BAB I

PENDAHULUAN

1.1 Latar Belakang

Tandatangan adalah suatu bentuk representasi identitas seseorang yang biasanya ditulis dengan tangan dan digunakan untuk mengesahkan dokumen atau menyatakan persetujuan. Tandatangan sering kali berupa nama atau simbol khas yang ditulis oleh individu. Secara legal, tandatangan memiliki fungsi penting dalam mengakui atau menyetujui kontrak, surat pernyataan, atau dokumen resmi lainnya (Lapian et al. 2024).

Digital Signature atau tandatangan digital adalah mekanisme kriptografi yang digunakan untuk memberikan jaminan keaslian dan integritas data dalam transaksi elektronik. Tandatangan digital memastikan bahwa pesan atau dokumen yang ditandatangani berasal dari sumber yang valid (autentik) dan tidak diubah sejak ditandatangani (integritas) (Ramdan 2024).

Untuk mengatasi resiko modifikasi atau pemalsuan dokumen digital, diperlukan suatu teknik keamanan dokumen digital. Salah satu cara efektif adalah dengan memberikan tandatangan digital.

Digital signature bukanlah tandatangan manual yang di digitalkan, melainkan sebuah pengkodean yang di dapat dari proses *Digital Signature Algorithm* (DSA). DSA menggunakan kunci publik dan kunci privat untuk membuat dan memverifikasi tandatangan digital.

Permasalahan utama pada penelitian ini tentang keamanan, pemilihan kunci DSA memerlukan dua bilangan prima yang besar untuk pembangkitan kunci. Keamanan DSA bergantung pada kerahasiaan kunci privat. Jika kunci privat

bocor, maka tandatangan digital dapat dipalsukan. Setelah itu DSA menggunakan fungsi hash untuk menghitung nilai menjadi faktor penting dalam efisiensi keseluruhan sistem. Penggunaan fungsi hash yang lebih lambat dapat memperlambat proses penandatanganan dan verifikasi.

Teknologi merupakan sesuatu hal yang sangat kita butuhkan saat ini terutama pada kehidupan kita sehari-hari. Hal ini dapat terjadi karena dengan teknologi manusia dapat melakukan pekerjaan yang efektif dan efisien. Salah satu penerapan dari teknologi yaitu tandatangan digital pada suatu berkas, dimana saat ini proses tandatangan banyak yang masih menggunakan tandatangan basah atau yang bisa kita sebut dengan manual, sebagian orang juga menggunakan tandatangan digital dengan menggunakan teknik memfoto tandatangan basah kemudian menempel atau memasukkan gambar tandatangan tersebut kedalam berkas yang akan ditandatangani (Alwan and Qomariasih 2024). Dengan perkembangan teknologi, dokumen tidak hanya diproduksi dalam bentuk cetak, tetapi juga dalam bentuk digital. Dokumen digital memiliki kelebihan seperti lebih mudah dan efisien dalam penggunaannya, namun juga lebih rentan terhadap modifikasi atau pemalsuan.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang diatas, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana menerapkan algoritma DSA *(Digital Signature Algorithm)* dalam sistem pengamanan dokumen digital?
2. Bagaimana mengamankan dokumen digital pada aplikasi digital *signature* dalam bentuk tandatangan digital berbasis *QR-Code*?

1.3 Batasan Masalah

Agar pembahasan lebih terarah dan sesuai dengan judul yang telah ditentukan, penulis hanya membahas pokok-pokok bahasan sebagai berikut:

1. Aplikasi yang dibangun merupakan aplikasi berbasis *GUI tkinter*.
2. Pembuatan aplikasi menggunakan bahasa pemrograman *python*.
3. Dokumen yang akan digunakan dalam penelitian jenis dokumen dalam format pdf.
4. Menggunakan algoritma DSA (*Digital Signature Algorithm*).
5. Aplikasi ini memvalidasi tandatangan digital pada dokumen menggunakan *QR-Code.*

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Menerapkan algoritma *Digital Signature Algorithm* (DSA) sebagai metode untuk pengamanan dokumen digital, guna meningkatkan keaslian dan integritas data.
2. Menggunakan pasangan kunci yang dihasilkan oleh DSA (*Digital Signature Algorithm*).

1.5 Manfaat Penelitian

Adapun manfaat penelitian ini adalah sebagai berikut:

1. Dapat meningkatkan keamanan dokumen digital melalui penerapan algoritma DSA (*Digital Signature Algorithm*) .
2. Tandatangan yang dihasilkan dari algoritma ini dapat digunakan untuk membuktikan bahwa dokumen berasal dari pengirim yang sah.

1.6 Metodologi Penelitian

Metodologi penelitian yang digunakan pada penelitian ini adalah:

1. Studi Kepustakaan

   Pada tahap ini dilakukan studi kepustakaan yaitu proses mengumpulkan informasi dengan melakukan pengumpulan, mempelajari, dan membaca berbagai bahan referensi yang berkaitan dengan aplikasi, algoritma serta DSA *(Digital Signature Algorithm).*

2. Analisis dan Perancangan

   Pada tahap ini dilakukan analisis spesifikasi aplikasi dan melakukan perancangan aplikasi, seperti perancangan proses dan antarmuka yang meliputi desain database, sketsa, dan lain sebagainya.

3. Pengkodean

   Pada tahap ini dilakukan pengkodean aplikasi sesuai dengan analisis spesifikasi dan perancangan yang telah ditentukan.

4. Pengujian Aplikasi

   Pada tahap ini dilakukan pengujian terhadap aplikasi yang telah dibangun, dan tingkat keakuratan dari sistem aplikasi yang telah dibuat.

5. Penyusunan Laporan

   Pada tahap ini dilakukan penulisan dokumentasi dan laporan dari aplikasi yang dikembangkan.

1.7 Sistematika Penulisan

Sistematika penulisan tugas skripsi ini dibagi atas beberapa bab, di mana masing-masing bab dibagi atas beberapa sub agar mempermudah penjelasan mengenai penelitian yang dilakukan dan mempermudah pembaca dalam memahami isi penelitian. Adapun sistematika penulisan tugas skripsi ini adalah sebagai berikut:

BAB 1 PENDAHULUAN

Pendahuluan berisi tentang Latar Belakang Masalah, Rumusan Masalah, Tujuan, Manfaat, Batasan Masalah, Metodologi Penelitian dan Sistematika Penulisan dalam pembuatan Tugas Skripsi.

BAB 2 TINJAUAN PUSTAKA

Bab ini berisi teori-teori pengetahuan dasar yang di peroleh dari studi kepustakaan atau literatur dan dokumentasi *internet* yang digunakan untuk memahami permasalahan yang dibahas pada penelitian ini. Teori-teori pengetahuan dasar yang disajikan antara lain tentang kriptografi, dokumen serta algoritma DSA *(Digital Signature Algorithm).*

BAB 3 METODE PENELITIAN

Bab ini menguraikan tahapan-tahapan sistematis yang digunakan untuk melakukan kajian penelitian. Tahapan-tahapan tersebut merupakan kerangka yang dijadikan pedoman penelitian untuk mencapai tujuan yang telah ditetapkan.

BAB 4 HASIL DAN PEMBAHASAN

Bab ini berisi tentang hasil dan pembahasan dari aplikasi implementasi algoritma DSA *(Digital Signature Algorithm)* dalam pengamanan dokumen digital.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari keseluruhan uraian bab-bab penulisan skripsi dan saran yang diajukan untuk pengembangan lebih lanjut.

BAB II

TINJAUAN PUSTAKA

2.1 Kriptografi

Kriptografi (*Cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan *graphia*. Kripto artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi (M.Miftakul 2016).

Kriptografi juga merupakan ilmu menjaga kerahasiaan pesan dengan cara menyandikannya dalam bentuk yang tidak dapat dipahami lagi. Dalam kriptografi terdapat dua proses yaitu enkripsi dan dekripsi. Pesan terenkripsi disebut *plaintext*. Disebut demikian karena informasi ini dapat dengan mudah dibaca dan dipahami oleh siapa saja. Algoritma yang digunakan untuk mengenkripsi dan mendekripsi *plaintext* melibatkan pengguna beberapa bentuk kunci. Pesan eksplisit dengan *ciphertext* disebut *ciphertext* dalam pengkodean (Azhari et al. 2022).

2.1.1 Enkripsi dan Dekripsi

Enkripsi adalah proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu (Muharram et al. 2018).

Sedangkan dekripsi merupakan kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Dekripsi adalah suatu proses mengubah sebuah pesan, data atau informasi yang tidak dapat dibaca menjadi sebuah informasi yang dimengerti dan dapat dibaca (Ajhari and Windarto 2018).

2.2 Validasi

Validasi merupakan proses penentuan apakah model konseptual simulasi benar-benar merupakan representasi akurat dari sistem nyata yang dimodelkan. Validasi model dapat pula dikatakan sebagai langkah dalam memvalidasi atau menguji apakah model yang telah disusun dapat merepresentasikan sistem nyata dengan benar. Validasi dapat dilakukan dengan menggunakan alat uji statik yang meliputi uji keseragaman data *output*, uji kesamaan dua rata-rata, uji kesamaan dua variansi dan uji kecocokan distribusi (Permana 2019).

2.3 Dokumen

Dokumen adalah berkas asli yang dipergunakan sebagai alat pembuktian atau sebagai bahan untuk mendukung suatu keterangan. Dijelaskan lebih lanjut bahwa istilah dokumen dalam dunia pengusaha di luar negeri, misalnya di Amerika Serikat, diartikan sama dengan *record* atau berkas asli. Dalam perkembangan selanjutnya istilah dokumen berarti naskah-naskah asli yang telah didaftar secara sah menurut ketentuan-ketentuan dalam suatu peraturan (piagam atau perjanjian) (Nugrohoadhi 2015).

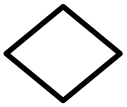
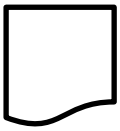
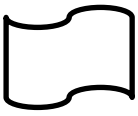
2.4 *Flowchart*

Flowchart atau sering disebut dengan diagram alir merupakan suatu jenis diagram yang merepresentasikan algoritma atau langkah-langkah instruksi yang berurutan dalam sistem. Seorang analis sistem menggunakan *flowchart* sebagai bukti dokumentasi yang menjelaskan gambaran logis sebuah sistem yang akan dibangun kepada programmer. Dengan begitu, *flowchart* dapat membantu untuk memberikan solusi terhadap masalah yang bisa saja terjadi dalam membangun sistem. Pada dasarnya, *flowchart* digambarkan dengan menggunakan simbol-simbol. Setiap simbol mewakili suatu proses tertentu. Sedangkan untuk menghubungkan suatu proses ke proses selanjutnya digambarkan dengan menggunakan garis penghubung. Dengan adanya *flowchart*, setiap urutan proses dapat digambarkan menjadi lebih jelas. Selain itu, ketika ada penambahan proses baru dapat dilakukan dengan mudah menggunakan *flowchart* ini. Setelah proses membuat *flowchart* selesai, maka giliran programmer yang akan menerjemahkan desain logis tersebut kedalam bentuk program dengan berbagai bahasa pemrograman yang telah disepakati (Rosaly and Prasetyo 2020).

Adapun arti dari simbol *flowchart* terdapat pada tabel 2.1

Tabel 2.1 Arti simbol *Flowchart*

Simbol	Arti
Input / *Output* 	Mempresentasikan *input* data atau *output* data yang diproses atau informasi
Proses 	Mempresentasikan Operasi

Penghubung 	Keluar ke atau masuk dari bagian lain *flowchart* khususnya halaman yang sama
Anak Panah 	Mempresentasikan alur kerja
Keputusan 	Keputusan dalam program
Predefined 	Rincian operasi berada di tempat lain
Preparation 	Pemberian harga awal
Punched Card 	*Input* / *Output* yang menggunakan kartu berlubang
Dokumen 	*Input* / *Output* dalam format yang dicetak
Magnetic Disk 	*Input* / *Output* yang menggunakan *Disk Magnetic*
Magnetic Drum 	*Input* / *Output* yang menggunakan *Drum Magnetic*
Punched Tape 	*Input* / *Output* yang menggunakan pita kertas berlubang

Manual Input 	*Input* yang dimasukkan secara manual dari *keyboard*
Display 	*Output* yang ditampilkan pada terminal
Manual Operation 	Operasi Manual

Sumber: (Rosaly and Prasetyo 2020).

2.5 Bahasa Pemrograman *Python*

Python adalah bahasa pemrograman yang fleksibel dan dapat digunakan untuk berbagai jenis tujuan seperti pengembangan perangkat lunak, pengembangan *web*, data *science*, dan lain sebagainya. *Python* awalnya dirancang sebagai bahasa pemrograman skrip *(scripting language)* untuk otomatisasi tugas-tugas administratif dan pengembangan aplikasi *web*. Namun, seiring berjalannya waktu, *python* telah berkembang menjadi bahasa pemrograman yang popular di berbagai bidang, termasuk pengembangan *web*, analisis data, kecerdasan buatan, pengembangan *game*, dan banyak lagi.

Python merupakan salah satu bahasa pemrograman yang mudah untuk dipelajari dibandingkan dengan bahasa pemrograman lainnya, karena *python* memiliki kaidah penulisan dan sintaks yang mudah dipahami dan dipelajari bahkan untuk seorang pemula untuk programmer bahasa ini sering dijadikan bahasa favorit. Kode dan sintaks pada *python* mudah dipahami karena mirip dengan bahasa manusia. Hal ini dapat memudahkan pengguna untuk mengenali

dan menyempurnakan sintaks dan kode yang ditulis. *Python* adalah bahasa pemrograman bersifat *open source*, yang artinya siapapun dapat dengan bebas menggunakannya, memodifikasi, dan mendistribusikan bahasa pemrograman *python*. *Python* memiliki pilihan perpustakaan yang lengkap dan beragam tergantung pada kebutuhan yang diinginkan (P. Rosyani, A. Riski 2023).

2.6 *QR-Code*

QR-Code merupakan teknik yang mengubah data tertulis menjadi kode-kode 2 dimensi yang tercetak kedalam suatu media yang lebih ringkas. *QR-Code* mampu mempunyai semua jenis data, seperti data angka/numerik, *alphanumeric*, biner. Selain itu *QR-Code* memiliki tampilan yang lebih kecil daripada *barcode.* Hal ini dikarenakan *QR-Code* mampu menampung data secara horizontal dan vertikal, jadi secara otomatis ukuran dari tampilan gambar *QR-Code* bisa hanya sepersepuluh dari sebuah *barcode*. Tidak hanya itu *QR-Code* juga tahan terhadap kerusakan, sebab *QR-Code* mampu memperbaiki kesalahan sampai dengan 30% tergantung dengan ukuran atau versinya. Oleh karena itu, walaupun sebagian simbol *QR-Code* kotor ataupun rusak, data tetap dapat disimpan dan dibaca (Musthofa et al. 2016).

Gambar 2.1 Contoh Gambar *QR-Code*

Sumber Gambar: https://barcodesindonesia.com/contoh-gambar

2.7 Dokumen Digital

Dokumen digital merupakan setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, huruf, angka, kode akses, simbol yang memiliki makna atau arti dapat dipahami oleh orang yang mampu memahaminya. Dokumen digital dapat dihasilkan dengan menggunakan apliksi pengolah kata *(word processor)* seperti *Microsoft Word*, *Notepad* atau *OpenOffice* untuk mengahsilkan sebuah berkas komputer ekstensi yang berbeda-beda sesuai dengan aplikasi pengolah kata yang digunakan (Hermawan and Ismiati 2020).

2.8 *Digital Signature*

Digital Signature (Tandatangan Digital) adalah suatu tandatangan yang dibuat secara elektronik yang berfungsi sama dengan tandatangan biasa pada dokumen kertas biasa. Tandatangan adalah data yang apabila dipalsukan, dapat berfungsi untuk menyatakan bahwa orang yang namanya tertera pada suatu dokumen setuju dengan apa yang tercantum pada dokumen yang ditandatanganinya itu (Rehulina 2018).

Dengan menggunakan *Digital Signature* keamanan sistem informasi sangat penting untuk menjaga integritas dan keaslian dari suatu dokumen. *Digital Signature* dapat memverifikasi keaslian dari dokumen dan dapat mengetahui isi dokumen tersebut sudah diubah atau belum (Taqiyyah and Adriansyah 2020).

2.9 DSA *(Digital Signature Algorithm)*

DSA *(Digital Signature Algorithm)* merupakan salah satu kriptografi kunci publik yang digunakan untuk otentikasi, pengamanan data dan memastikan kebenaran atau keaslian suatu data. Pada DSA dibutuhkan program khusus untuk

membangkitkan kunci dan masalah yang timbul adalah kepercayaan pengguna pada program tersebut. Algoritma DSA dirancang untuk menjaga lawan *(attacker)* yang diasumsikan tidak tahu kunci privat *signer* yang digunakan untuk membangkitkan tandatangan digital. Menurut peneliti, pengguna parameter, kunci publik dan privat yang tetap untuk suatu waktu tertentu dan diperpanjang untuk periode waktu tertentu, merupakan celah ketidakamanan penggunaan algoritma DSA. Karena pihak *attacker* mempunyai kesempatan dan waktu seiring dengan kecepatan *processor* yang semakin bertambah. Maka dari itu perlu dibangun aplikasi kriptografi dengan metode DSA *(Digital Signature Algorithm)* yang dapat membangkitkan kunci secara dinamis walaupun dengan masukan yang sama. Hal ini menjadi salah satu solusi dalam hal manajemen kunci (Sarjana and Diponegoro 2011).

2.8.1 Tujuan DSA*(Digital Signature Algorithm)*

DSA memiliki dua tujuan utama, yaitu:

1. Pembentukan tandatangan *(signature generation)*
2. Pemeriksaan keabsahan tandatangan *(signature verification)* (Alfani et al. 2024).

2.8.2 Keunggulan Dan Kekurangan DSA (*Digital Signature Algortihm*)

Keunggulan yang dimiliki algoritma DSA yaitu mempunyai verifikasi terhadap pengguna sehingga dapat menjaga keaslian pesan. Sedangkan kekurangan yang dimiliki algoritma DSA yaitu pada keamanan kunci bergantung pada keamanan komputer, operasional memakan daya besar, dan masalah legalitas (Rochman 2016).

Contoh perhitungan DSA (Digital Signature Algorithm),yaitu:

1. Membuat sepasang kunci:

   Pilih bilangan prima p dan q, dengan persamaan

   (p -1) mod q = 0 … (2.1)

g = $h^{(p-- 1)/q}$ mod p ... (2.2)

   < h < p – 1 dan $h^{(p-- 1)/q}$ mod p > 1 … (2.3)

   x < q = merupakan kunci privat

   y = g^{x} mod p = kunci publik

2. Proses pembuatan tandatangan

   k < q = bilangan acak

r = (g^{x} mod p) mod q … (2.4)

s = (k^{-1}(H(m) + x * r)) mod q. k^{-1} … (2.5)

   yaitu invers k mod q

   (r,s): tandatangan digital

3. Proses pembuktian tandatangan (verifikasi)

   W = s^{-1} mod q

   u1 = (H(m) * w) mod q

   u2 = ((g^{u1} * y^{u2}) mod p) mod q

   jika v = r, maka tandatangan terbukti asli(Eritza et al. 2022).

Keterangan Simbol DSA *(Digital Signature Algorithm)*

p= Bilangan prima besar

q= Bilangan prima kecil

g= Nilai yang dihitung dengan rumus:

$$g = h^{(p-1)/q} \bmod p$$

h= Bilangan acak perantara

x= Kunci privat

y= Kunci publik

H (m)= Hash pesan

K= Bilangan acak sementara

r,s= Komponen tandatangan digital

w, u_1, u_2, v= Nilai perantara dalam proses verifikasi.

2.9 Penelitian Terdahulu

Pada penelitian (Pardosi and Purba 2015) yang berjudul Pemeriksaan Integritas Dokumen Dengan *Digital Signature Algorithm* mengidentifikasi keraguan akan keaslian dokumen digital yang sudah ditandatangani. Penerima dokumen digital perlu sebuah *digital identifier* yang menyatakan bahwa dokumen tersebut memang berasal dari pengirim, bukan dari pihak lain yang tidak bertanggung jawab. Setelah permasalahan dapat diidentifikasi, maka tahap berikutnya yaitu analisa kebutuhan dan desain sistem. Hal yang dibutuhkan adalah sebuah antarmuka yang dapat dipergunakan dari sisi pengirim maupun penerima dokumen. Pengirim dapat mengirimkan dokumen dan disertai dengan *key* yang telah di *generate* oleh aplikasi. Dari sisi penerima, penerima dapat memverifikasi

dokumen dan *key* yang diberikan pengirim. Jika *key* milik penerima dan pengirim cocok, maka dokumen yang dikirimkan dapat diakui keabsahannya.

Sedangkan pada penelitian (Yuniati and Sidiq 2020) metode yang digunakan adalah *literature review* pada *paper* yang terkait dengan legalisasi dokumen elektronik menggunakan tandatangan digital. Langkah-langkah dari *literature review* meliputi 4 tahapan, yaitu: (1) formulasi permasalahan, (2) pencarian *literature,* (3) evaluasi data, serta (4) analisis dan interpretasi. Topik yang dipilih adalah mengenai tandatangan digital dan legalisasi dokumen elektronik. Langkah selanjutnya adalah pencarian *literature* yang relevan dengan topik penelitian. Langkah ini dapat memberikan gambaran mengenai tandatangan digital dan legalisasi dokumen elektronik. Proses pencarian dan pengumpulan artikel atau jurnal penelitian dilakukan menggunakan *Google Scholar, IEEE Xplore,* dan *Science Direct* dengan kata kunci "legalisasi dokumen elektronik", "tandatangan digital" dan *"digital signature*". Langkah ketiga adalah evaluasi data, yaitu dengan menyaring memilih dan memilah artikel jurnal yang benar-benar relevan dan baru. Relevansi dilihat dari kesesuaian judul *paper* dengan topik penelitian, yaitu mengenai legalisasi dokumen elektronik menggunakan tandatangan digital. Setelah keempat tahapan tersebut dilakukan, proses selanjutnya adalah pelaksanaan *literature review*. Adapun cara melakukan *literature review* yaitu: mencari kesamaan (*compare*), mencari ketidaksamaan (*contrast*), memberikan pandangan (*criticize*), membandingkan (*synthesize*), dan meringkas (*summarize*).