BAB I
PENDAHULUAN

1.1 Latar Belakang

Dokumen digital merupakan data yang berupa teks yang memiliki sifat terbuka yaitu isinya dapat dibaca dan diubah dengan sangat mudah oleh pihak-pihak yang tidak berhak. Hal ini menyebabkan faktor keamanan dari dokumen digital sangat tidak terjamin. Keamanan dokumen digital adalah bagaimana kita dapat mencegah penipuan, atau paling tidak mendeteksi adanya penipuan di sebuah sistem yang berbasis dokumen digital, untuk melindungi dokumen digital dari pengaksesan, penggunaan, penyebaran, perusakan, perubahan, dan penghancuran tanpa otorisasi yang sah. Untuk itu diperlukan sebuah pendekatan dalam melakukan pengamanan pada dokumen digital, seperti melakukan enkripsi, steganografi, *digital signature* dan *hashing* terhadap dokumen digital tersebut (Pungky, 2015).

Kriptografi berperan penting dalam layanan keamanan seperti kerahasiaan, integritas data, autentikasi dan pencegahan penyangkalan. Kriptografi modern menggunakan kunci yang harus dirahasiakan untuk mengatasi masalah keamanan kriptografi. Permasalahan dalam penggunaan satu kunci yang sama oleh dua orang yang saling berkomunikasi untuk bertukar pesan adalah cara mendistribusikan kunci. Permasalahan ini dapat diatasi dengan penggunaan kriptografi kunci-publik, yang memungkinkan pengguna berkomunikasi secara aman tanpa perlu berbagi kunci rahasia (Rahmawati, 2009).

Masalah kerahasiaan pesan, keaslian pesan, dan anti-penyangkalan dapat diselesaikan dengan autentikasi pesan (*message authentication*). Alternatif cara yang digunakan untuk autentikasi salah satunya adalah dengan menandatangani pesan secara digital atau biasa dikenal sebagai tanda tangan digital (*digital signature*). Dengan tanda tangan digital, penerima pesan dapat memastikan bahwa pesan yang diterima telah terjadi perubahan atau tidak. Ada beberapa metode tanda tangan digital, di antaranya adalah melakukan enkripsi dengan kriptografi kunci simetri, enkripsi dengan kunci publik, atau melakukan penandatanganan dengan menggunakan kriptografi kunci publik dan fungsi *hash* (Munir, 2004).

Fungsi hash adalah suatu fungsi yang menerima masukan berupa string yang panjangnya sembarang dan mengonversi masukan tersebut menjadi string yang mempunyai panjang tetap (*fixed*) dan umumnya menjadi lebih kecil dari panjang semula (Munir, 2004). Keluaran dari fungsi *hash* disebut juga nilai *hash* atau pesan ringkas (*message digest*). Fungsi *hash* merupakan fungsi satu arah (*one-way function*) yang dapat menghasilkan ciri (*signature*) dari data. Pesan berubah satu bit saja, akan memengaruhi nilai *hash* secara signifikan. Hal ini merupakan pengaplikasian yang tepat fungsi *hash* dalam menjaga integritas data.

ElGamal Signature Scheme atau skema tanda tangan ElGamal adalah salah satu kriptografi kunci publik, skema tanda tangan digital tersebut didasarkan pada sifat aljabar dari eksponen modular, bersama dengan masalah logaritma diskrit. Algoritma ini menggunakan pasangan kunci yang terdiri dari kunci publik dan kunci privat. Kunci privat digunakan untuk menghasilkan tanda tangan digital untuk sebuah pesan, dan tanda tangan tersebut dapat diverifikasi dengan menggunakan kunci publik yang sesuai dari penanda tangan. Keamanan algoritma ini terletak pada sulitnya menghitung logaritma diskrit, yaitu mencari nilai x sedemikian sehingga $g^x \equiv y \ (mod\ p)$ (Stinson, 2006).

Sahl Fawzy Sutopo (2020) melakukan implementasi *Digital Signature Algorthm* (DSA) menggunakan *Secure Hash Algorithm*-256 (SHA-256) pada media gambar. Pada penelitian tersebut dapat disimpulkan bahwa DSA tidak hanya dapat diimplementasikan pada pesan teks namun dapaat diimplementasikan pada pesan gambar. Algoritma DSA dapat dikonstruksi menjadi program computer sehingga dapat mempermudah pengguna dalam hal pembentukan tanda tangan dan autentikasi tanda tangan.

Salah satu fungsi *hash* adalah SHA (*Secure Hash* Algorithm). SHA diterbitkan oleh *National Institute of Standard and Technology* sebagai standar pemrosesan informasi federal di Amerika Serikat atau FIPS. SHA yang dibuat merupakan seperangkat *hash* kriptografi sederhana dan dikembangkan untuk menjaga dan meningkatkan integritas keamaan data. SHA yang mempunyai tingkat keamanan tinggi adalah SHA-256 yang merupakan pengembangan dari beberapa SHA sebelumnya. Di mana pada beberapa SHA sebelumnya, para peneliti menemukan beberapa kelemahan, yakni terjadinya tabrakan karena adanya proses

dua arah dan terjadi serangan (kolosi). Oleh karena itu, SHA yang sangat disarankan peneliti untuk saat ini dalam menjaga integritas data adalah SHA-256. Dengan mempertimbangan kekuatan fungsi *hash* SHA-256 dan kunci publik ElGamal, maka penulis akan menggunakan kedua algoritma tersebut untuk autentikasi dokumen digital.

Berdasarkan pemaparan sebelumnya, penulis tertarik untuk mengkaji autentikasi dokumen digital dengan menggunakan SHA-256 dan *ElGamal Signature Scheme* yang diimplementasikan ke program aplikasi Python. Oleh karena itu, penulis mengambil judul **"Autentikasi Dokumen Digital dengan Menggunakan *Secure Hash Algorithm-256* dan *ElGamal Signature Scheme*"**

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka yang menjadi rumusan masalah pada penulisan ini adalah:

1. Bagaimana prosedur autentikasi dokumen digital dengan menggunakan SHA-256 dan *ElGamal Signature Scheme*?
2. Bagaimana konstruksi program aplikasi untuk menjaga autentikasi dokumen digital dengan menggunakan SHA-256 dan *ElGamal Signature Scheme* berbantuan program aplikasi Python?

1.3 Batasan Masalah

Batasan masalah yang akan digunakan pada penulisan ini adalah jenis data yang digunakan berupa dokumen digital dengan ekstensi (*.pdf).

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah, tujuan dari penulisan ini adalah:

1. Mengidentifikasi konsep autentikasi dokumen digital dengan menggunakan SHA-256 dan *ElGamal Signature Scheme*.
2. Membuat program aplikasi untuk menjaga autentikasi dokumen digital dengan menggunakan SHA-256 dan *ElGamal Signature Scheme* berbantuan program aplikasi Python.

1.5 Manfaat Penelitian

Adapun manfaat dari penulisan ini adalah:

1. Meningkatkan pemahaman tentang konsep autentikasi suatu dokumen digital dengan menggunakan SHA-256 dan *ElGamal Signature Scheme*.
2. Memberikan kontribusi pada bidang matematika terapan serta mempermudah pengguna dalam proses autentikasi suatu dokumen digital menggunakan SHA-256 dan *ElGamal Signature Scheme* dengan program aplikasi Python.

1.6 Sistematika Penulisan

Berikut ini struktur penulisan dari pengkajian masalah dipaparkan sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi latar belakang dari masalah yang diambil, rumusan masalahnya, tujuan, manfaat serta batasan masalah dari pengkajian masalah yang dilakukan.

BAB II LANDASAN TEORI

Bab ini membahas teori-teori yang berkaitan dengan permasalahan dan penyelesaian yang akan diambil.

BAB III METODE PENELITIAN

Bab ini menjelaskan langkah-langkah yang diambil untuk menyelesaikan permasalahan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini memuat hasil penelitian mengenai Autentikasi Dokumen Digital Menggunakan *Secure Hash Algorithm*-256 dan *ElGamal Signature Scheme* serta implementasinya dengan program aplikasi Python.

BAB V SIMPULAN DAN SARAN

Bab ini memuat kesimpulan isi keseluruhan uraian bab-bab sebelumnya dan saran-saran dari hasil penulisan skripsi ini.