BAB I
PENDAHULUAN

1.1 Latar belakang

Dengan semakin berkembangnya teknologi, kini dokumen tidak hanya diproduksi dalam bentuk cetak tetapi diproduksi juga dalam bentuk digital. Untuk menjaga keaslian pada dokumen tersebut, dibutuhkanlah tanda tangan. Terdapat dua jenis tanda tangan, yaitu tanda tangan konvensional dan tanda tangan digital. Tanda tangan konvesional biasa digunakan dalam dokumen cetak sedangkan tanda tangan digital digunakan pada dokumen digital.

Pada dokumen cetak, tanda tangan konvensional digunakan untuk meng-identifikasi keabsahan seseorang pada dokumen yang ditandatanganinya. Selain itu, tanda tangan konvensional juga dapat digunakan untuk membuktikan bahwa penandatangan telah mengetahui dan menyetujui isi dari dokumen yang ditandatanganinya tersebut (Azdy, 2016).

Walaupun tanda tangan konvensional berperan dalam menjaga keaslian dokumen namun hal itu tidak sepenuhnya menjamin bahwa dokumen itu asli. Dilansir dalam news.detik.com, Bupati Bondowoso Salwa Arifin melaporkan kasus pemalsuan tanda tangan dan stempel Pemkab. Pemalsuan dilakukan sebagai modus untuk meminta sumbangan (Widarsha, 2019). Tanda tangan konvensional mudah disalin kembali baik secara manual tulis tangan maupun disalin secara digital. Oleh karena itulah dokumen cetak rentan untuk dipalsukan

Pada dokumen digital, tanda tangan digital digunakan untuk menjaga keaslian dokumen secara keseluruhan. Tanda-tangan digital adalah suatu nilai kriptografis yang bergantung pada isi berkas digital dan kunci pemilik berkas digital. Proses autentikasi dilakukan untuk membuktikan keaslian tanda tangan digital tersebut. Jika tanda-tangan digital asli maka berkas digital masih asli dan dan pemiliknya adalah orang yang sah (Munir, 2005).

Tanda tangan digital bukanlah sebuah tanda tangan konvensional yang di-digitalkan. Terdapat perbedaan antara tanda tangan konvensional dengan tanda

tangan digital. Perbedaan mencolok antara tanda tangan konvensional dan tanda tangan digital ialah tanda tangan konvensional bersifat tetap (dapat menggunakan tanda tangan konvensional yang sama pada dokumen yang berbeda) sedangkan tanda tangan digital bersifat tidak tetap (setiap dokumen yang berbeda memiliki tanda tangan yang berbeda pula). Setiap ada perubahan dokumen maka tanda tangannya pun ikut berubah. Karena sifat itulah tanda tangan digital tidak dapat disalin dan dipalsukan. Adapun proses pembentukan tanda tangan digital yaitu menggunakan *Digital Signature Algorithm* (DSA).

DSA merupakan kriptografi yang digunakan dalam autentikasi pesan. DSA digunakan untuk memberi keamanan pada pesan atau dokumen. Dengan pengaplikasian DSA, penerima dapat langsung mengetahui bahwa pesan yang diterimanya terjadi perubahan atau tidak. Apabila terjadi perubahan pesan saat pengiriman, maka dapat dipastikan bahwa pesan tersebut palsu dan sebaliknya apabila tidak terjadi perubahan pesan selama pengiriman maka dapat dipastikan bahwa pesan tersebut asli. Adapun contoh penerapannya adalah penandatanganan kontrak atau dokumen resmi berbasis elektronik seperti sertifikat digital.

Dalam prosesnya, DSA memerlukan fungsi hash. Fungsi hash adalah suatu fungsi yang dapat mengkonversi pesan teks dengan panjang karakternya sembarang menjadi pesan teks acak dengan panjang karakter yang tetap (Munir, 2005). Fungsi hash termasuk dalam kriptografi satu arah yaitu kriptografi yang hanya dapat enkripsi pesan namun tidak dapat dekripsi pesan. Output yang dihasilkan dari proses hashing disebut nilai hash (H(m)). Fungsi hash memiliki banyak macam contohnya ialah *Secure Hash Algorithm* (SHA) dan (*Message Digest*) MD. Saat ini suatu fungsi hash masih memungkinkan untuk memetakan dua pesan yang berbeda tetapi menghasilkan nilai hash yang sama. Hal itu disebut dengan *collision* (tumbukan) (Prihardhanto, 2010).

Dhea Pungky Precilia dan Ahmad Izzuddin (2015) dalam jurnalnya yang berjudul "Aplikasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritma Message Digest 5 (MD5)" membangkitkan tanda tangan digital menggunakan fungsi hash MD5 pada media teks (Precilia & sIzzuddin, 2016).

Arpan dan Nova Mayasari (2019) dalam jurnalnya yang berjudul "MEMBANGKITKAN DIGITAL SIGNATURE DENGAN ALGORITMA MD5 DAN ALGORITMA RSA UNTUK MEMASTIKAN KEASLIAN FILE" membangkitkan tanda tangan digital menggunakan fungsi hash MD5 pada media gambar (Mayasari & Arpan, 2019). Kedua jurnal tersebut menggunakan MD5 sebagai fungsi hash yang digunakan pada DSA. MD5 kurang baik digunakan pada DSA karena MD5 telah ditemukan tumbukan bahkan Tao Xie, Fanbao Liu dan Dengguo Feng telah menemukan algoritma untuk mencari tumbukan dalam MD5. Algoritma tersebut ditulis dalam jurnalnya yang berjudul "Fast Collision Attack on MD5" (Xie et al., 2006). DSA umumnya menggunakan fungsi hash SHA-1 pada prosesnya namun pada 23 februari 2017 google security mengumumkan bahwa CWI Institute in Amsterdam beserta Google berhasil menemukan kecacatan berupa tumbukan pada SHA-1 (Stevens Marc et al., 2017). Dikarenakan sudah banyak penelitian tentang *digital signature* menggunakan kriptografi RSA dengan fungsi hash MD5 dan pula MD5 dan SHA-1 telah ditemukan tumbukan maka penulis menggunakan DSA dengan fungsi hash SHA-256

Berdasarkan latar belakang yang telah dipaparkan sebelumnya maka penulis tertarik mengangkat masalah tersebut dengan judul "*IMPLEMENTASI DIGITAL SIGNATURE ALGORITHM (DSA) MENGGUNAKAN SECURE HASH ALGORITHM-256 (SHA-256) PADA MEDIA GAMBAR*". Penelitian ini akan merancang sebuah program komputer DSA yang dibangun dengan bahasa pemrograman Python 3.7.

1.2 Rumusan masalah

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, maka dapat disusun rumusan masalah sebagai berikut :

1. Bagaimana implementasi *Digital Signature Algorithm* pada media gambar?
2. Bagaimana konstruksi program *Digital Signature Algorithm* sebagai alat autentikasi media gambar?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dipaparkan sebelumnya, tujuan penelitian makalah ini sebagai berikut :

1. Mengetahui implementasi *Digital signature algorithm* pada media gambar.
2. Dapat mengkonstruksi program aplikasi *Digital Signature algorithm* sebagai alat autentikasi media gambar

1.4 Batasan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas, maka diperlukan Batasan masalah dalam tulisan ini. File gambar yang akan diberi tanda tangan digital memiliki ukuran resolusi kurang dari 1000x1000 karena semakin besar resolusi gambar maka semakin lama proses pembentukan tanda tangan

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut :

1) Manfaat teoritis :

   Hasil dari penelitian ini dapat menambah pengetahuan dalam pembuatan tanda tangan digital pada media gambar dan sebagai pengembangan model kriptografi dalam bidang tanda tangan digital. Selain itu dapat digunakan sebagai referensi bagi pembaca yang sedang mendalami bidang kriptografi.

2) Manfaat praktis :

   Hasil program yang telah dikonstruksi dapat digunakan pembaca untuk menjaga keaslian suatu gambar.

1.6 Sistematika Penulisan

1. BAB I PENDAHULUAN

   Menjelaskan latar belakang masalah, rumusan masalah, tujuan penelitian, Batasan masalah, manfaat penelitian dan sistematika penelitian.

2. BAB II KAJIAN PUSTAKA

   Menjelaskan kriptografi DSA, fungsi hash dan teori-teori yang mendukung.

3. BAB III METODOLOGI PENELITIAN

   Menjelaskan langkah-langkah perancangan kriptografi DSA menggunakan fungsi hash SHA-256 pada media gambar serta langkah mengkonstruksi program.

4. BAB IV HASIL DAN PEMBAHASAN

   Pada bab ini menjelaskan bahasan dan hasil program tentang implementasi DSA pada media gambar beserta contoh kasus.

5. BAB V KESIMPULAN DAN SARAN

   Pada bab ini menjelaskan kesimpulan dan saran atas penelitian makalah ini.