# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang Masalah

Dokumen digital merupakan suatu data dan informasi yang dibuat, diteruskan, dikirim, diterima, ataupun disimpan dalam bentuk analog, optikal, elektromagnetik, digital, atau sejenisnya, yang dapat dilihat, ditampilkan, dan didengar melalui komputer atau sistem elektronik. Tidak hanya terbatas pada tulisan, dokumen digital juga dapat berupa suara, gambar, peta, rancangan, huruf, tanda, angka, kode akses, atau simbol yang memiliki makna dan arti, serta dapat dipahami oleh orang yang mampu memahaminya (Hermawan & Ismiati, 2020). Dengan adanya digitalisasi dokumen ini, diharapkan dapat memberikan kemudahan akses dan membuat waktu pengiriman lebih efisien, tanpa harus bertatap muka. Namun, tak jarang digitalisasi dokumen ini juga memberikan beberapa kerugian, salah satunya adalah pengubahan isi konten dokumen oleh oknum yang tidak berkepentingan. Dengan memuat data dan informasi, tentu saja dokumen digital dapat dijadikan sebagai bukti atau keterangan. Mengingat sangat pentingnya peran dokumen digital, dibutuhkan suatu kegiatan untuk memeriksa apakah dokumen tersebut masih asli atau sudah diubah oleh pihak yang tidak bertanggung jawab. Salah satu keilmuan yang dapat digunakan untuk memeriksa keaslian suatu pesan adalah kriptologi.

Kriptologi adalah studi mengenai kriptografi dan kriptanalisis. Kriptografi adalah sebuah ilmu dan seni yang bertujuan untuk menjaga keamanan suatu pesan yang akan dikirim dengan cara mengubahnya menjadi sekumpulan kode acak sehingga pesan asli tidak diketahui oleh pihak ketiga (Sumandri, 2017). Sementara itu, kriptanalisis adalah usaha untuk mendapatkan pesan asli dari pesan sandi yang tidak diketahui sistem dan kuncinya. Sebuah pesan dapat dikatakan aman ketika memenuhi tiga prinsip dasar yang disebut dengan Triad CIA, yaitu *Confidentiality* (kerahasiaan), *Integrity* (integritas data), dan *Availability* (ketersediaan). Lebih lanjut, terdapat lima aspek keamanan lainnya, yaitu *Authentication*, *Non-repudiation*, *Authority*, *Privacy*, dan *Access Control* (Sari dkk., 2020). Terdapat berbagai algoritma dalam kriptografi yang bertujuan untuk mengamankan pesan, mulai dari kriptografi klasik hingga modern. Algoritma kriptografi *Rivest Shamer*

*Adleman* dan fungsi hash merupakan salah satu gabungan algoritma yang dapat dipakai untuk membuat tanda tangan digital serta melakukan autentikasi terhadap sebuah pesan (Atika, 2018).

RSA merupakan algoritma kriptografi kunci publik (asimetri) yang mempunyai dua buah kunci, yaitu kunci publik dan kunci rahasia, dengan menggunakan konsep dasar bilangan prima dan aritmatika modulo. Baik kunci enkripsi maupun kunci dekripsi, keduanya menggunakan bilangan bulat. Meskipun terdengar cukup mudah untuk dilakukan, tetapi memfaktorkan bilangan bulat menjadi faktor primanya bukanlah pekerjaan yang sederhana. Penemu algoritma RSA menyarankan bilangan yang digunakan memiliki panjang yang lebih dari 100 digit sehingga hasil kalinya akan berukuran lebih dari 200 digit. Semakin besar bilangan yang difaktorkan, semakin lama waktu yang dibutuhkan karena semakin sulit pemfaktorannya sehingga semakin kuat pula algoritma RSA. Hal tersebut menjadi salah satu kekuatan dan keamanan algoritma RSA sehingga tetap direkomendasikan untuk menyandikan pesan (Ginting dkk., 2015). Dalam pembuatan tanda tangan dan proses autentikasi sebuah pesan, algoritma RSA sering digabungkan dengan fungsi hash.

Fungsi hash adalah sebuah fungsi yang dapat menerima masukan *string* apa saja, di mana dilakukan pemetaan dari pesan yang memiliki panjang sembarang ke dalam sebuah teks khusus (*message digest*) dengan panjang tetap. Fungsi hash merupakan algoritma yang dapat dipakai untuk mengubah informasi dengan memasukan data yang akan diolah menjadi angka, huruf, atau karakter lain menjadi karakter terenkripsi tanpa mengubah ukuran, serta tak bisa dikembalikan lagi (*One Way Function* atau enkripsi satu arah). Setiap pesan memiliki nilai hash yang berbeda. Pada versi SHA-2, terdapat fungsi hash dengan ukuran *digest* 256 yang menggunakan beberapa logika kombinasi dasar, seperti AND, OR, XOR, pergeseran bit ke kanan (*shift right*), dan rotasi ke kanan (*rotate right*), yang disebut SHA-256 (*Secure Hash Algorithm*-256) (Sulastri & Putri, 2018).

Terdapat beberapa penelitian terdahulu yang sudah menggabungkan algoritma kriptografi RSA dan fungsi hash SHA untuk pembuatan tanda tangan digital, baik dengan tujuan pengamanan data maupun autentikasi pesan. Pada tahun 2018, Sugiyatno dan Atika melakukan sebuah penelitian berjudul “Digital

Signature dengan Algoritma SHA-1 dan RSA sebagai Autentikasi" yang menyimpulkan bahwa algoritma RSA dan SHA-1 dapat dikombinasikan dengan baik dalam membuat sebuah tanda tangan digital pada file PDF, serta terbukti mampu diandalkan dalam autentikasi file dari tindak pemalsuan dan modifikasi data. Namun, Wang dkk. (2005) telah menemukan kolisi pada SHA-1 dengan mengubah kompleksitas dari $2^{80}$ menjadi $2^{69}$. Hal itu membuat SHA-1 dianggap sudah tidak aman dan tidak disarankan untuk digunakan kembali.

Pada tahun 2022, Melina dkk. melakukan penelitian yang berjudul "Verifikasi Tanda Tangan Elektronik dengan Teknik Otentikasi Berbasis Kriptografi Kunci Publik Sistem Menggunakan Algoritma Kriptografi *Rivest-Shamir-Adleman*" dengan simpulan bahwa verifikasi tanda tangan digital dengan algoritma RSA adalah metode yang sangat tepat untuk menjamin keaslian suatu dokumen. Pada tahun yang sama, Fachrul dkk. melakukan penelitian mengenai "Penerapan Konsep *Digital Signature* terhadap Verifikasi Keaslian Dokumen Transkrip Nilai Mahasiswa menggunakan Enkripsi *Rivest Shamir Adleman*" yang menyimpulkan bahwa waktu yang dibutuhkan sistem untuk proses enkripsi dan dekripsi akan semakin lama apabila kunci yang digunakan semakin tinggi. Selain itu, Fachrul dkk. juga menyarankan untuk melakukan sebuah pengembangan dalam proses verifikasi dengan menggunakan QR Code (*Quick Response Code*).

Firdaus dkk. (2017) melakukan sebuah penelitian berjudul "Penyandian Pesan Menggunakan Kombinasi Algoritma RSA yang Ditingkatkan dan Algoritma ElGamal" dengan kesimpulan bahwa terdapat perbedaan antara proses pembangkitan kunci algoritma RSA standar dengan RSA yang ditingkatkan sehingga menyebabkan durasi proses enkripsi dan dekripsi menjadi lebih cepat. Kecepatan algoritma kriptografi RSA ditingkatkan melalui penambahan satu buah bilangan prima pada proses pembangkitan kunci. Algoritma RSA standar umumnya menggunakan dua buah bilangan prima, tetapi Firdaus dkk. meningkatkan algoritma RSA standar dengan cara menambahkan satu buah bilangan prima lain yang berbeda sehingga membutuhkan tiga buah bilangan prima.

Beberapa penelitian terdahulu terkait penggabungan algoritma kriptografi RSA dan QR Code, di antaranya dilakukan oleh Sarasvananda dan Iswara (2022) yang mengkaji tentang pembuatan tanda tangan elektronik pada sistem informasi

surat menyurat LPIK INSTIKI dalam mengamankan keaslian dokumen surat dan mempermudah proses tanda tangan dengan skema QR Code untuk menampung kode tanda tangan RSA yang cukup panjang sehingga dapat disisipkan pada dokumen surat. Penelitian lainnya dilakukan oleh Hendrawaty dkk. (2016) yang mengkaji tentang perancangan sistem keamanan pada transkrip nilai sehingga isinya tidak mudah dipalsukan atau dimodifikasi dan proses verifikasi keasliannya dapat dilakukan dengan cepat, mudah, serta secara *offline* menggunakan *smartphone* berbasis android. Penelitian yang dilakukan oleh Pangan dkk. (2022) mengkaji tentang langkah keamanan untuk transfer data melalui kartu vaksinasi dan menghasilkan VacciFied.net, Sistem Pencatatan COVID-19 Terpusat dengan melibatkan proses transfer data yang diautentikasi. Penelitian yang dilakukan oleh Ikhsan (2022) mengkaji tentang penggunaan QR Code dengan algoritma RSA standar untuk akses masuk kampus atau area umum lainnya. Perbedaan penelitan terdahulu dengan penelitian yang akan dilakukan terletak pada penggunaan bahasa pemrograman, kombinasi fungsi hash, jenis RSA, tujuan penelitian, dan basis program aplikasi.

Berdasarkan pemaparan tersebut, penulis terdorong untuk melakukan sebuah kajian terkait implementasi program aplikasi Python untuk autentikasi tanda tangan pada dokumen digital dengan QR Code menggunakan fungsi hash SHA-256 dan algoritma RSA yang ditingkatkan. Maka dari itu, judul yang diambil dalam penelitian ini adalah "Penggunaan QR Code dalam Autentikasi Tanda Tangan pada Dokumen Digital dengan Algoritma Secure Hash Algorithm-256 (SHA-256) dan Rivest Shamir Adleman (RSA) yang Ditingkatkan".

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, penelitian ini mengangkat beberapa rumusan masalah, yaitu:

1. Bagaimana skema autentikasi tanda tangan pada dokumen digital dengan QR Code menggunakan SHA-256 dan RSA yang ditingkatkan?
2. Bagaimana hasil konstruksi program aplikasi GUI Python untuk memeriksa keaslian tanda tangan pada dokumen digital dengan QR Code menggunakan SHA-256 dan RSA yang ditingkatkan?

## 1.3 Tujuan Penelitian

Dilihat dari rumusan masalah, terdapat beberapa tujuan dilaksanakannya penelitian ini, yaitu:

1. Mengidentifikasi skema untuk autentikasi tanda tangan pada dokumen digital dengan QR Code menggunakan SHA-256 dan RSA yang ditingkatkan.
2. Mengonstruksi program aplikasi GUI Python untuk memeriksa keaslian tanda tangan pada dokumen digital dengan QR Code menggunakan SHA-256 dan RSA yang ditingkatkan.

## 1.4 Batasan Masalah

Terdapat beberapa batasan pada penelitian ini, yaitu:

1. Dokumen yang digunakan berbentuk PDF (*Portable Document Format*) dan bukan hasil *scan* yang disimpan dalam format PDF.
2. Hasil QR Code berbentuk JPG (*Joint Photographic experts Group*).

## 1.5 Manfaat Penelitian

Adapun beberapa manfaat dari penelitian ini, yaitu:

1. Manfaat Teoritis

   Secara teoritis, diharapkan penelitian ini dapat memberikan pemahaman mengenai penggunaan QR Code serta algoritma kriptografi SHA-256 dan RSA yang ditingkatkan dalam autentikasi tanda tangan pada digital.

2. Manfaat Praktis

   Secara praktik, penelitian ini akan menghasilkan sebuah program aplikasi GUI Python yang *user-friendly* untuk memeriksa keaslian tanda tangan pada dokumen digital dengan memanfaatkan QR Code serta algoritma kriptografi SHA-256 dan RSA yang ditingkatkan.