Bab I

Pendahuluan

1.1 Latar Belakang

Pandemi *Corona Virus Disease* 2019 (COVID-19) telah memaksa sebagian besar orang untuk melakukan pekerjaannya dari rumah atau yang biasa dikenal dengan *Work From Home* (WFH). Konsep WFH ini adalah melakukan semua pekerjaan kantor melalui rumah dengan media internet. Salah satu pekerjaan yang sering dilakukan para pekerja adalah melakukan pengiriman dokumen secara online. Namun kegiatan ini mempunyai resiko yang cukup berbahaya, salah satunya adalah pemalsuan dokumen. Salah satu cara pemalsuan dokumen adalah dengan cara memalsukan tanda tangan yang ada pada suatu dokumen.

Tanda tangan digital merupakan sebuah alat kriptografi yang digunakan untuk menandatangani dan memverifikasi pesan untuk menyediakan autentikasi, integritas dan non-repudiasi pada sebuah dokumen elektronik Aggarwal and Kumar (2021). Setelah munculnya *public key cryptosystem*, tanda tangan digital telah banyak digunakan oleh sistem komersial seperti email dan transfer elektronik karena integritas dan non-repudiasi dari tanda tangan digital dianggap lebih baik daripada tanda tangan basah yang ditulis tangan Yang, Zhang, Xiao and Zhao (2021)

Sudah banyak algoritma tanda tangan digital telah diusulkan sebelumnya, namun demikian algoritma yang paling sesuai untuk dokumen PDF dari segi keamanan dan *processing time* tanda tangan digital masih belum diketahui. Sebelumnya juga sudah banyak dilakukan analisis algoritma tanda tangan digital seperti penelitian Aufa, Affandi et al. (2018) yang membandingkan kecepatan *processing time* antara algoritma RSA dengan nilai bit yang berbeda, penelitian Gondaliya, Savani, Dhaduvai and Hossain (2018) yang membandingkan *processing time* antara algoritma HRSA, ERSA dan RSA, serta penelitian Toradmalle, Singh, Shastri, Naik and Panchidi (2018) yang membandingkan *processing time* antara algoritma RSA dan ECC. Namun penelitian yang membandingkan algoritma RSA, ECDSA dan DSA untuk tanda tangan digital sebuah dokumen PDF masih belum ditemukan. Disamping hal tersebut, sistem layanan tanda tangan digital untuk dokumen PDF yang tersedia

relatif mahal dan sistem yang berbasis *open-source* masih terbilang sedikit.

Penelitian ini dilakukan untuk memberikan kontribusi pada bidang tanda tangan digital dengan berfokus pada analisis beberapa algoritma tanda tangan digital dan memilih yang terbaik diantaranya. Selain itu, dilakukan pembangunan prototype sebagai bentuk keluaran hasil penelitian sehingga dapat dianalisis hasil kinerjanya dan dapat dikembangkan lebih lanjut.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah tugas akhir ini adalah sebagai berikut:

1. Bagaimana mendapatkan algoritma terbaik untuk digunakan dalam penandatanganan dokumen PDF?
2. Bagaimana mengembangkan *prototype* tanda tangan digital yang dapat memilih algoritma tanda tangan digital?
3. Bagaimana melakukan analisis performansi *prototype* yang dikembangkan?

1.3 Pernyataan Masalah

Berdasarkan latar belakang di atas, dapat disimpulkan terdapat permasalahan pada algoritma ekstraksi ciri dan deteksi yang sudah ada sebagai berikut :

1. Penelitian terkait analisis algoritma mana yang terbaik untuk digunakan dalam penandatanganan dokumen PDF masih sedikit dilakukan
2. Performansi dari pengembangan *prototype* tanda tangan digital dokumen PDF masih jarang dilakukan

1.4 Tujuan

1. Melakukan analisis beberapa algoritma digital signature untuk mendapatkan algoritma terbaik untuk tanda tangan digital pada dokumen PDF
2. Mengembangkan *prototype* tanda tangan digital yang dapat memilih algoritma tanda tangan digital
3. Melakukan analisis performansi *prototype* yang dikembangkan

1.5 Batasan Masalah

Berikut adalah ruang lingkup yang ada pada penulisan tugas akhir ini :

1. Algoritma yang dianalisis hanya menggunakan DSA, ECDSA dan RSA
2. Parameter keamanan yang diukur yaitu integrity pada dokumen yang ditanda tangani

1.6 Hipotesis

1. Algoritma digital signature terbaik untuk tanda tangan dokumen PDF berhasil ditentukan

2. Dokumen yang ditanda tangani menggunakan *prototype* dapat dicek keasliannya pada website kominfo

1.7 Sistematika Penulisan

Tugas Akhir ini disusun dengan sistematika penulisan sebagai berikut :

- **BAB I Pendahuluan**. Bab ini membahas mengenai latar belakang, rumusan masalah, dan tujuan pengerjaan Tugas Akhir ini.

- **Bab II Kajian Pustaka**. Bab ini membahas fakta dan teori yang berkaitan dengan perancangan sistem untuk mendirikan landasan berfikir. Dengan menggunakan fakta dan teori yang dikemukakan pada bab ini penulis menganalisis kebutuhan akan rancangan arsitektur sistem yang dibangun.

- **BAB III Metodologi dan Desain Sistem**. Bab ini menjelaskan metode penelitian, rancangan sistem dan metode pengujian yang dilakukan dalam penelitian.

- **BAB IV Hasil dan Pembahasan**. Bab ini menunjukkan hasil penelitian dan membahas hasil penelitian.

- **BAB V Kesimpulan dan Saran**. Bab ini menjelaskan kesimpulan dan saran terhadap penelitian yang dilakukan.