BAB I
PENDAHULUAN

1.1. Latar Belakang

Dengan kemajuan modernisasi, tingkat risiko kejahatan cenderung meningkat. Hal ini mendorong perlunya perubahan sistem, baik sebagian maupun keseluruhan, dari yang bersifat konvensional menjadi digital secara bertahap dan signifikan. Salah satu dampak kecil dari kejahatan tersebut adalah terkait dokumentasi. Kejahatan terhadap dokumentasi seringkali melibatkan pemalsuan dokumen, yang dapat merugikan pihak yang terkena dampak. Contohnya adalah tindakan pemalsuan tanda tangan dengan maksud untuk mencuri hak korban demi kepentingan pelaku. Tercatat sebanyak 301.098 kasus pelanggaran yang terkait dengan kata kunci "Pemalsuan Dokumen" [1].

Pada tahun 2019 terdapat kasus pemalsuan tanda tangan pada surat jual beli tanah yang menyebabkan seseorang kehilangan hak atas tanahnya dan menimbulkan kerugian [2]. Sebagai contoh pelanggaran dokumentasi lain, mantan bupati Sragen, Untung Wiyono, menggunakan ijazah Sekolah Menengah Atas (SMA) palsu ketika mencalonkan diri sebagai bakal calon Bupati Sragen pada Pemilihan Kepala Daerah (Pilkada) 2000-2006. Ijazah palsu tersebut adalah ijazah SMA Sembada tahun 1971 bernomor seri LAA 001054, yang ternyata dimiliki oleh Ratna Hidayat dari SMA Negeri 6 Jakarta [3]. Permasalahan ini juga muncul karena penggunaan bentuk fisik dokumen yang keamanannya sudah sangat berisiko.

Bukan hanya karena pertimbangan keamanan, penggunaan bentuk fisik dokumen ini juga semakin berkurang berkat kampanye ramah lingkungan dan efisiensi yang ditawarkan oleh teknologi saat ini. Program atau sistem yang menggantikan penggunaan kertas dalam bentuk fisik dengan konsep "*paperless office"*, seperti tata naskah dinas elektronik yang telah diterapkan di beberapa internal instansi atau perusahaan, menjadi semakin umum. Meskipun bentuk *paperless office* ini mengalami beberapa perubahan dalam sistem keamanan, prinsip dasarnya tetap sama dengan dokumen dalam bentuk fisik atau kertas.

Tanda tangan adalah satu bentuk identifikasi dan otorisasi yang paling umum digunakan dalam berbagai transaksi dan dokumen resmi di berbagai negara di seluruh dunia.Simbol ini mencakup berbagai bentuk seperti paraf, tanda tangan dengan tulisan lengkap, cap tanda tangan, cap paraf, cap nama, atau bentuk lain yang berfungsi sebagai pengganti tanda tangan. Penggunaan tanda tangan telah ada sejak zaman kuno dan tetap relevan hingga saat ini karena merupakan tanda kesepaktan dan persetujuan secara hukum antara pihak–pihak terlibat. Selain itu, tanda tangan elektronik juga diakui sebagaimana dijelaskan dalam undang-undang tentang informasi dan transaksi elektronik [4].

Seiring dengan kemajuan teknologi dan kebutuhan akan efisiensi dalam berbagai sektor, penggunaan tanda tangan tradisional secara manual mulai menemui kendala. Proses tanda tangan konvensional sering kali membutuhkan waktu dan sumber daya yang signifikan, terutama dalam lingkup transaksi dan bisnis yang melibatkan pihak yang berlokasi di berbagai wilayah geografis. Di sinilah kebutuhan untuk mengadopsi tanda tangan digital muncul sebagai solusi yang praktis dan canggih. Tanda tangan digital adalah bentuk tanda tangan elektronik yang telah ditingkatkan tingkat keamanannya dan diakui secara hukum untuk berbagai transaksi dan proses digital.

Dengan keamanan yang terintegrasi dalam mekanisme tanda tangan digital, berbagai sektor mulai mengadopsi dan mengandalkan teknologi ini dalam berbagai proses bisnis dan transaksi online. Perbankan, perusahaan, keuangan, kantor pemerintahan, hingga sektor Kesehatan semuanya telah beralih ke penggunaan tanda tangan digital untuk meningkatkan efisiensi, mengurangi biaya operasional, dan memberikan kepercayaan pada pelanggan serta pihak terkait. Tanda tangan digital tidak hanya menghemat waktu, tetapi juga memberikan tingkat keamanan yang lebih tinggi dibandingkan tanda tangan tradisional, karena setiap tanda tangan digital memiliki informasi yang khusus dan unik yang tidak dapat dipalsukan. Hal tersebut menjadikan tanda tangan digital sebagai aspek kritis dalam dunia digital yang memberikan kepastian dan integritas terhadap dokumen elektronik serta transaksi daring. Dalam era digital yang semakin berkembang, kebutuhan akan metode tangan

yang aman dan efisien menjadi semakin mendesak. RSA (Rivest-Shamir-Adleman), Chaca20, dan SHA-3 (Secure Hash Algorithm 3) adalah tiga algoritma kriptografi yang telah terbukti efektif dalam mengamankan data dan digunakan secara luas untuk berbagai aplikasi keamanan [5].

Algoritma RSA (Rivest-Shamir-Adleman) adalah metode kriptografi yang pertama kali dikembangkan oleh tiga ilmuwan, yaitu Ron Rivest, Adi Shamir, dan Len Adleman,di Institut Teknologi Massachussets(MIT) pada tahun 1978. Keamanan algoritma RSA didasarkan pada kesulitan dalam memecahkan masalah faktorisasi bilangan bulat besar menjadi faktor – faktor primanya. Semakin besar bilangan prima yang digunakan dalam algoritma ini, semakin tinggi tingkat keamanan yang dihasilkan. RSA melibatkan proses perkalian antara dua bilangan prima besar, yang kemudian melibatkan operasi matematika lain untuk menghasilkan dua kunci, yaitu kunci pribadi *(private key)* dan kunci publik *(public key)*. Penggunaan kunci yang berbeda untuk melakukan enkripsi dan dekripsi membantu meningkatkan tingkat keamanan dan potensi peretasan atau penemuan kunci RSA [6].

Algoritma Chacha20 adalah sebuah algoritma enkripsi simetris yang populer dan efisien, digunakan untuk mengamankan data dalam berbagai aplikasi, termasuk komunikasi melalui internet dan penyimpanan data. Algoritma ini dikembangkan oleh Daniel J. Bernstein pada tahun 2008 dan merupakan varian dari algoritma Salsa20 yang juga dikembangkan olehnya [7].Chacha20 telah menonjol sebagai pilihan populer untuk implementasi enkripsi karena kombinasi kecepatan dan keamanannya yang unggul. Dengan perangkat keras modern yang mendukung instruksi SIMD (*Single Instruction Multiple Data)* dan optimasi perangkat keras lainnya, Chacha20 mampu memberikan kecepatan enkripsi yang lebih baik daripada beberapa algoritma enkripsi lain yang umum digunakan seperti AES. Algoritma ini juga telah diuji dan dianalisis secara luas oleh komunitas kriptografi dan sejauh ini Chacha20 telah terbukti aman terhadap serangan – serangan kriptografi yang terkenal [8].

Algoritma Keccak adalah algoritma SHA-3 adalah pemenang kompetisi fungsi hash NIST pada tahun 2012. Kehadiran SHA-3 bukan berarti untuk menggantikan SHA- 2, karena tidak ada serangan yang signifikan pada SHA-2 dibuktikan. Karena

serangan pada MD5, SHA-0, dan SHA-1 sehingga dibutuhkan alternatif untuk kriptografi yang menjadikan SHA-3. Performa SHA-3 memiliki performa kecepatan yang lebih baik dari SHA-2, dengan melakukan pengujian terhadap file berukuran 10 sampai belasan Mb. Keccak hanya membutuhkan waktu sekitar 2 detik dibandingkan SHA-2 yang membutuhkan waktu sekitar 6 detik. Untuk segi keamanannya SHA-2 dan Keccak belum ada serangan yang terbukti kecuali pada kondisi abnormal pada kedua algoritma [9].

Kombinasi dari algoritma RSA, Chacha20 dan SHA-3 dalam implementasi tanda tangan digital telah terbukti mampu meningkatkan tingkat keamanan dan keandalan untuk memastikan bahwa dokumen atau transaksi elektronik tidak dapat dimanipulasi oleh pihak yang tidak berwenang [10]. Meskipun algoritma RSA, Chacha20 dan SHA-3 telah terbukti efektif dan aman, impelementasinya tidaklah sederhana, tertutama dalam lingkungan yang memerlukan kecepatan dan efisiensi tinggi seperti aplikasi berbasis internet. Oleh karena itu, penelitian ini bertujuan untuk melakukan implementasi yang optimal dari algoritma RSA, Chacha20 dan SHA-3 untuk tanda tangan digital dalam lingkungan sistem informasi dan transaksi elektronik.

Pada penelitian sebelumnya, telah dilakukan pengkombinasian antara algoritma RSA dan AES untuk membuat sebuah super enkripsi guna meningkatkan performa keamanan yang dapat dihasilkan untuk membuat sebuah digital signature. Hasilnya, waktu komputasi yang dibutuhkan tidak berbeda jauh secara signifikan dan masih dibawah 0,1 *milisecond* dengan nilai entropi (tingkat keacakan) dari signature yang lebih tinggi [5]. Hal ini yang mendasari penelitian ini untuk melakukan uji kinerja penggabungan algoritma RSA dengan Chacha20 untuk melihat apakah hasil yang didapatkan lebih baik dari penelitian sebelumnya. Penggabungan algoritma RSA dengan Chacha20 sudah dilakukan sebelumnya pada penelitian lain yang mencoba untuk melakukan enkripsi data yang akan disembunyikan dalam file media menggunakan pendekatan LSB [11]. Berdasarkan hal tersebut penelitian ini akan melakukan pengkombinasian antara algoritma RSA dan Chacha20 untuk membuat sebuah super enkripsi guna meningkatkan performa keamanan yang dapat dihasilkan untuk membuat sebuah *digital signature.*

Berdasarkan uraian di atas, penelitian ini akan mengkaji lebih lanjut mengenai analisis penggabungan algoritma RSA dengan Chacha20 untuk membuat super enkripsi dan diterapkan kedalam *digital signature algorithm*. Oleh karena itu, judul yang dipilih adalah **"Implementasi Tanda Tangan Digital Menggunakan Algoritma Keccak dengan *Rivest-Shamir-Adleman* dan Chacha20"**.

1.2. Rumusan Masalah

1. Bagaimana implementasi tanda tangan digital menggunakan algoritma Keccak dengan RSA dan Chacha20?
2. Bagaimana kinerja dari implementasi tanda tangan digital menggunakan algoritma Keccak dengan RSA dan Chacha20?

1.3. Tujuan dan Manfaat

Dengan didapatnya hasil dari penelitian ini diharapkan bahwa kinerja dari Digital Signature Platform dapat terus ditingkatkan dan dikembangkan guna terus mendapatkan hasil yang lebih baik, sehingga dapat mencapai tujuan sebagai berikut :

1. Menerapkan algoritma Keccak dengan super enkripsi RSA dan Chacha20 pada Digital Signature Algorithm dalam bentuk website.
2. Mengetahui kinerja dari super enkripsi RSA dan Chacha20 pada Digital Signature Algorithm.

1.4. Batasan Masalah

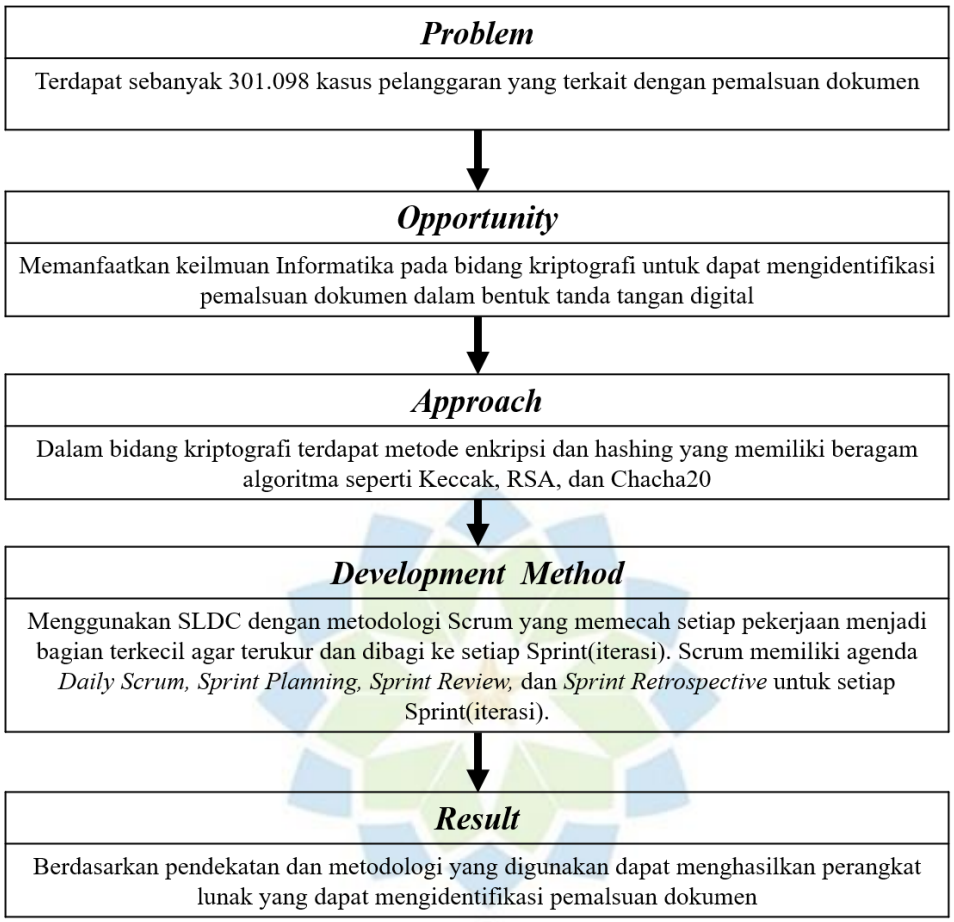
Agar penelitian dan sistem dapat terarah dan sesuai dengan tujuan yang diinginkan, maka diberikan batasan masalah. Adapun yang menjadi batasan masalah sebagai berikut:

1. Tanda tangan digital dalam sistem hanyalah berupa hasil enkripsi yang disimpan ke dalam metadata pdf dan tidak memiliki rupa seperti gambar tanda tangan digital atau gambar QR-Code.
2. Pembuktian akan mensimulasikan proses pengajuan tanda tangan yang terjadi di Jurusan Teknik Informatika UIN Bandung dengan penanda tangan lebih dari 1.

3. Untuk melakukan verifikasi dari dokumen yang diberikan digital signature, dokumen hanya dapat di verifikasi melalui website yang dibangun untuk sebuah prototype.
4. Algoritma Hashing yang digunakan adalah Keccak
5. Algoritma Enkripsi yang digunakan pada super enkripsi adalah RSA (asimetris) dan Chacha20 (simetris)
6. Sistem yang dibangun untuk sebuah prototype hanya dapat melakukan verifikasi dari dokumen yang telah diberikan digital signature melalui sistem.
7. Ekstensi file yang digunakan dibatasi hanya menerima file dengan ekstensi .pdf
8. Ukuran maksimal file pdf adalah 2MB.
9. Sistem dibangun menggunakan framework Flask Python dan ReactJS.
10. Fitur yang akan dibangun pada sistem:
    a. Pengajuan Tanda Tangan
    b. Tanda Tangan Pengajuan
    c. Verifikasi Dokumen

1.5. Kerangka Pemikiran

Kerangka pemikiran dari penelitian ini dapat dipahami melalui ilustrasi yang diberikan pada Gambar 1.1 :



Gambar 1. 1 Kerangka Pemikiran

Pada Gambar 1.1 mengilustrasikan awal dari kerangka pemikiran, yang dimulai dengan mengidentifikasi permasalahan yang sedang dihadapi, yaitu penggunaan tanda tangan konvensional yang saat ini tidak cukup untuk menjamin sifat otentik dan integritas dari sebuah dokumen. Hal ini memunculkan peluang untuk membuat sebuah sistem yang dapat mengidentifikasi penyalahgunaan tanda tangan atau dokumen yang telah dimanipulasi serta mendapatkan kinerja yang lebih baik lagi dari penerapan *Digital Signature Algorithm* dengan menggunakan pendekatan yang berbeda dari yang telah ada sehingga dapat terus dikembangkan dan ditingkatkan kembali. Pendekatan yang dilakukan adalah dengan menggabungkan algoritma RSA dan Chacha20 untuk menghasilkan sebuah ciphertext dengan tingkat keacakan yang tinggi dibantu dengan metodologi pengembangan aplikasi Spiral untuk membuat sebuah sistem prototype yang dapat mensimulasikan hasil dari penelitian ini. Penerapan akan dilakukan

menggunakan bahasa pemrograman python untuk menyimpan fungsi logika utamanya dan javascript untuk menampilkan sistem yang dibangun. Output dari pemikiran adalah hasil kinerja dari super enkripsi RSA dan Chacha20 pada Digital Signature.

1.6. Metodologi Penelitian

Metode penelitian ini menggunakan kerangka kerja Scrum untuk memudahkan setiap perubahan pada perencanaan dan perancangan agar menjadi lebih fleksibel. Scrum dapat mempercepat pengembangan sistem dengan melakukan iterasi dalam jangka waktu tertentu dengan target yang telah ditentukan Berikut adalah langkah-langkah yang dilakukan pada metode Scrum [12]:

a) ***Sprint***

Sprint merupakan tahapan berdurasi 1 – 4 minggu dengan waktu tetap setiap *Sprint* nya agar tercipta konsistensi. Segera setelah *Sprint* sebelumnya berakhir langsung dimulailah *Sprint* yang baru. Semua pekerjaan yang diperlukan untuk mencapai *Product Goal*, termasuk *Sprint Planning*, *Daily Scrum*, *Sprint Review*, dan *Sprint Retrospective*, terjadi dalam Sprint.

b) ***Sprint Planning***

Dimulai dengan *Sprint Planning*, *Sprint* mengorganisir pekerjaan yang akan dilaksanakan selama periode tersebut. Rencana ini disusun secara kolaboratif oleh seluruh anggota Tim Scrum.

c) ***Daily Scrum***

Daily Scrum berlangsung selama 15 menit untuk para *Developers* dalam Tim Scrum. Dalam upaya untuk menyederhanakan, pertemuan ini diadakan pada waktu dan tempat yang sama setiap hari kerja selama *Sprint*.

d) ***Sprint Review***

Sprint Review merupakan acara kedua terakhir di akhir *Sprint*, dengan batas waktu maksimal empat jam untuk *Sprint* selama satu bulan. Jika *Sprint* berdurasi lebih singkat, umumnya acara ini lebih singkat.

e) ***Sprint Retrospective***

Sprint Retrospective adalah acara penutup untuk setiap *Sprint*, dengan batas waktu maksimal tiga jam untuk *Sprint* selama satu bulan. Apabila *Sprint* berlangsung lebih singkat, umumnya durasi acara ini juga lebih singkat.

1.7. Sistematika Penulisan

Penulisan tugas akhir ini dibagi ke dalam lima bab. Adapun penyusunan sistematika penulisannya sebagai berikut :

BAB I PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang masalah, perumusan masalah, batasan - batasan masalah, tujuan dan manfaat penelitian, hingga metodologi penelitian dan sistematika penulisan.

BAB II KAJIAN LITERATUR

Bab ini berisi penjelasan teori – teori yang mendukung dan menunjang penelitian tugas akhir ini serta menyelesaikan permasalahan yang akan dikaji pada penelitian ini.

BAB III METODOLOGI PENELITIAN

Pada bab ini akan dituliskan mengenai metodologi penelitian meliputi metode yang digunakan, analisis sistem, perancangan arsitektur dan diagram yang akan digunakan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi penjelasan mengenai hasil dan pembahasan berupa hasil yang didapat dari penelitian serta pembahasan mendetail dari hasil yang didapat.

BAB V SIMPULAN DAN SARAN

Bab ini berisi pernyataan singkat yang menjelaskan kesimpulan dari penelitian yang dilakukan secara keseluruhan. Bab ini juga berisi saran untuk pengembangan penelitian yang lebih baik lagi kedepannya.

DAFTAR PUSTAKA

Daftar Pustaka berisi referensi atau sumber berupa jurnal, website, maupun buku cetak yang digunakan dalam penelitian dan dikutip dalam penyusunan.

LAMPIRAN

Pada lampirkan ini berisi dokumen – dokumen yang telah digunakan dalam proses penyusunan dan juga perancangan seperti *source code* serta kelengkapan dokumen lainnya.

uin
UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI
BANDUNG