

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada era globalisasi seperti saat ini, ilmu di dunia berkembang sangat pesat terutama di bidang teknologi. Perkembangan ilmu dan teknologi sangat mempengaruhi segala aspek kehidupan, salah satunya yaitu aspek komunikasi. Komunikasi berupa pertukaran pesan teks sangatlah mudah dan cepat untuk dilakukan, namun hal ini tidak menutup kemungkinan bahwa pesan tersebut dapat diketahui oleh pihak ketiga yang mana seharusnya pengirim hanya mengirimkan pesan tersebut secara pribadi kepada penerima yang dituju. Penerima pesan harus memastikan bahwa pesan yang ia terima adalah pesan asli yang dituliskan oleh pengirim tanpa adanya perubahan pesan yang dilakukan oleh pihak ketiga. Upaya yang dilakukan untuk menjaga kerahasiaan, integritas, dan otentikasi pesan tersebut, maka pesan yang akan dikirim oleh pengirim kepada penerima disandikan menjadi kode-kode yang tidak dapat dipahami, sehingga apabila ada pihak ketiga yang ingin membaca atau mengubah pesan tersebut maka akan merasa kesulitan dalam menerjemahkan isi pesan tersebut. Selain menyandikan pesan, hal lain yang dapat memperkuat kerahasiaan dan keaslian pesan yaitu dengan dibubuhkan sebuah tanda tangan digital pada pesan. Suatu tanda tangan digital diberikan dalam bentuk nilai hasil hashing dan dienkripsi dengan algoritma kriptografi (Wiyono & Hardjianto, 2016).

Tanda tangan digital (*Digital Signature*) merupakan mekanisme otentikasi dimana pengirim pesan menambahkan kode yang memiliki fungsi sebagai tanda tangan (Munir, 2006). Tanda tangan digital dibuat dengan menentukan nilai hash dari pesan teks yang diinputkan serta mengenkripsinya menggunakan algoritma kriptografi. Algoritma kriptografi yang digunakan pada proses pembuatan tanda tangan digital yaitu algoritma kunci asimetri yang memiliki sepasang kunci diantaranya kunci publik yang berfungsi sebagai verifikasi pesan oleh penerima dan kunci privat bersifat rahasia sehingga tidak boleh diberikan kepada siapapun karena kunci privat digunakan saat

proses menandatangani pesan yang akan dikirim. Selain algoritma kriptografi, terdapat sebuah fungsi yang sesuai sebagai aplikasi keamanan seperti otentikasi dan integritas pesan. Fungsi tersebut merupakan fungsi hash yang menerima *string* dengan panjang sembarang lalu dikonversi menjadi *string* keluaran yang penjangnya tetap (*fixed*). Fungsi hash ini digunakan untuk mengubah pesan ke dalam nilai hash atau *Message Digest* (MD) (Maryanto, 2008).

Algoritma kriptografi Elgamal merupakan salah satu algoritma kriptografi yang banyak digunakan dalam pembuatan tanda tangan digital (*digital signature*) karena algoritma ini efektif dan tahan terhadap serangan kriptanalisis dengan menggunakan bilangan prima cukup besar. Algoritma ini ditemukan oleh ilmuwan Mesir bernama Taher Elgamal pada tahun 1985 (Sari, dkk., 2018). Algoritma Elgamal memiliki kelebihan yaitu tingkat kesulitan untuk dipecahkan oleh pihak ketiga karena menggunakan logaritma diskrit, terutama jika memilih bilangan prima yang besar. Oleh karena itu algoritma Elgamal banyak digunakan sebagai tanda tangan digital karena telah dilakukan banyak penelitian dan terbukti memiliki tingkat keamanan yang tinggi (Kromodimoeljo, 2009). Berikut ini adalah beberapa penelitian mengenai algoritma kriptografi Elgamal oleh kriptografer, antara lain Penerapan Algoritma Kriptografi Elgamal Untuk Pengamanan File Citra (Tamam, dkk., 2010), Pembuatan Tanda Tangan Digital dengan Elgamal atas Z_p^* (Arizka, 2011), Algoritma Kriptografi Elgamal (Singh dan Kumar, 2012), Keamanan Informasi Menggunakan Enkripsi Elgamal (Fujun, 2013).

Selain menggunakan algoritma kriptografi dalam pembuatan tanda tangan digital (*digital signature*), juga diperlukan fungsi hash untuk mengubah pesan teks ke dalam bentuk nilai hash atau *message digest* (MD), dimana *message digest* (MD) merupakan suatu pengolahan pesan untuk menghasilkan suatu *digest* menggunakan fungsi hash. Terdapat banyak sekali fungsi hash, antara lain Whirlpool, SHA-512, DSA, dan sebagainya. Whirlpool merupakan fungsi hash yang didesain oleh Vincent Rijmen dan Paulo S. L. M. Barreto yang beroperasi pada pesan dengan ukuran kurang dari 2^{256} bit, dan menghasilkan *message digest* berukuran 512 bit (Setiawan,

2010/2011). Whirlpool memiliki kelebihan yaitu menghasilkan nilai hash yang stabil dibandingkan fungsi hash lainnya untuk digunakan sebagai kata kunci sehingga Whirlpool sangat baik digunakan sebagai fungsi hash (**Setiawan 2010/2011**). Fungsi hash Whirlpool telah dilakukan beberapa penelitian antara lain Keamanan Fungsi Hash Whirlpool (Stallings, 2005), Implementasi Fungsi Hash Whirlpool (Kitsos, 2004), Penerapan Fungsi Hash Whirlpool Dalam Verifikasi Integritas Data (Rachmadan, 2019).

Algoritma Kriptografi Schnorr ditemukan pada tahun 1989 oleh Claus Schnorr. Pada Algoritma Schnorr terdapat proses otentikasi dimana pada proses ini pengirim dan penerima pesan dapat saling memverifikasi atau mengidentifikasi kebenaran kedua belah pihak dengan menggunakan kunci publik dan kunci privat yang telah dibentuk sebelumnya. Dengan menggunakan algoritma ini maka dapat diidentifikasi kebenaran pihak yang berkomunikasi maupun mengidentifikasi sumber pesan. Kelebihan dari algoritma ini yaitu sulit dalam memecahkannya karena menggunakan logaritma diskrit, sehingga algoritma ini sangat cocok digunakan sebagai otentikasi (**Manurung, 2019**). Algoritma kriptografi Schnorr telah banyak dilakukan penelitian sebelumnya, antara lain Otentikasi dengan Metode Simulasi Schnorr (Manurung, 2019), Penerapan Schnorr pada Tanda Tangan Sigital (Isnaini, dkk., 2017), Simulasi Otentikasi Data dengan Metode Schnorr (Mustari, 2010). Implementasi Algoritma Schnorr pada File Teks Berbasis Android (Nugraha, 2017).

Berdasarkan uraian diatas, penulis tertarik untuk mengimplementasikan algoritma kriptografi Elgamal dan fungsi hash Whirlpool untuk membuat tanda tangan digital (*digital signature*) serta otentikasi pesan menggunakan algoritma kriptografi Schnorr. Diharapkan penggunaan algoritma kriptografi Elgamal dan fungsi hash Whirlpool dapat menghasilkan tanda tangan digital (*digital signature*) yang memiliki tingkat keamanan yang tinggi serta otentikasi pesan menggunakan algoritma kriptografi Schnorr untuk mengidentifikasi kebenaran pihak yang berkomunikasi maupun mengidentifikasi sumber pesan.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, dapat dirumuskan pokok permasalahan yang akan menjadi kajian dari makalah ini, antara lain:

1. Bagaimana prosedur pembuatan tanda tangan digital menggunakan algoritma kriptografi Elgamal dan fungsi hash Whirlpool serta proses otentikasi menggunakan algoritma kriptografi Schnorr?
2. Bagaimana membuat program tanda tangan digital menggunakan algoritma kriptografi Elgamal dan fungsi hash Whirlpool serta proses otentikasi menggunakan algoritma kriptografi Schnorr?
3. Bagaimana mengimplementasikan program tanda tangan digital menggunakan algoritma kriptografi Elgamal dan fungsi hash Whirlpool serta proses otentikasi menggunakan algoritma kriptografi Schnorr pada contoh kasus ?

1.3 Tujuan

Tujuan dari penelitian ini adalah:

1. Mengetahui prosedur pembuatan tanda tangan digital menggunakan algoritma kriptografi Elgamal dan fungsi hash Whirlpool serta proses otentikasi menggunakan algoritma kriptografi Schnorr.
2. Mengetahui pembuatan program tanda tangan digital menggunakan algoritma kriptografi Elgamal dan fungsi hash Whirlpool serta proses otentikasi menggunakan algoritma kriptografi Schnorr.
3. Mengimplementasikan tanda tangan digital menggunakan algoritma kriptografi Elgamal dan fungsi hash Whirlpool serta proses otentikasi menggunakan algoritma kriptografi Schnorr pada contoh kasus.

1.4 Manfaat

Manfaat dari penelitian ini adalah:

1. Menjadi sarana informasi bagi pembaca mengenai materi kriptografi khususnya tanda tangan digital menggunakan algoritma kriptografi Elgamal dan fungsi hash Whirlpool, serta otentikasi menggunakan algoritma kriptografi Schnorr.
2. Memberikan wawasan mengenai cara menjaga kerahasiaan dan integritas pesan melalui tanda tangan digital menggunakan algoritma kriptografi Elgamal dan fungsi hash Whirlpool serta otentikasi menggunakan algoritma kriptografi Schnorr.
3. Menjadi pembandingan bagi pembaca mengenai algoritma kriptografi maupun fungsi hash lain sebagai pendukung dalam perkembangan ilmu dan teknologi di masa mendatang.

1.5 Batasan Masalah

Batasan masalah dari penelitian ini adalah:

1. Format *file* yang dapat diproses pada program yaitu (.txt).
2. Panjang pesan maksimal yang dapat diproses yaitu sebesar 2^{256} bit.