Tanda Tangan Elektronik Menggunakan Algoritma Rivest Shamir Adleman (RSA) pada Sistem Informasi Surat Menyurat LPIK INSTIKI

Ida Bagus Gede Sarasvananda[1]*, Ida Bagus Ary Indra Iswara[2]
Teknik Informatika[1], [2]
Institut Bisnis dan Teknologi Indonesia
Denpasar, Indonesia
sarasvananda@instiki.ac.id[1], indraiswara@instiki.ac.id[2]

***Abstract*— The correspondence system at LPIK INSTIKI already uses a computerized system. However, the correspondence information system currently in use still has drawbacks. The drawbacks include the unavailability of an electronic signature facility (digital signature) and the letter signing process still uses the conventional signature method. With the electronic signature facility on the correspondence information system, it is hoped that it can support the implementation of INSTIKI Indonesia's Work From Home policy during the pandemic. In this study, for the electronic signing process on the LPIK INSTIKI correspondence information system using the RSA cryptographic algorithm. RSA RSA is an algorithm that uses a public key cryptography system that can provide security guarantees on key distribution transmission lines. However, the RSA algorithm produces a signature code that is long enough to make it difficult to insert the code into the document. To overcome this, this study also uses a QR-code scheme to accommodate an electronic signature code that is long enough so that it can be inserted into a letter document. The results of this study are the use of the RSA algorithm accompanied by a QR-Code to perform electronic signatures to secure the authenticity of letter documents and simplify the process of signing letter documents. The test results mean the encryption time is 0.000072932243347168 seconds, and the average decryption time is 1.9866268873215 seconds.**

***Keywords*— Digital signature, RSA, Cryptography, QR-Code**

***Abstrak*— Sistem surat menyurat pada LPIK INSTIKI sudah menggunakan sistem terkomputerisasi. Namun, sistem informasi surat menyurat yang sedang dipergunakan saat ini masih memiliki kekurangan. Kekurangannya meliputi belum tersedianya fasilitas tanda tangan secara elektronik (digital signature) dan proses penandatanganan surat masih menggunakan cara tanda tangan konvensional. Dengan adanya fasilitas tanda tangan elektronik pada sistem informasi surat menyurat diharapkan dapat mendukung penerapan kebijakan Work From Home INSTIKI Indonesia selama pandemi berlangsung. Pada penelitian ini, untuk proses penandantangan elektronik pada sistem informasi surat menyurat LPIK INSTIKI menggunakan algoritma kriptografi RSA. RSA RSA merupakan algortima yang menggunakan sistem kriptografi kunci publik yang dapat memberikan jaminan keamanan pada jalur transmisi distribusi kunci. Namun, algoritma RSA menghasilkan kode tanda tangan yang cukup panjang sehingga kesulitan dalam menyisipkan kode pada dokumen. Untuk mengatasi hal tersebut, penelitian ini juga menggunakan skema QR-code untuk menampung kode tanda tangan elektronik yang cukup panjang sehingga dapat disisipkan pada dokumen surat. Hasil dari penelitian ini yaitu penggunaan algoritma RSA disertai dengan QR-Code untuk melakukan tanda tangan elektronik dapat mengamankan keaslian dokumen surat dan mempermudah proses tanda tangan dokumen surat. Hasil pengujian rata-rata waktu enkripsi yaitu 0,000072932243347168 detik, dan rata-rata waktu dekripsi yaitu 1,9866268873215 detik.**

***Kata Kunci*— Tanda tangan elektronik, RSA, Kriptografi, QR-Code**

I. PENDAHULUAN

Lembaga Pengembangan Inovasi dan Kreativitas (LPIK) Institut Bisnis dan Teknologi Indonesia (INSTIKI) merupakan salah satu Lembaga yang terdapat di Kampus INSTIKI. LPIK memiliki tujuan untuk memfasilitasi produk hasil inovasi dan kreativitas dari Civitas Akademika INSTIKI. Untuk membantu proses administrasi surat menyurat yang diperlukan oleh LPIK INSTIKI yang mencakup keperluan Laboratorium, Sumber Daya Manusia, dan Proyek dikelola oleh sekretaris LPIK. Surat menyurat yang dikelola oleh Sekretaris LPIK diantaranya yaitu Surat Keputusan Pengangkatan Kepala Laboratorium, Pemanfaatan Produk Laboratorium, Kreativitas Dosen INSTIKI (KDS), Asisten Laboratorium, dan Laboran.

Dalam penerapannya, sistem administrasi surat menyurat pada LPIK INSTIKI sudah menggunakan sistem terkomputerisasi. Sistem informasi surat menyurat pada LPIK INSTIKI dapat mempermudah tata kelola arsip surat, penomeran index surat dilakukan secara otomatis, mencetak surat secara langsung ke printer atau menyimpan dalam bentuk pdf. Namun, sistem informasi surat menyurat yang sedang dipergunakan saat ini masih memiliki kekurangan. Kekurangannya meliputi belum tersedianya fasilitas tanda tangan secara elektronik (*digital signature*) dan proses penandatanganan surat masih menggunakan cara tanda tangan konvensional. Dengan adanya fasilitas tanda tangan elektronik

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i2.1403, Copyright ©2022
Submitted : May 20, 2022; Revised : July 30, 2022; Accepted : August 8, 2022; Published : September 7, 2022

pada sistem informasi surat menyurat diharapkan dapat mendukung penerapan kebijakan *Work From Home* INSTIKI Indonesia selama pandemi berlangsung.

Tanda tangan dipergunakan untuk mengindentifikasi keabsahan dan juga sebagai bukti bahwa seseorang yang menandatangani telah mengetahui dan menyetujui isi dari dokumen yang ditandatangani [1]. Tanda tangan elektronik dengan tanda tangan konvensional memiliki perbedaan dari sisi penggunaannya [1]. Tanda tangan konvensional dapat disalin secara manual ataupun dengan cara *scan copy* dan dapat dipergunakan secara berulang sedangkan tanda tangan elektronik sangat bergantung kepada identitas dari setiap dokumen, sehingga setiap dokumen akan menghasilkan tanda tangan elektronik yang berbeda [1]. Tanda tangan elektronik dapat memberikan jaminan otentifikasi, integritas dan non-repudiation [2].

Semakin berkembangnya teknologi, sebuah dokumen tidak hanya diterbitkan dalam bentuk cetak saja (*hardcopy*), tetapi juga dalam bentuk digital (*softcopy*). Dokumen dalam bentuk digital rentan terhadapat kemungkinan modifikasi serta sulitnya pembuktian keaslian dokumen tersebut [2]. Untuk mengatasi permasalahan tersebut dibutuhkan sebuah sebagai jaminan keamanan data surat dengan menerapkan tanda tangan elektronik.

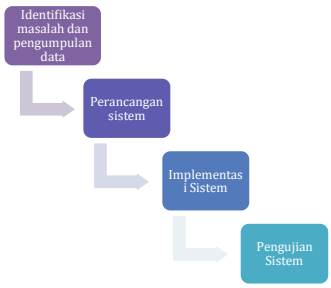
Tanda tangan elektronik dapat menjamin keamanan dokumen yang ditandatanganinya dalam aspek *integrity*, *authentication*, serta *non-repudiation* [3]. 1) *Integrity*: Tanda tangan elektronik dapat memastikan bahwa pesan yang dikirim adalah pesan yang sebenarnya dan tidak dimodifikasi pada saat transmisi. Hal ini dikarenakan pada dokumen asli tidak diberlakukan proses enkripsi, sehingga dokumen dapat dibaca oleh banyak pihak. Keaslian pesan dapat diperoleh dengan membandingkan *message digest* dari dokumen asli dengan *plaintext* hasil verifikasi tandatangan digital. Jika hasilnya sama, maka dokumen telah terjamin keasliannya. 2) *Authenticity*: Tanda tangan elektronik dibuat dengan mengenkripsi *message digest* dari pesan asli menggunakan kunci privat pengirim. *Ciphertext* ini hanya bisa didekripsi menggunakan pasangan kunci publik dari kunci privat tersebut, sehingga jika hasil verifikasi membuktikan bahwa message digest dokumen sama dengan hasil dekripsi dari ciphertext, maka dapat dipastikan bahwa pengirim adalah benar orang yang memiliki kunci privat tersebut. 3) *Non-repudiation*: Jika tanda tangan elektronik telah terbukti ditandatangani menggunakan kunci privat tertentu, maka tidak dapat disangkal bahwa pemilik kunci privatlah yang telah menulis dokumen tersebut.

Jaminan keamanan data surat yang ditandatangani secara digital bergantung pada metode kriftografi dan panjang kunci yang digunakan [4]. Salah satu algoritma yang digunakan untuk penerapan tanda tangan elektronik adalah *Rivest Shamir Adleman* (RSA) [1],[2],[5],[6]. Algoritma RSA banyak dipergunakan sebagai metode pada tanda tangan elektronik karena keamanan dari algoritma RSA yaitu sulitnya memfaktorkan bilangan prima yang sangat besar menjadi faktor-faktor prima yang lebih kecil [1].

Pada penelitian ini, untuk proses penandantangan elektronik pada sistem informasi surat menyurat LPIK INSTIKI menggunakan algoritma kriptografi RSA. Namun, algoritma RSA menghasilkan kode tanda tangan yang cukup panjang sehingga kesulitan dalam menyisipkan kode pada dokumen [5]. Untuk mengatasi hal tersebut, penelitian ini juga menggunakan skema QR-code untuk menampung kode tanda tangan elektronik yang cukup panjang sehingga dapat disisipkan pada dokumen surat [6]. Dengan adanya skema *QR-code*, dapat digunakan untuk menampung kode tanda tangan elektronik yang cukup panjang sehingga dapat disisipkan pada dokumen. [7] dalam penelitiannya menggunakan *QR-Code* untuk penyisipan kode dalam sertifikat elektronik, [8] juga menggunakan *QR-Code* untuk menyisipkan kode inventaris. *QR-Code* (*quick response code*) yang dapat menyimpan data numerik, alphanumerik, binary dan kanji, serta memiliki penyimpanan yang jauh lebih besar dibandingkan *barcode* [9]. *QR-Code* ini dapat digunakan untuk menyembunyikan suatu pesan dibalik sebuah kode yang dapat memberikan jaminan keaman dan privasi terhadap orang yang melakukan pengiriman pesan [10]. Namun pembangkitan *QR-code* ini belum memiliki kunci yang memberikan parameter perubahan yang dapat menyembunyikan data asli, sehingga untuk keamanan data lebih tinggi, maka kriptografi dapat digunakan untuk mengenkripsi data sebelum dibangkitkan *QR-code*nya [11].

II. METODE PENELITIAN

Metode yang akan digunakan dalam penelitian ini yaitu metode pengembangan perangkat lunak waterfall seperti pada Gambar 1. Adapun tahapan dari metode pengembangan perangkat lunak waterfall yaitu terdiri dari 1) identifikasi masalah dan pengumpulan data, 2) perancangan sistem untuk proses sign dan verifikasi surat, 3) implementasi sistem untuk proses sign dan verifikasi menggunakan algoritma kriptografi RSA, dan 4) pengujian sistem [12].



Gambar 1. Metode pengembangan perangkat lunak

A. *Identifikasi Masalah dan Pengumpulan Data*

Tahapan pengumpulan data dilakukan dengan menggunakan metode wawancara [13]. Wawancara dilakukan dengan seluruh stakeholder yang terlibat dalam proses penandatangan surat menyurat di LPIK. Adapun stakeholder yang terlibat yaitu: Kepala LPIK, Bidang Sumber Daya Manusia, Bidang Proyek dan Inovasi, Bidang Infrastruktur dan Sekretaris LPIK. Kemudian dilakukan proses observasi untuk mengamati proses penerbitan surat sampai proses penandatangan surat.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i2.1403, Copyright ©2022
Submitted : May 20, 2022; Revised : July 30, 2022; Accepted : August 8, 2022; Published : September 7, 2022

Untuk menganalisis dari sistem yang sedang berjalan, dalam penelitian ini menggunakan metode Analisa PIECES (*Performance*, *Information*, *Economics*, *Control*, *Efiency*, *Service*). Metode PIECES dapat menggambarkan bagaimana peran sistem dalam membantu menyelesaikan permasalahan dalam pekerjaan sehingga dapat dioptimalisasi [14] [15]. [16] Dalam penelitiannya menggunakan metode PIECES untuk analisis website. Hasil analisa sistem dapat dilihat pada Tabel 1.

Tabel 1. Hasil Analisa sistem

	Permasalahan	Yang Diusulkan
P	Masih memerlukan waktu tambahan ketika memerlukan file surat yang sudah ditandatangani berupa *softcopy*, karena harus melalui proses cetak surat, tanda tangan surat, *scanner* surat.	Tidak perlu melakukan proses cetak, dan scanner surat untuk membuat file softcopy surat yang telah ditandatangani
I	Susahnya membedakan surat asli yang diterbitkan oleh LPIK dengan surat yang telah dimodifikasi oleh pihak-pihak yang tidak bertanggung jawab	Dibuatkan fasilitas pada sistem untuk melakukan validasi dari surat yang diterbitkan
E	Membutuhkan biaya kertas untuk mencetak surat yang akan ditandatangani sebelum diterbitkan	Dengan menggunakan sistem, tidak perlu mencetak surat terlebih dahulu sebelum ditandatangani.
C	Stempel dan tanda tangan tidak bisa dikontrol dan masih ada kemungkinan bilamana seseorang yang tidak bertanggung jawab memalsukan tanda tangan atau membuat ulang stempel	Proses penandatangan menggunakan *digital signature* berupa kunci private dan kunci publik sehingga akan sulit digandakan.
E	Proses penandatangan surat tidak efisien karena harus mencetak surat terlebih dahulu sebelum ditandatangani	*User* penandatangan surat dapat menandatangani surat secara langsung menggunakan sistem
S	Sistem belum bisa mengakomodir proses tanda tangan elektronik	Dokumen surat akan ditandatangani secara elktronik

B. Perancangan Sistem

Pada subbab ini menyajikan tahap analisa dan perancangan dari sistem yang akan dibangun berdasarkan permasalahan yang telah dirumuskan. Analisis dan rancangan sistem merupakan sebuah tahapan untuk mendefinisikan kebutuhan-kebutuhan sistem dan memberikan gambaran yang jelas dan terstruktur dari sisitem yang dibangun.

1) Deskripsi Umum Rancangan Sistem

Dalam penerapannya, sistem administrasi surat menyurat pada LPIK INSTIKI sudah menggunakan sistem terkomputerisasi. Sistem informasi surat menyurat pada LPIK INSTIKI dapat mempermudah tata kelola arsip surat, penomeran *index* surat dilakukan secara otomatis, mencetak surat secara langsung ke printer atau menyimpan dalam bentuk pdf. Namun, sistem informasi surat menyurat yang sedang dipergunakan saat ini masih memiliki kekurangan. Adapun kekurangannya seperti belum tersedianya fasilitas tanda tangan secara elektronik (*digital signature*) dan proses penandatanganan surat masih menggunakan cara tanda tangan konvensional.

Pada penelitian ini, untuk proses penandantangan digital pada sistem informasi surat menyurat LPIK INSTIKI menggunakan algoritma kriptografi RSA. Hasil enskripsi dari algoritma RSA menghasilkan kode *chipertext* yang cukup panjang. Untuk mempermudah penyisipan *chipertext* sebagai tanda tangan elekronik dalam dokumen surat, maka dalam penelitian ini menggunakan skema *QR-code* sebagai solusinya.

Rivest Shamir Adleman (RSA)

Jaminan keamanan data surat yang ditandatangani secara digital bergantung pada metode kriftografi dan panjang kunci yang digunakan [4]. Salah satu algoritma yang digunakan untuk penerapan tanda tangan elektronik adalah *Rivest Shamir Adleman* (RSA). RSA merupakan algortima yang menggunakan sistem kriptografi kunci publik yang dapat memberikan jaminan keamanan pada jalur transmisi distribusi kunci. RSA serta mendukung tanda tangan elektronik yang memverifikasi pesan yang diterima merupakan pesan asli yang dikirim oleh pengirim pesan [5][6][17]. RSA dikatakan aman, karena sulitnya memfaktorkan bilangan n, dimana n = pxq, p dan q adalah bilangan prima yang sangat besar [1].

RSA membangkitkan kunci privat dan kunci publik-nya, dengan langkah-langkash sebagai berikut [6]:

a) Membangkitkan nilai p dan q secara sembarang, dimana p dan q ini adalah bilangan prima yang besar.
b) Menghitung n

$$n = p \,.\, q \tag{1}$$

c) Menghitung $\varphi(n)$ yaitu

$$\varphi(n) = (\mathrm{p} - 1)(\mathrm{q} - 1) \tag{2}$$

d) Memilih kunci public e yang relative prima terhadap rumus (3)

$$\varphi(\mathrm{n}).\,\mathrm{GCD}(\varphi(\mathrm{n}), \mathrm{e}) = 1 \tag{3}$$

e) Membangkitkan kunci private d menggunakan rumus (4)

$$\mathrm{e.d} = \mathrm{k}.\varphi(\mathrm{n}) + 1 \tag{4}$$

f) Dihasilkanlah pasangan kunci public (e,n) dan kunci private (d,n).

Sedangkan untuk proses enkripsi dan dekripsi, RSA melakukan langkah-langkah seperti berikut:

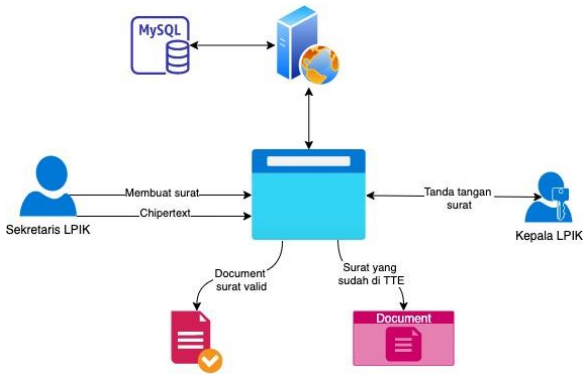
a) Enkripsi suatu pesan (m) menggunakan kunci public (e, n)

$$c = m^d \; mod \; n \tag{5}$$

b) Dekripsi suatu *cipherteks* (c) menggunakan kunci privat (d,n)

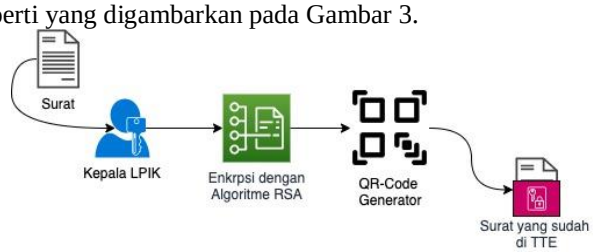
$$m = c^d \; mod \; n \tag{6}$$

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i2.1403, Copyright ©2022
Submitted : May 20, 2022; Revised : July 30, 2022; Accepted : August 8, 2022; Published : September 7, 2022



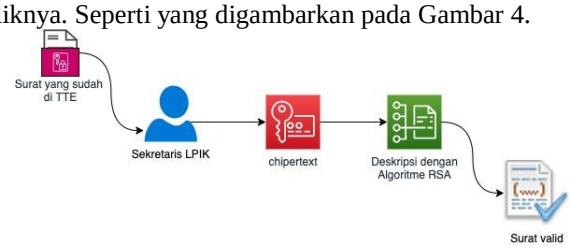
Gambar 2. Arsitektur sistem

Gambar 2 merupakan gambaran umum arsitektur sistem dari perancangan sistem yang diusulkan. Secara garis besar terdapat dua buah proses dalam arsitektur sistem. Proses tersebut meliputi tanda tangan elektronik pada sistem surat menyurat LPIK INSTIKI dan proses validasi surat yang telah ditandatangan secara elektronik. Proses pembuatan tandangan elektronik pada dokumen surat diawali dari proses pembuatan surat baru oleh Sekretaris, kemudian surat diajukan kepada Ketua untuk ditandatangani menggunakan algoritma RSA seperti yang digambarkan pada Gambar 3.



Gambar 3. Proses pembuatan tanda elektronik

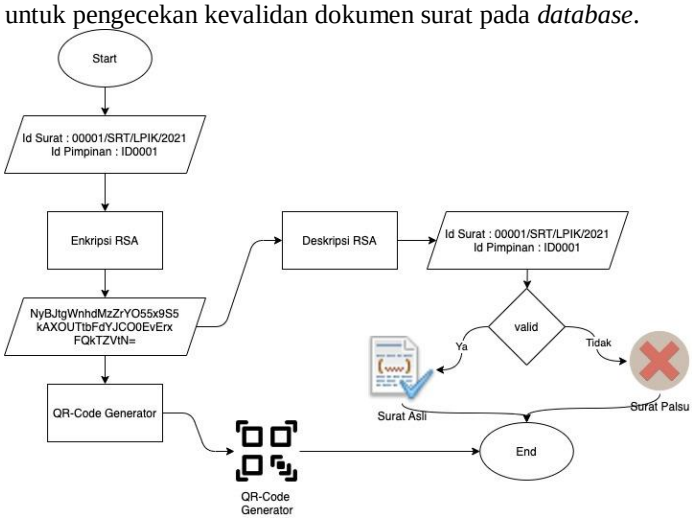
Sedangkan untuk proses validasi surat yang telah ditandatangani secara elektronik, Sekretaris atau pengguna umum dapat melakukan validasi dengan memasukan kode *chipertext* yang telah disisipkan pada *Qr-Code*. Setelahnya sistem akan melakukan deskripsi menggunakan algoritma RSA. Hasil enkripsi berupa kode *plaintext* selanjutnya akan dilakukan pencocokan di *database*, jika data berhasil ditemukan maka dokumen surat dianggap valid, pun sebaliknya. Seperti yang digambarkan pada Gambar 4.



Gambar 4. Proses validasi surat yang telah ditandatangani secara elektronik

2) Rancangan Tanda Tangan Elektronik

Adapun data yang akan dienkripsi pada setiap dokumen surat yaitu data nomer surat yang dikombinasikan dengan kode Ketua LPIK. Data yang dikombinasikan akan menjadi *plaintext*, *plaintext* akan dienkripsi menggunakan algoritma RSA. Hasil enkripsi dari algoritma RSA akan digenerate terlebih dahulu menjadi *QR-code* sebelum disisipkan pada dokumen surat. Setiap dokumen surat yang telah disisipkan kode *QR-code* menjadikan dokumen surat tersebut telah ditandatangani secara elektronik. Sedangkan untuk proses validasi surat yang telah ditandatangani dengan menginputkan kode *chipertext* dari hasil *scanner QR-code*, kemudian dilakukan deskripsi menggunakan algoritma RSA sehingga menghasilkan kode *plaintext. Plaintext* merupakan teks yang di*encode* dalam format ASCII *Plaintext* akan di-*parsing* untuk mendapatkan nomer surat dan kode Ketua LPIK untuk pengecekan kevalidan dokumen surat pada *database*.



Gambar 5. Rancangan tanda elektronik menggunakan algoritma RSA

C. *Implementasi*

Sistem informasi tanda tangan elektronik LPIK INSTIKI akan diimplementasikan dengan menggunakan bahasa pemrograman *Hypertext Prepocessor* (PHP). Basis data untuk menyimpan data surat menggunakan basis data *MySQL*. Sistem yang telah dibangun akan di-*install* pada *server cloud* agar bisa diakses dari mana dan kapan saja. Seiring perkembangan internet sehingga memudahkan setiap orang untuk mengakses informasi [18]. Sehingga untuk dosen yang memerlukan dokumen surat hanya perlu mengakses sistem yang sudah di-install, dan tidak perlu datang secara langsung ke LPIK INSTIKI.

D. *Pengujian*

Untuk dapat menguji peningkatan keamanan dari sistem tanda tangan elektronik yang dirancang, dilakukan perhitungan waktu proses enkripsi dan deskripsi untuk sistem kriptografi dengan RSA. Untuk menguji fungsionalitas dari sistem tanda tangan elektronik menggunakan pengujian *Black-box* . Pengujian *black-box* merupakan pengujian yang yang berfokus pada kebutuhan fungsionalitas dari sistem yang dibangun [19],[20][21].

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i2.1403, Copyright ©2022
Submitted : May 20, 2022; Revised : July 30, 2022; Accepted : August 8, 2022; Published : September 7, 2022

III. HASIL DAN PEMBAHASAN

Sistem yang dibangun merupakan pengembangan dari sistem informasi surat menyurat LPIK INSTIKI. Sistem informasi surat menyurat LPIK INSTIKI merupakan sistem yang dibangun berbasis *website* yang dapat diakses dari mana saja. Pengembangan dari sistem surat menyurat LPIK INSTIKI yaitu dengan menambahkan fitur tanda tangan secara elektronik (*digital signature*) pada setiap dokumen yang diterbitkan oleh LPIK INSTIKI. Selain itu, dikembangkan juga fitur untuk mengecek keaslian dokumen surat untuk berbagai keperluan lainnya.

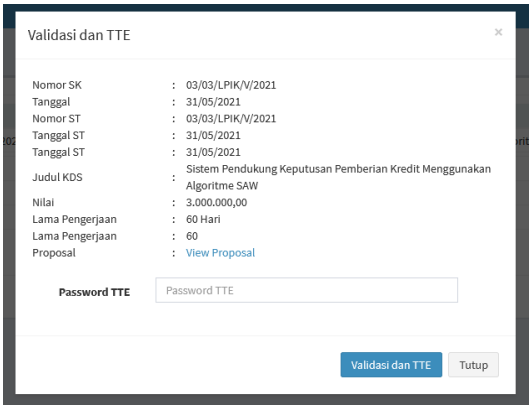
A. *Proses Tanda Tangan Elektronik*

Proses tanda tangan elektronik dimulai dari Sekretaris LPIK membuat surat pada sistem, surat yang telah selesai dimasukkan dalam sistem akan diajukan ke Kepala LPIK untuk divalidasi dan ditanda tangan secara digital. Adapun data yang akan dienkripsi pada setiap dokumen surat yaitu data *id* surat yang dikombinasikan dengan kode Ketua LPIK. Data yang dikombinasikan akan menjadi *plaintext*, *plaintext* akan dienkripsi menggunakan algoritma RSA. Hasil enkripsi dari algoritma RSA akan digenerate terlebih dahulu menjadi *QR-code* sebelum disisipkan pada dokumen surat. Setiap dokumen surat yang telah disisipkan kode *QR-code* menjadikan dokumen surat tersebut telah ditandatangani secara elektronik. Contoh proses enkripsi tanda tangan elektronik dapat dilihat pada Tabel 2.

Tabel 2. Hasil Enkripsi dan pembangkitan QR-Code

Data dokumen surat	Id Surat : 1622427761 Id Kepala LPIK : usr008
Plaintext	1622427761/ usr008
Konfirmasi TTE	Password : password dari Kepala LPIK
Hasil Enkripsi	2457527. 2156165. 107278. 107278. 2697093. 107278. 1679105. 1679105. 2156165. 2457527. 646351. 1950212. 2080129. 2437947. 2224416. 817758. 2224416. 817758. 2437947. 1628137. 1950212
QR-Code	

Untuk rangkain proses pembubuhan tanda tangan elektronik pada dokumen surat LPIK INSTIKI, Kepala LPIK akan melakukan validasi terhadap dokumen surat yang telah diinput oleh Sekretaris LPIK. Proses pembubuhan tanda tangan elektronik, Kepala LPIK harus memasukkan *password* untuk melakukan tanda tangan elektronik. *Password* dibutuhkan untuk memastikan bahwa memang benar yang melakukan tanda tangan elektronik adalah Kepala LPIK. Setelah memasukkan *password*, proses enkripsi RSA akan diproses, dan hasil enkripsi RSA akan degenerate menjadi *QR-Code* sebelum disisipkan pada dokumen surat. Gambar 6 merupakan halaman proses tanda tangan elektronik oleh Kepala LPIK.

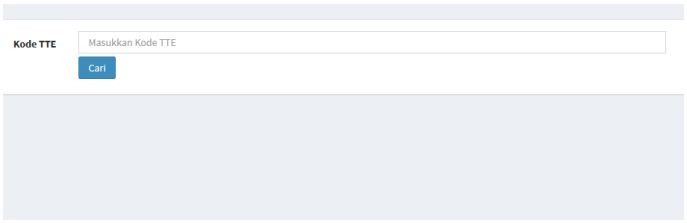


Gambar 6. Halaman proses tanda tangan elektronik.

.

B. *Proses Validasi Keaslian Tanda Tangan Elektronik*

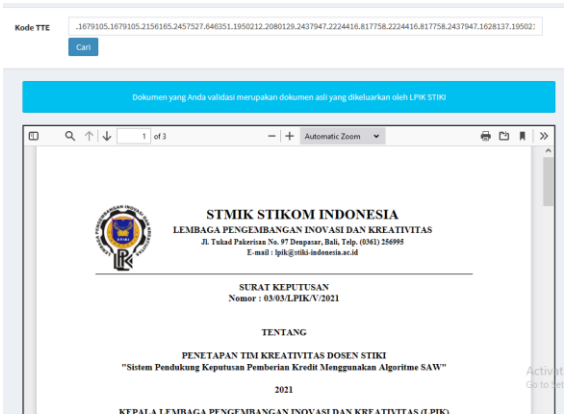
Proses validasi keaslian tanda tangan elektronik berfungsi untuk mengecek keaslian dokumen surat yang diterbitkan oleh LPIK INSTIKI. Setiap dokumen surat yang diterbitkan dan di tanda tangan secara elektronik memiliki kode unik hasil enkripsi menggunakan algoritma RSA. Kode unik hasil enksripsi tersebut disisipkan dalam sebuah gambar berupa *QR-Code*. Proses pengecekan dilakukan dengan memasukkan kode yang telah disisipkan pada *QR-Code*. Untuk membaca kode yang telah disisipkan pada *QR-Code* dapat dilakukan dengan menggunakan *QR-Code reader*. Gambar 7 merupakan halaman untuk melakukan validasi dokumen surat yang telah ditandatangan secara elektronik.



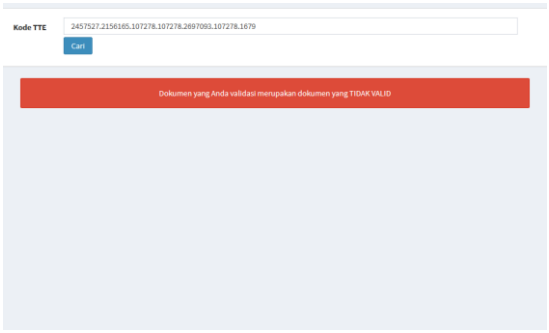
Gambar 7. Halaman validasi dokumen surat

Setelah memasukkan kode hasil enkripsi (*chipertext*), sistem akan melakukan dekripsi menggunakan algoritme RSA. Hasil dekripsi akan diparsing untuk mendapatkan *Id* Surat dan Kode user Kepala LPIK, yang selanjutnya akan digunakan sebagai parameter untuk mencari dokumen surat yang tersimpan pada sistem. Jika dokumen surat ditemukan dalam sistem, maka dokumen surat tersebut merupakan dokumen surat yang valid dan sudah ditanda tangan secara elektronik, pun sebaliknya.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i2.1403, Copyright ©2022
Submitted : May 20, 2022; Revised : July 30, 2022; Accepted : August 8, 2022; Published : September 7, 2022



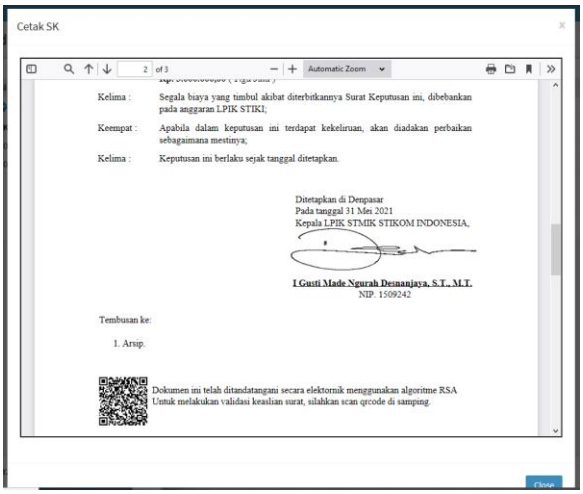
Gambar 8. Halaman hasil validasi dokumen valid tanda tangan elektronik



Gambar 9. Halaman hasil validasi dokumen tidak valid

C. *Hasil Tanda Tangan Elektronik*

Setiap dokumen surat yang berhasil dibubuhkan tanda tangan secara elektronik akan disisipkan QR-Code yang merupakan hasil enkripsi menggunakan algoritma RSA. *QR-Code* dipilih untuk menyisipkan kode tanda tangan elektronik untuk mengoptimalisasi penyisipan hasil enkripsi algoritma RSA [10], karena algoritma RSA menghasilkan kode tanda tangan yang cukup panjang sehingga kesulitan dalam menyisipkan kode pada dokumen surat. Gambar 10 merupakan hasil dokumen surat yang telah ditanda tangan secara elektronik menggunakan algoritma RSA.



Gambar 10. Dokumen surat yang telah ditanda tangan secara elektronik

D. *Hasil Pengujian Waktu Eksekusi*

Pengujian waktu eksekusi dilkakukan untuk mengetahui waktu rata-rata yang dibutuhkan untuk membubuhkan tanda tangan elektronik serta waktu rata-rata untuk memvalidasi keaslian dokumen surat. Data yang digunakan untuk mengetahui waktu rata-rata yaitu sebanyak 10 data. Tabel 3 merupakan hasil pengujian waktu proses enkripsi dan proses dekripsi.

Tabel 3. Hasil pengujian waktu proses enkripsi dan dekripsi

Data	Waktu Enkripsi	Waktu Deksripsi
Data 1	0,000072956085205078	1,9354140758514
Data 2	0,000070810317993164	1,9187588691711
Data 3	0,000074148178100586	2,0354928970337
Data 4	0,000074148178100586	1,9858169555664
Data 5	0,000072002410888672	1,9329349994659
Data 6	0,000071048736572266	2,0281062126160
Data 7	0,000071048736572266	2,0522820949554
Data 8	0,000072002410888672	1,9804599285126
Data 9	0,000076055526733398	2,0330808162689
Data 10	0,000075101852416992	1,9639220237732
Rata-rata	**0,000072932243347168**	**1,9866268873215**

Berdasarkan hasil pengujian waktu yang dilakukan rata-rata waktu yang dibutuhkan untuk melakukan enkripsi dalam pembubuhan tanda tangan elektronik yaitu 0,000072932243347168 detik, sedangkan waktu rata-rata yang dibutuhkan untuk melakukan dekripsi dalam validasai keaslian dokumen surat yaitu 1,9866268873215 detik. Waktu yang dibutuhkan untuk melakukan dekripsi dalam validasi keasliaan dokumen lebih lama dibandingkan dengan waktu enkripsi dalam pembubuhan tanda tangan.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i2.1403, Copyright ©2022
Submitted : May 20, 2022; Revised : July 30, 2022; Accepted : August 8, 2022; Published : September 7, 2022

E. Hasil Pengujian Fungsionalitas Sistem

Pengujian fungsionalitas sistem dilakukan dengan menggunakan metode pengujian *black-box* untuk mengetahui apakah sistem sudah berjalan sesuai dengan kebutuhan fungsionalitas sistem. Proses pengujian dilakukan dengan cara menguji setiap fungsionalitas sistem dengan sistem yang telah dibangun. Tabel 4 merupakan hasil dari pengujian dengan metode *black-box*.

Tabel 4. Hasil pengujian sistem dengan *blackbox testing*

No.	Fungsionlitas Sistem	Hasil Pengujian
1.	Melakukan enkripsi untuk tanda tangan elektronik	Sistem telah mampu melakukan enkripsi menggunakan algoritma RSA untuk melakukan tanda tangan elektronik
2.	Mampu men-*generate chipertext* menjadi QR-Code	Sistem telah mampu mengenerate *chipertext* menjadi QR-Code, *chipertext* merupakan hasil kode enkrpisi dari algoritma RSA
3.	Menyipsikan *QR-Code* dalam dokumen surat	Sistem mampu menyisipkan *QR-Code* dalam dokumen surat yang diterbitkan oleh LPIK INSTIKI
3	Memvalidasi keaslian tanda tangan elektronik	Sistem mampu melakukan validasi keaslian tanda tangan elektronik dengan melakukan dekripsi dari *chipertext*.

IV. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan, maka dapat disimpulkan sebagai berikut:

1. Penggunaan algoritma RSA disertai dengan *QR-Code* untuk melakukan tanda tangan elektronik dapat mengamankan keaslian dokumen surat dan mempermudah proses tanda tangan dokumen surat.
2. Hasil pengujian rata-rata waktu yang dibutuhkan untuk melakukan enkripsi algoritma RSA pada penelitian ini yaitu 0,000072932243347168 detik, sedangkan rata-rata waktu yang dibutuhkan untuk melakukan dekripsi yaitu 1,9866268873215 detik.
3. Tanda tangan elektronik pada sistem informasi surat menyurat LPIK INSTIKI dapat berjalan sesuai dengan fungsionalitas sistem yang diharapkan, hal tersebut dibuktikan dengan hasil pengujian dengan metode pengujian *black-box*.

DAFTAR PUSTAKA

[1] R. A. Azdy, "Tanda tangan Digital Menggunakan Algoritme Keccak dan RSA," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 5, no. 3, pp. 184–191, 2016, doi: 10.22146/jnteti.v5i3.255.

[2] Y. Anshori, A. Y. Erwin Dodu, and D. M. P. Wedananta, "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital," *Techno.Com*, vol. 18, no. 2, pp. 110–121, 2019, doi: 10.33633/tc.v18i2.2166.

[3] F. Information and P. Standards, "Digital Signature Standard," *Safeguarding Crit. E-Documents*, no. July, pp. 221–221, 2015, doi: 10.1002/9781119204909.app1.

[4] A. E. Mezher, "Enhanced RSA cryptosystem based on multiplicity of public and private keys," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 3949–3953, 2018, doi: 10.11591/ijece.v8i5.pp3949-3953.

[5] F. Nuraeni, Y. H. Agustin, and I. M. Muharam, "Implementasi Tanda Tangan Digital Menggunakan RSA dan SHA-512 Pada Proses Legalisasi Ijazah," *Knsi 2018*, pp. 864–869, 2018.

[6] F. Nuraeni, Y. H. Agustin, D. Kurniadi, and I. D. Ariyanti, "Implementasi Skema QR-Code dan Digital Signature menggunakan Kombinasi Algoritma RSA dan AES untuk Pengamanan Data Sertifikat Elektronik," *Semin. Nas. Teknol. Informasi, Komun. dan Ind. 12*, pp. 43–52, 2020.

[7] I. K. Arya *et al.*, "Sosialisasi Penggunaan Sistem Informasi Sertifikat Elektronik pada Lembaga Penjamanin Mutu Pendidikan Provinsi Bali Menurut Peraturan Menteri Pendidikan Dan Kebudayaan Republik Indonesia No 26 Tahun 2020 tentang Organisasi Dan Tata Kerja Unit Pelaksana Te," vol. 2, no. 1, pp. 42–49, 2021.

[8] I. N. T. A. Putra, "Pengembangan Sistem Inventaris Berbasis Qr Code Menggunakan Web Service Pada Bidang Sarana Dan Prasarana Stmik Stikom Indonesia," *J. Nas. Pendidik. Tek. Inform.*, vol. 7, no. 3, p. 315, 2019, doi: 10.23887/janapati.v7i3.16658.

[9] E. Ardhianto *et al.*, "Dengan Memanfaatkan Gambar Qr Code," *Pengemb. Metod. OTENTIKASI KEASLIAN IJASAH DENGAN MEMANFAATKAN GAMBAR QR CODE Eka*, vol. 13, pp. 35–41, 2016.

[10] S. Murni and R. Sabaruddin, "Pemanfaatan Qr Code Dalam Pengembangan Sistem Informasi Kehadiran Siswa Berbasis Web," *J. Teknol. dan Manaj. Inform.*, vol. 4, no. 2, 2018, doi: 10.26905/jtmi.v4i2.2144.

[11] L. Kartika and Yudi, "Rancang Bangun Aplikasi Penyembunyian Pesan QRCode Dengan Menggunakan Metode Caesar Cipher Berbasis Android," *J. FTIK*, vol. 1, no. 1, pp. 511–518, 2020.

[12] Y. Handrianto and B. Sanjaya, "Model Waterfall Dalam Rancang Bangun Sistem Informasi Pemesanan Produk Dan Outlet Berbasis Web," *J. Inov. Inform.*, vol. 5, no. 2, pp. 153–160, 2020, doi: 10.51170/jii.v5i2.66.

[13] I. B. G. Sarasvananda, I. G. M. N. Desnanjaya, and Y. Dewi, "Klasterisasi Sebaran Kasus Covid-19 Di Kota Denpasar Menggunakan Algoritme K-Means," *J. Sains Komput. Inform. (J-SAKTI*, vol. 5, no. September, p. 565, 2021.

[14] A. H. Sidiq and A. Kurniawati, "Analisis Kebutuhan Sistem Administrasi Bagian Sidang Ujian Universitas Gunadarma Dengan Metode Pieces," *J. Ilm. Teknol. dan Rekayasa*, vol. 24, no. 1, pp. 22–34, 2019, doi: 10.35760/tr.2019.v24i1.1931.

[15] I. B. G. Sarasvananda, I. P. E. G. Gunawan, I. K. A. G. Wiguna, M. S. Ariantini, and I. G. I. Sudipa, "PIECES ANALYSIS IN THE INFLUENCE OF THE DESIGNING DIGITAL SIGNATURE CERTIFICATE SYSTEM," *J. Mantik*, vol. 6, no. 36, pp. 984–991, 2022.

[16] R. S. Dewi, R. R. Marchada, and A. Rifai, "Analisa Pieces Penerapan Digital Monitoring Informasi Penyewaan Ruko Pasar 8 Pada Pt . Alam Sutera Realty , Tbk," *Semin. Nas. Teknol. Inf. dan Komun. 2016 (SENTIKA 2016)*, vol. 2016, no. Sentika, pp. 18–19, 2016.

[17] A. Aminudin, G. P. Aditya, and S. Arifianto, "RSA algorithm using key generator ESRKGS to encrypt chat messages with TCP/IP protocol," *J. Teknol. dan Sist. Komput.*, vol. 8, no. 2, pp. 113–120, 2020, doi: 10.14710/jtsiskom.8.2.2020.113-120.

[18] M.A. Muslim, "PENGEMBANGAN SISTEM INFORMASI JURUSAN BERBASIS WEB UNTUK MENINGKATKAN PELAYANAN DAN AKSES INFORMASI," *J. MIPA*, vol. 37, no. 2, pp. 105–114, 2014.

[19] S. Roohullah Jan, S. Tauhid Ullah Shah, Z. Ullah Johar, Y. Shah, and F. Khan, "An Innovative Approach to Investigate Various Software

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i2.1403, Copyright ©2022
Submitted : May 20, 2022; Revised : July 30, 2022; Accepted : August 8, 2022; Published : September 7, 2022

Testing Techniques and Strategies," *Int. J. Sci. Res. Sci. Eng. Technol.*, vol. 2, no. 2, pp. 682–689, 2016.

[20] T. S. Jaya, "Pengujian Aplikasi Dengan Metode Blackbox Testing Boundary Value Analysis (Studi Kasus: Kantor Digital Politeknik Negeri Lampung)," *J. Inform. J. Pengemb. IT*, vol. 3, no. 2, pp. 45–48, 2018, doi: 10.30591/jpit.v3i1.647.

[21] I. Bagus Gede Sarasvananda, I. Komang Arya Ganda Wiguna, and Styawati, "Pendekatan Metode Extreme Programming untuk Pengembangan Sistem Informasi Manajemen Surat Menyurat pada LPIK STIKI," *J. Inform. Univ. Pamulang*, vol. 6, no. 2, pp. 258–267, 2021, [Online]. Available: http://openjournal.unpam.ac.id/index.php/informatika258.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v11i2.1403, Copyright ©2022
Submitted : May 20, 2022; Revised : July 30, 2022; Accepted : August 8, 2022; Published : September 7, 2022