TANDA TANGAN DIGITAL PADA DOKUMEN DENGAN MENGGUNAKAN FUNGSI HASH SATU ARAH SHA-1 DAN ALGORITMA *RSA*

SKRIPSI SARJANA MATEMATIKA

OLEH :

ENDANG SUPRIHATIN
05134049

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS ANDALAS
PADANG
2010

ABSTRAK

Tanda tangan digital pada dokumen menggunakan fungsi hash satu arah SHA-1 dan algoritma *Rivest Shamir Adleman (RSA)*. Metode yang digunakan adalah proses *hashing* terhadap dokumen masukan, dan hasilnya disebut sebagai *message digest*. Kemudian *message digest* tersebut dienkripsi dengan Algoritma *RSA* sehingga dihasilkan tanda tangan digital. Tanda tangan digital dideskripsi dengan menggunakan algoritma *RSA* sehingga diperoleh nilai *h*. Dokumen yang dikirim juga dilakukan proses *hashing* untuk mendapatkan *message digest* dokumen awal kemudian dimodulokan dengan *n* (hasil dari perkalian bilangan prima sebarang yang dipilih) sehingga diperoleh nilai *h'*. Kemudian dibandingkan nilai *h* dengan nilai *h'* untuk mengetahui otentikasi dari dokumen yang dikirim. Jika nilainya sama berarti dokumen tersebut asli sedangkan jika tidak sama, maka dokumen tersebut tidak asli atau telah diubah saat pengiriman.

Kata kunci : *tanda tangan digital, fungsi hash satu arah SHA-1, Rivest Shamir Adleman (RSA), message digest, algoritma RSA*

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.* Dalam tugas akhir ini akan membahas tanda tangan digital dengan menggunakan algoritma *RSA* dan fungsi *hash* satu arah SHA-1.

1.2 Perumusan Masalah

Dalam tugas akhir ini akan dibahas hal-hal mengenai :

1. Bagaimana melakukan tanda tangan digital pada dokumen dengan menggunakan fungsi *hash* satu arah SHA-1 dan algoritma *RSA*.
2. Bagaimana membuktikan bahwa pesan yang telah bertanda tangan digital adalah pesan yang asli dikirim oleh pengirim.

1.3 Pembatasan Masalah

Adapun batasan masalah tugas akhir ini adalah :

1. Tidak membahas bagaimana cara pengiriman pesan yang telah ditanda tangani secara digital.
2. Dokumen yang ditanda tangani merupakan *file text*.
3. Protokol komunikasi yang digunakan adalah penandatanganan dokumen dengan sistem kriptografi kunci publik (*RSA*) dan fungsi *hash* satu arah SHA-1.

BAB IV

KESIMPULAN

Fungsi *hash* satu arah SHA-1 dapat digunakan untuk memastikan keaslian suatu dokumen dengan pembangkit *message digest*. Fungsi *hash* satu arah SHA-1 menjamin keaslian suatu dokumen yang berarti bahwa suatu dokumen yang dikirim sama dengan dokumen asli.

Algoritma RSA menjamin identitas pembuat dokumen yaitu otentikasi terhadap tanda tangan digital yang berhasil memastikan bahwa pemilik kunci privat adalah pemilik dokumen yang sedang diproses.

DAFTAR PUSTAKA

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

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

[3] Hoffstein, J, Jill P. dan Joseph H. S. 2008. *An Intoduction to Mathematical Cryptography*. Springer Science+Busines Media, LLC.

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

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

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

[7] Rosen, K. H. 2007. *An Introduction to Cryptography*. Taylor & Francis Group, LLC .

[8] Siang, J. J. 2004. *Matematika Diskrit dan Aplikasinya pada Ilmu Komputer*. Andi Offset.Yogyakarta.