

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era pandemi *covid-19* yang telah terjadi di Indonesia bahkan seluruh dunia ini, semua orang harus menjaga kesehatan dengan benar, dengan menjaga pola makan, pola hidup dan pembatasan sosial. Dengan adanya pembatasan sosial banyak kegiatan yang awalnya dilakukan dengan tatap muka beralih dengan menggunakan teknologi informasi sebagai media untuk berkumpul dan melakukan komunikasi dalam jaringan (*daring/online*) supaya terhindar dan mencegah menyebarnya virus *covid-19*[1]. Dengan adanya pembatasan sosial, kegiatan yang masih dilakukan secara langsung (tatap muka) harus menyatakan bahwa semua orang harus dalam keadaan kondisi tubuh yang sehat, oleh sebab itu dibutuhkan surat keterangan sehat untuk menyatakan orang yang sedang melakukan kegiatan secara langsung (tatap muka) dalam keadaan kondisi tubuh yang sehat[2].

Surat keterangan sehat merupakan dokumen penting yang dibutuhkan untuk berbagai keperluan administrasi seperti ketika melamar kerja, mengurus SIM, hingga melanjutkan pendidikan, dan sebagainya, biasanya akan diminta untuk menyertakan surat keterangan sehat[3]. Apalagi di era pandemi seperti sekarang ini surat keterangan sehat menjadi penting peranannya supaya kegiatan yang dilakukan dengan tatap muka bisa berjalan[2]. Seseorang dapat dinyatakan sehat secara jasmani bisa di buktikan dengan surat keterangan sehat dari lembaga kesehatan yang berwenang, dalam hal ini lembaga kesehatan berwenang yang umum mengeluarkan surat keterangan sehat adalah puskesmas dan rumah sakit[4]. Namun pada masa pandemi surat keterangan sehat berlaku tiga hari saja namun ada juga yang sampai empat belas hari yang berlaku untuk perjalanan jauh, sehingga masyarakat harus mengurusnya setiap tiga atau empat belas hari sekali[2]. Karena hanya berlaku tiga atau empat belas hari dokumen surat keterangan sehat ini rentan dengan adanya perubahan data oleh pihak-pihak yang tidak bertanggung jawab sehingga memunculkan surat keterangan sehat palsu. Seperti yang terjadi di pelabuhan tanjung perak yang terjadi pemalsuan surat keterangan sehat *covid (Rapid Test)*, "Mereka menawarkan surat hasil rapid test kepada calon penumpang kapal laut antar pulau sebagai syarat pembelian tiket agar bisa berangkat," kata Kapolres Pelabuhan Tanjung Perak AKBP Ganis Setyaningrum kepada wartawan, Senin (21/12/2020) (sumber: surabaya.kompas.com)[5]. Maka dari itu perlu adanya tanda bukti yang sah dan fasilitas yang

dapat memberikan layanan pengecekan keaslian dari dokumen dan kebenaran data pada dokumen tersebut dengan cepat dan mudah.

Salah satu cara yang bisa di gunakan adalah mengubah isi informasi menjadi suatu kode-kode yang tidak bisa di mengerti sehingga pihak ketiga akan kesulitan untuk mengetahui isi yang sebenarnya dari informasi tersebut. Namun, hanya dengan mengubah pesan menjadi suatu kode tidak menutup kemungkinan pesan tersebut dapat diubah oleh pihak ke tiga. Salah satunya yaitu memberikan *digital signature* yang sudah diberikan sandi sehingga pelaku tidak bisa mengubah isi dari surat keterangan sehat. Dalam pembuatan *digital signature* digunakan suatu ilmu yang mempelajari tentang teknik matematika yang mempunyai hubungan dengan aspek keamanan informasi, integritas suatu data, dan otentikasi data yaitu kriptografi[6].

Sistem kriptografi dapat digunakan dalam mengatasi masalah keaslian sebuah dokumen, salah satunya tanda tangan digital (*digital signature*), yaitu suatu teknik kriptografi yang dapat dimanfaatkan dalam menjaga isi dari dokumen. *Digital signature* bukanlah tanda tangan yang dibuat secara manual kemudian di pindaikan dimasukkan ke komputer dengan menggunakan alat *scanner* atau sejenisnya, tetapi *digital signature* ini memiliki fungsi sebagai bukti yang dapat memastikan bahwa data atau dokumen tersebut merupakan data yang asli[6]. *Digital signature* juga merupakan salah satu teknik dari kriptografi dalam mengotentifikasi sebuah pesan atau dokumen[7]. *Digital signature* merupakan suatu skema matematis yang secara unik mengidentifikasi seorang pengirim, dan juga dapat membuktikan keaslian sebuah pesan atau dokumen digital dari pemiliknya, sehingga menjadi dokumen yang mempunyai *digital signature* yang autentik (sah), adanya *digital signature* pada dokumen atau file sudah cukup menjadi alasan bagi penerima untuk mempercayai bahwa sebuah pesan atau dokumen yang diterima berasal dari pengirim yang sudah diketahui[8].

Pembuatan *digital signature* diawali dengan proses pendapatan ringkasan isi dokumen kemudian dienkripsi memakai algoritma kunci asimetris supaya menghasilkan kode yang merupakan *digital signature*, dan diakhiri dengan penyisipan *digital signature* pada dokumen. Dalam proses untuk mendapatkan ringkasan isi dokumen dengan memakai fungsi *hash*, fungsi *hash* merupakan salah satu fungsi algoritma satu arah yang dapat menerima inputan pesan dengan panjang sembarang kemudian di konversikan menjadi suatu kode pesan acak dengan panjang yang tetap atau disebut *message digest*[8]. Salah satu fungsi *hashing* yang terbukti aman adalah MD5, algoritma ini dapat mengambil inputan pesan berukuran panjang berapapun yang akan di konversikan dengan menghasilkan output yang terdiri dari 128-bit. Algoritma *Message Digest 5* (MD5) bersifat *one way hash*, sehingga berapapun inputan yang

diberikan hasilnya tetap yaitu sepanjang 32 karakter[7].Algoritma MD5 akan digunakan untuk aplikasi *digital signature*, di mana sebelum pesan atau dokumen dienkripsi dengan kunci privat di bawah *cryptosystem publickey* seperti RSA.

Setelah peringkasan dokumen selesai, dokumen di enkripsi menggunakan algoritma kunci asimetris, yaitu dengan kriptografi RSA yang dapat digunakan sebagai *digital signature* karena mempunyai dua kunci yaitu kunci publik dan kunci privat. Kriptografi RSA merupakan salah satu dari *public key cryptosystem* yang sangat sering digunakan untuk menjamin kerahasiaan terhadap keaslian suatu data digital[9].Dalam kriptografi RSA panjang kunci dapat diatur dalam satuan bit, semakin panjang bit maka semakin sulit untuk dipecahkan, karena sulitnya pemfaktoran dari dua bilangan yang sangat besar, tetapi dalam proses diskripsinya juga membutuhkan waktu yang semakin lama.Dan tahap yang terakhir yaitu menyisipkan *digital signature* dengan mengkonversinya kedalam *qr code*, *qr code* adalah gambar dua dimensi yang dapat menampilkan data berupa teks dengan cara memindai gambar tersebut.Penggunaan *qr code* harus berada di tempat pencahayaan yang cukup supaya pada saat memindai kode pada *qr code* bisa terbaca. *Qr code* biasmenampung banyak informasi dengan panjang 7.089 karakter numerik dan 4296 karakter alfanumerik[10].Sehingga *qr code* dapat dijadikan sebagai bukti cetak bahwa dokumen tersebut telah di tandatangani

Maka dari itu penelitian ini membahas tentang impementasi *digital signature* pada surat keterangan sehat dengan menggunakan Metode MD5 dan RSA. Fungsi metode MD5 pada penelitian ini yaitu menjaga keaslian pada isi dokumen surat keterangan sehat supaya tidak terjadi perubahan karena jika terjadi perubahan pada isi surat keterangan sehat tersebut merkipun hanya satu karakter saja nilai *hash* akan mempunyai nilai yang berbeda. Dan fungsi dari metode RSA ini yang memanfaatkan kunci publik dan kunci privat untuk mengamankan nilai *hash* dari isi surat keterangan sehat, pada penelitian ini akan digunakan metode modifikasi RSA kunci ganda untuk proses enkripsi dan dekripsinya, metode modifikasi RSA kunci ganda dalam proses enkripsi dan dekripsinya menggunakan satu pasang kunci yang berbeda di sisi pengirim dan penerimanya dengan saling bertukar kunci publik mereka, proses pengenkripsian dilakukan dengan mengenkripsi pesan dengan kunci privat si pengirim kemudian di enkripsi lagi menggunakan publik key si pengirim dan pada proses validasinya penerima akan mendekripsi *chiphertext* yang sudah di kirim dengan menggunakan kunci privat mereka kemudian di dekripsi lagi menggunakan kunci publik si pengirim[11]. Penelitian ini juga memanfaatkan metode *QR code* yang digunakan untuk mengkonversi nilai yang dihasilkan dari enkripsi. *QR code* akan ditempelkan atau disatukan dengan file/dokumen surat keterangan sehat yang nantinya akan

menjadi bukti bahwa dokumen tersebut sudah ditandatangani dan digunakan untuk menguji validitas dokumen. Karenadengan adanya *digital signature*bisa menjamin keaslian pada surat keterangan sehat yang diberikan oleh lembaga kesehatan kepada masyarakat yang berkepentingan sehingga tidak perlu khawatir bahwa surat keterangan sehat tersebut palsu, karena dengan adanya *digital signature* pada surat keterangan tersebut dokumen dapat dibuktikan secara langsungkeasliannya dan dapat mencegah terjadinya pemalsuan terhadap penduplikasian surat keterangan sehat yang di berikan kepada masyarakat.

1.2 Perumusan Masalah

1.2.1 Permasalahan(ResearchProblem)

Pada era pandemi Covid-19 masyarakat di Indonesia bahkan seluruh dunia harus menjaga kesehatan tubuhnya, salah satu caranya yaitu menjaga jarak sosial (*social distancing*), dengan diberlakuknya *social distancing* masyarakat dalam melakukan kegiatan di luar rumah sangat di batasi dan juga dibutuhkan surat keterangan sehat untuk melakukan kegiatan seperti bepergian maupun bekerja sebagai bukti bahwa kondisi tubuh benar dikatakansehat. Dengan adanya surat keterangan sehat ini pada umumnya sudah di beri keluluasan dalam melakukan kegiatan bepergian dan bekerja, tetapi surat keterangan tersebut berlaku hanya dua minggu saja dengan begitu masyarakat yang melakukan kegiatan tersebut harus selalu mengecek kesehatan mereka setiap dua minggu sekali. Hal ini mengakibatkan pihak dari dinas kesehatan seperti puskesmas harus membuat begitu banyak surat keterangan sehat untuk masyarakat yang meminta surat keterangan sehat, sebagai bukti surat keterangan sehat yang sah pada dokumen biasanya di sertakan tanda tangan dan stempel dari pihak lembaga kesehatan. Tetapi masih ada juga pihak tidak bertanggung jawab yang memalsukan surat keterangan sehat tersebut, oleh sebab itu dibutuhkannya tanda tangan yang tidak bisa di ubah oleh pihak tertentu seperti *digital signature* dan dibutuhkan juga pengecekan dokumen surat keterangan sehat tersebut supaya bisa di katan asli atau palsu.Untuk mengatasi permasalahan yang terjadi, penulis berinisiatif membuat surat keterangan sehat dengan menggunkana tanda tangan digital(*digital signature*)yang berperan menjadi tanda bukti yang sah sebagai pengganti tanda tangan dan stempel dalam proses pembuatan surat keterangan sehat dan proses verifikasi atau pengecekan keaslian pada dokumen tersebut.

1.2.2 Metode Usulan(*Proposed Method*)

Untuk penelitian ini metode yang digunakan untuk pembuatan *digital signature* pada surat keterangan sehat adalah metode algoritma kriptografi RSA dan MD5 dengan mencocokkan nilai hasil dekripsi *chipertext* dan nilai *hashing*.

Dalam penelitian ini menggunakan algoritma MD5 yang merupakan salah satu algoritma fungsi *hash* yang dapat menerima input dengan panjang sembarang yang mempunyai nilai panjang tetap dan mempunyai nilai *hash* yang tidak akan sama yang berarti setiap ada salah satu perbedaan dalam sebuah pesan nilai *hash* juga akan berubah, dengan begitu pesan yang dihasilkan akan tetap aman. Dalam penelitian ini algoritma MD5 digunakan untuk mengamankan data pasien yang di inputkan pada surat keterangan sehat dan menjaga keaslian isi dari surat keterangan sehat karena jika terdapat perbedaan atau perubahan pada isi dokumen/file tersebut nilai *hash* akan menghasilkan nilai *hash* yang berbeda. Penelitian ini juga menggunakan algoritma kriptografi RSA untuk mengamankan nilai *hash* yang didapat dari data pasien. Algoritma kriptografi RSA merupakan salah satu algoritma kriptografi asimetris yang menggunakan sepasang kunci, yaitu kunci publik dan kunci pribadi dengan kunci publik sebagai enkripsi dan kunci pribadi sebagai dekripsi. RSA panjang kunci dapat diatur dalam satuan bit, semakin panjang bit maka semakin sulit untuk dipecahkan, karena sulitnya pemfaktoran dari dua bilangan yang sangat besar, tetapi dalam proses dekripsinya juga membutuhkan waktu yang semakin lama. Pada penelitian ini akan menggunakan algoritma RSA kunci ganda dengan memanfaatkan dua pasang kunci RSA yang berbeda pada proses enkripsi dan dekripsinya[11]. Dan penelitian ini juga menggunakan QR code untuk mempersingkat pesan sehingga lebih efisien, QR Code disini digunakan sebagai bukti cetak yang sah dan yang nantinya bisa di scan untuk mengecek keaslian dokumen surat keterangan sehat dari pihak puskesmas. Dengan adanya dua algoritma tersebut yang berfungsi untuk mengamankan dan menjaga keaslian isi pesan dari dokumen yang telah dibuat sehingga tidak dapat diduplikasi maupun dipalsukan.

1.2.3 Pertanyaan Penelitian (*Research Question*)

1. Bagaimana melakukan pengujian validitas surat keterangan sehat berbasis *Digital Signature*?
2. Bagaimana tingkat kemudahan penggunaan aplikasi yang telah dibangun?

1.3 Tujuan dan Manfaat Penelitian

1.3.1 Tujuan Penelitian

Adapun tujuan yang akan dicapai melalui penulisan skripsi ini adalah:

Mengimplementasikan digital signature menggunakan metode RSA dan MD5 pada surat keterangan sehat yang bisa menjadi tanda tangan yang sah dan dibuktikan keasliannya.

1.3.2 Manfaat Penelitian

Manfaat yang diperoleh dari tugas akhir ini yaitu:

1. Memberikan pengetahuan baru mengenai apakah sistem dengan teknologi QR code dan digital signature dapat menjadi alternatif solusi untuk permasalahan pengesahan dokumen yang telah dicetak.
2. Pihak puskesmas Dawarblandong dapat menerapkan sistem ini untuk mempermudah dan mempercepat pengerjaan dalam pembuatan surat keterangan sehat.

1.4 Batasan Masalah

Dalam usulan proposal Tugas Akhir ini memerlukan batasan masalah atau biasa disebut dengan ruang lingkup bertujuan agar pembahasan dari tugas akhir ini lebih terarah dengan jelas. Berikut hal-hal yang menjadi batasan masalah:

1. Studi kasus penelitian ini yaitu di daerah kabupaten Mojokerto tepatnya di UPT Puskesmas Dawarblandong.
2. *Digital signature* ini dapat digunakan sebagai tanda bukti yang paten pada sebuah surat keterangan sehat yang dibuat oleh UPT Puskesmas Dawarblandong.
3. File atau dokumen hanya bisa ditandatangani oleh satu pihak.
4. File dikeluarkan oleh pihak UPT Puskesmas Dawarblandong.
5. File atau dokumen divalidasi hanya bisa di web yang sudah dibuat.
6. Bahasa pemrograman yang digunakan adalah PHP dan JavaScript.
7. Sistem berbasis web dengan menggunakan *framework CI* dan basis data MySQL.

1.5 Sistematika Proposal

Adapun sistematika pembahasan skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisikan latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, dan sistematika penulisan laporan.

BAB II KAJIAN PUSTAKA

Bab ini menjelaskan mengenai materi-materi yang dijadikan sebuah landasan dalam penyusunan penelitian ini. Materi-materi yang digunakan adalah mulai dari penelitian-penelitian tentang digital signature tentang kriptografi yang menggunakan kriptografi asimetris RSA, algoritma MD5, QR code, dan teori – teori yang dapat menunjang dalam penyusunan laporan tugas akhir ini.

BAB III METODE USULAN

Bab ini dijelaskan tentang rancangan dari *digital signature* yang akan dibuat setelah melakukan proses analisa terhadap kebutuhan perangkat keras (hardware), perangkat lunak (software), rancangan dari sistem *signature* nantinya dan juga alur dari sistem yang akan dikembangkan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan hasil dan pembahasan dari uji coba yang telah dilakukan pada penelitian ini. Dengan melakukan pengujian verifikasi surat keterangan sehat, pengujian fungsionalitas menggunakan metode *black-box testing* dan pengujian *usability testing*.

BAB V PENUTUP

Bab ini menjelaskan tentang kesimpulan dan saran yang di peroleh dari hasil penelitian yang sudah di buat.