BAB I
PENDAHULUAN

I.1 Latar Belakang

Tandatangan *digital* adalah suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan/ *signer* (Munir, 2005). Namun algoritma kriptografi untuk membuat tandatangan *digital* misalnya DSA (*Digital Signature Algorithm*), RSA (Rivest, Shamir, Adleman) atau ECDSA (*Elliptic Curve Digital Signature Algorithm*) hanya menghasilkan satu tandatangan *digital* untuk satu e-dokumen. Hal ini tidak sesuai dengan konsep tandatangan *digital* yang bergantung pada pengirim/ *signer* dimana *signer* lebih dari satu. Sehingga diperlukan konsep baru mengenai tandatangan *digital* yang dapat berfungsi sebagai otorisasi suatu e-dokumen sama halnya otorisasi tandatangan (*handwritten)* beberapa *signer* pada dokumen fisik. Salah satu metode yang dapat memenuhi kebutuhan tandatangan *digital* oleh lebih dari satu *signer* adalah dengan biometrik tanda tangan *manual/ offline.* Tandatangan *offline* adalah tandatangan pada dokumen fisik yang didigitasi oleh *scanner* (Najmul, 2006).

DSA (*Digital Signature Algorithm)* merupakan salah satu kriptografi kunci publik yang digunakan untuk otentikasi, pengamanan data dan perangkat anti sangkal. Kunci privat digunakan untuk jangka waktu tertentu dan dapat diperpanjang selama pembangkitan tandatangan *digital* menggunakan kunci privat tersebut. Demikian juga berlaku untuk kunci publik yang dapat digunakan terus-menerus selama pasangannya yaitu kunci privat digunakan untuk membangkitkan tandatangan *digital.* Demikian juga parameter DSA dapat digunakan bersama pada sekelompok pengguna dan bersifat publik. Parameter DSA bernilai tertentu (tetap) dan dapat tetap dipakai atau diperpanjang untuk beberapa periode waktu. Algoritma DSA dirancang untuk menjaga dari lawan *(attacker)* yang diasumsikan tidak tahu kunci privat *signer* yang digunakan untuk membangkitkan tandatangan *digital.* Menurut peneliti, penggunaan parameter, kunci publik dan privat yang tetap untuk suatu waktu tertentu dan diperpanjang untuk

periode waktu tertentu, merupakan celah ketidakamanan penggunaan algoritma DSA, karena pihak *attacker* mempunyai kesempatan dan waktu seiring dengan kecepatan *processor* yang semakin bertambah. Pihak *attacker* dapat memecahkan kunci privat sebagai pasangan kunci publik yang digunakan untuk membuat tandatangan *digital*. Jika hal ini terjadi maka *attacker* dapat menyamar sebagai *signer* sah (pemegang kunci privat) dan mengubah e-dokumen yang sah sekaligus membuat tandatangan *digital*-nya untuk dikirimkan pada pihak *verifier*. Pada proses verifikasi di pihak *verifier*, akan didapat hasil verifikasi "valid" karena hasil dekripsi tandatangan *digital* sama dengan nilai *massage hash* e-dokumen walaupun berasal dari *attacker*. Sehingga fungsi tandatangan *digital* sebagai otentifikasi e-dokumen dan *signer* sah menjadi tidak berguna. Solusi dari masalah ini yaitu dengan menggunakan parameter, kunci publik dan kunci privat yang dinamis yaitu bernilai berbeda untuk tiap proses pembuatan tandatangan *digital*. Jadi sangat perlu bahwa setiap kunci diubah jauh sebelum ia dapat ditemukan dengan cara *exhaustive search* (Munir, 2006). Sehingga perlu dibangun aplikasi kriptografi dengan metode DSA (*Digital Signature Algorithm*) yang dapat membangkitkan kunci secara dinamis walaupun dengan masukan yang sama. Tandatangan dapat digunakan dalam proses menurunkan kunci privat untuk menandatangani e-dokumen. Kunci privat dibangkitkan secara dinamis dari salah satu sampel tandatangan. Pembangkitan dinamis kunci privat membuktikan kemudahan penandatanganan e-dokumen sebagaimana dapat menandatangani e-dokumen kapanpun dimanapun tanpa membawa *disk* atau *smart card*.

I.2 Perumusan Masalah

Berdasarkan uraian pada latar belakang, permasalahan yang diteliti yaitu bagaimana menerapkan aplikasi untuk keamanan e-dokumen dengan metode penggabungan tandatangan manual dan DSA (*Digital Signature Algorithm*) pada NISSIN ELECTRIC CO., LTD., sebagai solusi dalam hal manajemen kunci dengan pembangkitan sepasang kunci secara dinamis walaupun dengan masukan yang sama dan memenuhi.

I.3 Batasan Masalah

Batasan masalah pada penelitian ini yaitu:

a. Dokumen fisik ditandatangani secara manual dan digitasi dengan scanner.
b. Fungsi Hash yang digunakan adalah SHA-1.
c. E-berkas adalah data *digital* atau *message* dengan format biner berupa file dengan ekstensi Pdf, docx, pptx, xlsx, txt, jpeg, png, gif, mp3, exe.
d. Pengamanan e-dokumen hanya meliputi: kerahasiaan yaitu dekripsi terhadap tandatangan *digital*, autentikasi *signer* dan integritas e-dokumen sebagai hasil verifikasi pada pihak *verifier*.
e. Tidak membahas aspek keamanan pada jalur komunikasi yaitu pada proses transmisi e-dokumen lewat internet via *email*.

I.4 Tujuan Penelitian

Tujuan yang dicapai dalam penelitian ini adalah menerapkan aplikasi kriptografi untuk pengamanan e-berkas dengan metode penggabungan tandatangan manual dan DSA (*Digital Signature Algorithm)* sehingga menjadi solusi dalam hal manajemen kunci dengan pembangkitan parameter dan sepasang kunci secara dinamis walaupun dengan masukan yang sama dan memenuhi kebutuhan ketidaktunggalan *signer*. Pengamanan e-dokumen dijamin dengan hasil proses verifikasi.

I.5 Manfaat Penelitian

Sistem yang dibangun menggunakan biometrik tandatangan yang dikombinasikan dengan keuntungan dari penggunaan kriptografi kunci public DSA yaitu integritas dan kepercayaan yang bermanfaat untuk menjaga keotentikan isi e-dokumen dan kepercayaan pada pihak penandatangan/ *signer* yang sebenarnya.

I.6 Sistematika Penulisan

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

BAB I PENDAHULUAN

Bab I Menguraikan tentang latar belakang permasalahan, mencoba merumuskan inti permasalahan yang dihadapi, menentukan tujuan dan kegunaan penelitian, yang kemudian diikuti dengan pembatasan masalah, asumsi, serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab II Membahas berbagai konsep dasar atau teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan serta tinjauan terhadap penelitian-penelitian serupa yang telah dilakukan sebelumnya termasuk sintesisnya.

BAB III METODOLOGI PENELITIAN

Bab III membahas analisis kebutuhan sistem meliputi kebutuhan perangkat lunak, kebutuhan perangkat keras, serta tahap perancangan sistem.

BAB IV PERANCANGAN DAN IMPLEMENTASI SISTEM

Bab IV membahas tahapan pada saat sistem tersebut akan implementasi atau setelah tahapan perancangan selesai. Bab ini juga mendefinisikan kebutuhan implementasi serta melakukan ujicoba pada sistem yang telah dibangun.

BAB V KESIMPULAN DAN SARAN

Bab V Berisi kesimpulan yang diperoleh dari hasil implementasi dan ujicoba sistem serta saran-saran guna pengembangan sistem/ aplikasi ini di masa yang akan datang.

DAFTAR PUSTAKA

DAFTAR RIWAYAT HIDUP

LAMPIRAN