OTENTIFIKASI DOKUMEN ELEKTRONIK DENGAN MENGGUNAKAN ALGORITMA *DSA*

SKRIPSI SARJANA MATEMATIKA

ERMANELY
05134043

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS ANDALAS
PADANG
2009

ABSTRAK

Pada saat melakukan proses pemindahan data melalui internet diperlukan suatu jaminan bahwa informasi tersebut tetap terjaga keasliannya dan keutuhannya. Semua persoalan ini dapat diatasi dengan menggunakan tanda tangan digital. *Digital Signature Standard (DSS)* merupakan sebuah bakuan untuk tanda tangan digital yang diresmikan pada tahun 1991 oleh NIST (*The National Institute of Standard and Technology*). *DSS* terdiri atas 2 komponen yaitu: algoritma tanda tangan digital yang disebut *Digital Signature Algorithm* (*DSA*) dan *Fungsi Hash Standard* yang disebut *Secure Hash Algorithm* (*SHA*). *DSA* memiliki dua fungsi utama yaitu pembentukan tanda tangan dan pemeriksaan keabsahan tanda tangan (verifikasi). *DSA* menggunakan dua buah kunci yaitu kunci publik dan kunci rahasia (*private*). Prosedur pembentukan tanda tangan menggunakan kunci rahasia pengirim sedangkan prosedur pemeriksaan tanda tangan menggunakan kunci publik pengirim. Disamping itu, *DSA* juga menggunakan fungsi *hash* satu arah *SHA*-1 untuk mengubah pesan menjadi *message digest* yang berukuran 160 bit.

Kata kunci : *Tanda Tangan Digital, Digital Signature Standard (DSS), Digital Signature Algorithm (DSA), Fungsi hash satu arah SHA-1*

BAB I

PENDAHULUAN

1.1 Latar Belakang

Semakin tingginya perkembangan teknologi informasi dan telekomunikasi dewasa ini, telah mengakibatkan semakin beragamnya pula fasilitas telekomunikasi yang ada. Komputer sebagai alat bantu manusia dengan didukung perkembangan teknologi informasi telah membantu akses ke dalam jaringan internet dalam melakukan pemindahan data dan informasi.

Keamanan informasi *(information security)* merupakan bagian yang sangat penting dari sebuah sistem dalam jaringan komputer terutama yang terhubung dengan internet. Kriptografi sebagai ilmu dan seni untuk menjaga keamanan pesan merupakan salah satu dasar dalam memahami keamanan pada komputer, khususnya jaringan. Ketika saling berkomunikasi dengan pihak lain melalui suatu jaringan seperti internet tidak menutup kemungkinan ada salah satu pihak yang sedang berkomunikasi melakukan penyangkalan dan juga tidak menutup kemungkinan adanya pihak yang tidak berhak melakukan perubahan terhadap pesan sehingga mengakibatkan kesalahpahaman yang berakhir pertengkaran. Permasalahan ini menunjukkan bahwa perlu adanya proses legalisasi digital. Proses legalisasi ini dapat diterapkan dengan menggunakan tanda tangan digital *(digital signature)*.

Sistem kriptografi yang cocok digunakan untuk tanda tangan digital adalah sistem kriptografi kunci publik. Hal ini disebabkan karena sistem kriptografi kunci publik mempunyai tingkat keamanan yang sebanding dengan panjang kunci yang

dipakai. Panjang kunci ini biasanya dihitung dalam bit. Semakin panjang kunci yang dipakai semakin tinggi tingkat keamanannya. Ada tiga algoritma yang digunakan dalam aplikasi tanda tangan digital yaitu: *Rivest Shamir Adleman (RSA), Digital Signature Algorithm (DSA),* dan *ElGamal.* Karena *DSA* merupakan algoritma yang dikhususkan untuk pembuatan tanda tangan digital dan merupakan bakuan (Standard) untuk *Digital Signature Standard* (*DSS*) maka penulis memutuskan untuk membahas algoritma *DSA* dalam otentifikasi dokumen digital.

1.2 Perumusan Masalah

Tanda tangan digital merupakan suatu mekanisme yang memungkinkan pembuat pesan menambahkan sebuah kode-kode yang bertindak sebagai tanda tangan. Mekanisme yang digunakan adalah dengan menggabungkan algoritma kunci publik dan fungsi *hash*. Salah satu algoritma yang menggunakan mekanisme ini adalah algoritma *DSA*.

Tugas akhir ini akan membahas mengenai algoritma *DSA* dengan inti permasalahannya adalah "Bagaimana menyelesaikan permasalahan otentifikasi dengan Algoritma *DSA* ?".

1.3 Batasan Masalah

Adapun batasan masalah yang digunakan dalam tugas akhir ini adalah :

1. Informasi yang akan di enkripsi dan di dekripsi adalah berupa huruf, angka, dan simbol.
2. Fungsi *hash* satu-arah yang digunakan untuk menghasilkan *message digestnya* adalah *Secure Hash Algorithm-1* (*SHA*-1).

BAB IV

KESIMPULAN

Adapun kesimpulan yang dapat diambil dari pembuatan tugas akhir ini adalah jika seseorang ingin mengirimkan suatu dokumen penting kepada orang lain dengan menggunakan jalur internet, kekhawatiran akan perubahan dokumen oleh pihak-pihak yang tidak berhak dapat diatasi dengan memberikan tanda tangan pada dokumen tersebut. Tanda tangan tersebut adalah bukti bahwa dokumen masih asli dan berasal dari pengirim yang asli. Pemberian tanda tangan pada dokumen dapat dilakukan dengan cara membangkitan sepasang kunci (kunci publik dan kunci rahasia), membuat sepasang tanda tangan *r* dan *s*, tetapi sebelumnya harus dicari terlebih dahulu nilai *message digest* atau pesan singkat dari pesan yang akan dikirim dengan menggunakan fungsi *hash SHA*-1. Pembuktian keaslian dokumen yang diterima dapat dilakukan dengan cara memverifikasikan tanda tangan r dan s, pada proses ini penerima pesan sudah mengetahui kunci publik si pengirim pesan dan fungsi *hash* yang digunakan oleh pengirim pesan untuk mendapatkan nilai *message digest*. Verifikasi dilakukan dengan membandingkan nilai *v* yang didapat dengan nilai tanda tangan yang dikirim, tanda tangan akan sah atau keotentikan dari suatu dokumen akan terjamin jika tanda tangan yang dikirim *r* sama dengan v yang didapatkan.

DAFTAR PUSTAKA

[1] Ariyus, D. 2008. *Pengantar Ilmu Kriptografi*. ANDI. Yogyakarta.

[2] Durbin, J. R. 2000. *Modern Algebra An Introduction*. New York. John Wiley and Sons, Inc.

[3] Menezes, A. V. O. dan S. Vanstone. 1997. *Handbook Of Applied Cryptography*. ISC Press.

[4] Munir, R. 2006. *Kriptografi*. Informatika .Bandung.

[5] Munir, R. 2005. *Matematika Diskrit*, edisi-3. Informatika. Bandung.

[6] Siang, J. J. 2004. *Matematika Diskrit dan Aplikasinya pada Ilmu Komputer*. ANDI.Yogyakarta.