Berdasarkan uraian pada latar belakang, permasalahan yang diteliti yaitu bagaimana membangun aplikasi untuk keamanan e-dokumen dengan penggabungan metode RSA dan tanda tangan manual sebagai solusi dalam hal manajemen kunci dengan pembangkitan sepasang kunci secara dinamis.

1.3 Maksud dan Tujuan

Berdasarkan latar belakang permasalahan yang diteliti, maka maksud dari penulisan skripsi ini adalah untuk membangun aplikasi kriptografi *digital signature* untuk pengamanan e-dokumen dengan penggabungan metode RSA dan tanda tangan manual.

Tujuan yang akan dicapai dalam penelitian ini adalah membuktikan bahwa:

1. Kerahasiaan pesan (*confidentiality/secrecy*), untuk menjaga isi pesan dari siapapun yang tidak berhak untuk membacanya.
2. Keaslian (*autentifikasi*), Mengetahui kebenaran sumber pesan yang diterima bahwa pesan tersebut asli dari pengirim yang benar.
3. Keutuhan pesan (*data integrity*), menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman.

4. Anti-penyangkalan (*non-repudiation*), mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

1.4 Batasan Masalah

Untuk mempermudah dalam melakukan perancangan pembangunan aplikasi ini diperlukan suatu pembatasan dari masalah-masalah yang ada, sehingga dapat diketahui ruang lingkup dari aplikasi yang akan di rancang. Batasan tersebut seperti dijabarkan di bawah ini:

1. Memerlukan tanda tangan manual atau disebut juga tanda tangan *offline*.
2. Tanda tangan manual discan terlebih dahulu.
3. Scan tandatangan manual dalam file dengan ekstensi JPG, JPEG, PNG & GIF.
4. Keaslian tanda tangan manual seseorang merupakan tanggung jawab seorang staf atau suatu unit yang diberi kepercayaan pada suatu lembaga.

1.5 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan skripsi ini adalah sebagai berikut:

1.5.1 Metode Pengumpulan Data

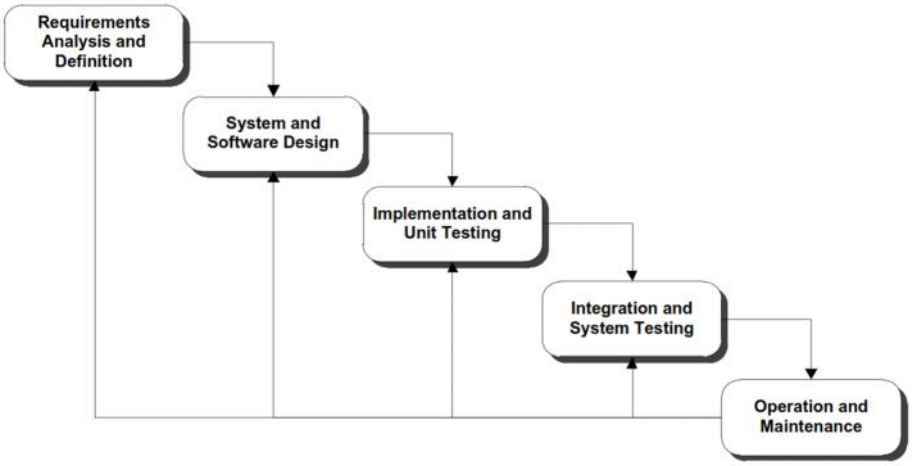
a. Studi Literatur

Metode pengumpulan data yang digunakan dalam penelitian ini adalah studi pustaka yang merupakan pengumpulan data dengan cara mengumpulkan literatur-literatur dari perpustakaan yang bersumber dari buku-buku, jurnal ilmiah, situs-situs di internet, paper dan bacaan-bacaan yang ada kaitannya dengan judul penelitian dan mendukung hasil penelitian. Hasil dari studi pustaka yang dipelajari berupa teori dan perkembangan terkini mengenai kriptosistem *digital signature* dan teori pendukung lainnya mengenai kriptografi pada dokumen digital, Algoritma RSA (Rivest, Shamir, Adleman).

1.5.2 Metode Pembangunan Perangkat Lunak

Metode analisis data dalam pembuatan perangkat lunak menggunakan meode *waterfall*. Metode *waterfall* adalah sebuah metode pengembangan software yang bersifat sekuensial dan terdiri dari 5 tahap yang saling terkait dan mempengaruhi yang meliputi beberapa proses berikut:

Berikut ini akan dijelaskan mengenai tahap-tahap pembangunan sistem dengan menggunakan metode *waterfall*.



Gambar 1.1 Metode Waterfall (Pressman)

Keterkaitan dan pengaruh antar tahap ini ada karena output sebuah tahap dalam *Waterfall* Model merupakan input bagi tahap berikutnya, dengan demikian ketidaksempurnaan hasil pelaksanaan tahap sebelumnya adalah awal ketidaksempurnaan tahap berikutnya. Memperhatikan karakteristik ini, sangat penting untuk melakukan analisa kebutuhan dan desain sistem sesempurna mungkin sebelum masuk ke dalam tahap-tahap berikutnya. Berikut adalah penjelasan detail dari masing-masing tahap dalam *waterfall* model, yaitu:

a. *Requirements analysis and definition*

   Tahap ini merupakan bagian dari kegiatan sistem yang terbesar dalam pengerjaan suatu proyek. Pada tahap ini merupakan tahap pertama yang menjadi dasar proses pembuatan perangkat lunak dilakukan analisa

terhadap permasalahan dan menetapkan berbagai kebutuhan yang diperlukan dalam pembangunan atau pengembangan suatu perangkat lunak. Kelancaran proses pembuatan perangkat lunak secara keseluruhan dan kelengkapan fitur perangkat lunak yang dihasilkan sangat tergantung pada hasil analisa kebutuhan ini. Untuk memperoleh informasi tentang proses bisnis dan kebutuhan perusahaan, umumnya dilakukan wawancara, diskusi dan survey. Beberapa cara untuk membantu memperlancar penyelesaian tahap ini dengan terlebih dahulu menyusun *scope of work software* yang akan dibuat sebagai acuan kerja. Hasil analisa kebutuhan yang tidak lengkap berpotensi menyebabkan beberapa permasalahan yang tidak diharapkan, antara lain : waktu pembuatan perangkat lunak menjadi lebih lama, proses dalam perangkat lunak tidak sesuai dengan proses bisnis dan perangkat lunak tidak dapat memenuhi semua analisa kebutuhan.

b. *System and software design*

   Tahap menerjemahkan kebutuhan-kebutuhan yang dianalisis ke dalam bentuk yang mudah dimengerti. Sehingga didapat jelas fungsi dan kebutuhan yang diinginkan dari pembangunan atau pengembangan perangkat lunak tersebut. Langkah selanjutnya yang dilakukan adalah merancang tampilan perangkat lunak agar mudah dimengerti oleh pengguna sesuai dengan fungsi dan kebutuhan perangkat lunak tersebut. Ini merupakan tahap penyusunan proses, data, aliran proses dan hubungan antar data yang paling optimal untuk menjalankan proses bisnis.

c. *Implementation and unit testing*

   Tahap penerjemahan data atau pemecahan masalah yang telah dirancang kedalam suatu bahasa pemrograman tertentu. Ini merupakan tahap penerjemahan desain sistem yang telah dibuat ke dalam bentuk perintah-perintah yang dimengerti komputer dengan mempergunakan bahasa pemrograman, *middleware* dan *database* tertentu yang menghasilkan sebuah lunak yang sesuai dengan kebutuhan pengguna. Setiap fungsional

yang ada pada perangkat lunak tersebut dilakukan uji kelayakan, sehingga perangkat lunak tersebut dapat berjalan dengan baik.

d. Integration and System Testing

Pada tahap ini, dilakukan penyempurnaan terhadap perangkat lunak secara keseluruhan agar dapat berjalan sesuai dengan kebutuhan. Pengujian perangkat lunak terhadap data nyata perlu dilakukan untuk memastikan kelayakan dari perangkat lunak tersebut.

e. Operation and Maintenance

Tahap akhir dimana suatu perangkat lunak yang sudah selesai dapat dioperasikan langsung oleh pengguna. Tahap maintenance perlu dilakukan untuk disesuaikan apabila ada perubahan sesuai dengan permintaan pengguna.

1.6 Sistematika Penulisan

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

BAB 1 PENDAHULUAN

Bab ini akan menguraikan tentang latar belakang permasalahan, merumuskan inti permasalahan yang dihadapi, menentukan maksud dan tujuan skripsi, batasan masalah, metodologi penelitian yang digunakan serta sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab ini membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik skripsi yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan.

BAB 3 ANALISIS MASALAH DAN PERANCANGAN SISTEM

Bab ini membahas mengenai sub-sub sistem yang diuraikan dari system utama dengan tujuan untuk mengetahui dan mengefektifkan cara kerja dan interaksi dari tiap sub system dalam fungsinya untuk mencapai tujuan system utama. Didalamnya terdapat analisis terhadap proses pembentukan sepasang

kunci, proses pembangkitan *Digital signature*, proses verifikasi *Digital signature*, proses embedding dan proses ekstrakting. Selain itu terdapat juga kebutuhan fungsional dan non-fungsional dari sistem, perancangan antarmuka untuk aplikasi yang akan dibangun sesuai dengan hasil analisis yang telah dibuat.

BAB 4 PENGUJIAN DAN IMPLEMENTASI SISTEM

Bab ini membahas tentang penerapan dari rancangan perangkat lunak sebelumnya ke dalam bahasa pemrograman tertentu dan pengujian terhadap perangkat lunak apakah telah benar dan sesuai seperti yang diharapkan.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi tentang kebenaran hipotesis yang diajukan pada batasan masalah berdasarkan hasil penelitian yang telah dilakukan dan masukan-masukan yang dapat digunakan untuk pengembangan perangkat lunak selanjutnya.