

BAB I PENDAHULUAN

1.1 Latar Belakang

Di era globalisasi ini pertumbuhan teknologi semakin pesat, pertukaran pesan semakin mudah dilakukan melalui jaringan publik seperti internet atau media lain. Dengan semakin berkembangnya internet, sebuah dokumen kini tidak hanya diterbitkan dalam bentuk cetak saja, tetapi juga dalam bentuk digital. Akan tetapi, sebuah dokumen yang ditransmisikan melalui internet sangat rentan terhadap kemungkinan modifikasi serta sulitnya pembuktian keaslian dokumen tersebut. Masalah dalam pertukaran pesan tersebut merupakan masalah kriptografi yang berhubungan dengan keamanan pesan yakni kerahasiaan, integritas, serta autentikasi (**Ranti, dkk., 2018**). Permasalahan dalam pertukaran pesan tersebut dapat diatasi dengan memberikan tanda tangan digital pada pesan. Pemberian tanda tangan digital bertujuan untuk memastikan identifikasi kebenaran penandatanganan sekaligus menjamin keaslian isi yang tercantum dalam pesan. Suatu tanda tangan digital akan diberikan dalam bentuk nilai hasil hashing dan dienskripsi dengan algoritma kriptografi (**Munir, 2006**).

Tanda tangan digital sebenarnya merupakan hasil dari diberlakukannya teknik kriptografi terhadap pesan atau dokumen asli. Tanda tangan digital harus memiliki fungsi yang sama dengan tanda tangan konvensional, yaitu dapat menjamin autentikasi, integritas, dan kerahasiaan (**Azdy, 2016**). Algoritma kriptografi yang digunakan untuk membuat tanda tangan digital adalah algoritma kriptografi asimetri yang memiliki sepasang kunci yakni kunci publik yang berfungsi untuk proses verifikasi serta kunci privat yang berfungsi untuk proses tanda tangan. Beberapa algoritma kriptografi yang dapat digunakan untuk membangun tanda tangan digital adalah RSA, DSA (*Digital Signature Algorithm*), ElGamal, dan Schnorr. Algoritma kriptografi yang aman digunakan adalah algoritma DSA (*Digital Signature Algorithm*), karena sulit untuk dipalsukan. DSA (*Digital Signature Algorithm*) dikembangkan dari algoritma

Schnorr dan ElGamal. DSA (*Digital Signature Algorithm*) merupakan salah satu kriptografi kunci publik yang digunakan untuk otentikasi, pengamanan data, dan perangkat anti sangkal (Nurhasanah, 2013). Pada DSA (*Digital Signature Algorithm*) dibutuhkan program khusus untuk membangkitkan kunci dan masalah yang timbul adalah kepercayaan pengguna pada program tersebut. Parameter yang digunakan yaitu menggunakan parameter kunci *public* dan kunci *private* yang dinamis yaitu bernilai berbeda untuk tiap proses pembuatan tanda tangan digital (Arisandi, 2020).

Selain menggunakan algoritma kriptografi, dalam membuat tanda tangan digital juga membutuhkan fungsi hash yang bertujuan untuk mengubah pesan kedalam bentuk nilai hash atau *message digest*. Terdapat banyak jenis fungsi hash yang digunakan dalam mengubah pesan seperti SHA-0, SHA-1, SHA-2, MD2, MD4, MD5 dan masih banyak yang lainnya. Fungsi hash yang aman digunakan adalah fungsi hash SHA-512, karena selain tidak mengalami kolisi, *message digest* yang dihasilkan juga besar yakni 512 bit (Munir, 2006). Fungsi hash SHA-512 juga tahan terhadap serangan kriptanalisis karena memiliki ukuran *message digest* yang besar yaitu 512 bit, serangan berupa *preimage*, *second preimage* dan *collision* membutuhkan sangat banyak pesan yang membuat serangan menjadi tidak layak (Sadikin, 2012). Fungsi hash SHA-512 merupakan fungsi hash yang didesain oleh NSA (*National Security Agency*) dan dipublikasikan oleh NIST (*National Institute of Standard and Technology*) sebagai *Federal Information Processing* (FIPS) pada tahun 1993. Fungsi hash SHA-512 menerima sebarang masukan pesan dengan ukuran maksimum 2^{128} bit dan mengubahnya menjadi nilai hash atau *message digest* yang panjangnya tetap berukuran 512 bit. Fungsi hash SHA-512 bekerja dalam satu arah artinya suatu pesan yang telah diubah dalam nilai hash atau *message digest* tidak dapat dikembalikan lagi dalam bentuk aslinya serta tidak mungkin mendapatkan nilai hash atau *message digest* yang sama untuk pesan yang berbeda (NIST, 2008).

Masalah keamanan dengan tanda tangan digital sebelumnya sudah pernah dibuat yakni pembuatan tanda tangan digital menggunakan DSA (*Digital Signature Algorithm*) dan fungsi hash SHA-1. Fungsi hash SHA-1 merupakan

fungsi hash satu arah yang menerima pesan dengan ukuran maksimum 2^{64} bit dan menghasilkan nilai hash atau *message digest* yang panjangnya tetap yakni berukuran 160 bit. Pada tahun 2005, Rijmen dan Oswald mempublikasikan serangan pada versi SHA-1 dan menemukan kolisi, sedangkan pada tahun yang sama pada bulan Februari Xiayoun Wang, Yiqun Lisa Yin, dan Hongho Yo mempublikasikan serangan yang dapat menemukan kolisi pada versi penuh SHA-1 sehingga fungsi hash SHA-1 sudah tidak aman lagi digunakan karena sudah mengalami serangan (Munir, 2006).

Berdasarkan uraian diatas sangatlah menarik untuk mengaplikasikan fungsi hash SHA-512 dan algoritma kriptografi DSA (*Digital Signature Algorithm*) untuk membuat tanda tangan digital. Diharapkan dengan menggunakan fungsi hash SHA-512 dan algoritma kriptografi DSA (*Digital Signature Algorithm*), tanda tangan digital yang dihasilkan dapat digunakan untuk autentikasi pesan.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka dapat diajukan rumusan masalah sebagai berikut:

1. Bagaimana implementasi algoritma kriptografi *Digital Signature Algorithm* (DSA) dan fungsi hash SHA-512 dalam pembuatan tanda tangan digital pada pesan teks?
2. Bagaimana membuat program tanda tangan digital menggunakan algoritma kriptografi *Digital Signature Algorithm* (DSA) dan fungsi hash SHA-512?
3. Bagaimana implementasi program tanda tangan digital menggunakan algoritma kriptografi *Digital Signature Algorithm* (DSA) dan fungsi hash SHA-512 pada pesan teks?

1.3 Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengimplementasikan algoritma kriptografi *Digital Signature Algorithm* (DSA) dan fungsi hash SHA-512 dalam pembuatan tanda tangan digital pada pesan teks.
2. Membuat program pembuatan tanda tangan digital menggunakan algoritma kriptografi *Digital Signature Algorithm* (DSA) dan fungsi hash SHA-512.
3. Mengimplementasikan program tanda tangan digital menggunakan algoritma kriptografi *Digital Signature Algorithm* (DSA) dan fungsi hash SHA-512 pada pesan teks.

1.4 Manfaat

Manfaat dari penelitian ini adalah sebagai berikut:

1. Menambah wawasan mahasiswa tentang cara membuat tanda tangan digital menggunakan *Digital Signature Algorithm* (DSA) dan fungsi hash SHA-512.
2. Dapat dijadikan bahan untuk perbandingan dengan algoritma kriptografi maupun fungsi hash lain dan dapat mendukung perkembangan ilmu dan teknologi di masa mendatang.
3. Mengetahui hasil dari implementasi program pada contoh kasus.

1.5 Batasan Masalah

Batasan masalah dari penelitian ini adalah sebagai berikut:

1. Format pesan teks yang diinputkan hanya bisa menggunakan *.txt*
2. Panjang pesan teks yang diinputkan maksimal sebesar 2^{128} bit.