Pengamanan Tanda Tangan Digital Dalam *QR Code* Berbasis *Website* Menggunakan Metode RSA (Studi Kasus: Kantor Desa Parit Baru)

Rahmat Wahyudi*[1], Uray Ristian[2], Suhardi[3]
[1,2,3]Jl. Prof. Dr. H. Hadari Nawawi, Kota Pontianak, Kalimantan Barat
[1,2,3]Jurusan Rekayasa Sistem Komputer, Fakultas MIPA Universitas Tanjungpura
e-mail: ***[1]rahmat.allstar@gmail.com**, [2]Suhardi@siskom.untan.ac.id,
[3]eristian@siskom.untan.ac.id

Abstrak

Sistem administrasi surat menyurat di Kantor Desa Parit Baru sudah menggunakan sistem terkomputerisasi. Namun, masih terdapat kekurangan dalam sistem informasi surat menyurat yang saat ini diterapkan. Salah satu kekurangan utama adalah kurangnya fasilitas tanda tangan digital, dengan proses penandatanganan surat masih mengandalkan tanda tangan konvensional. Penelitian ini bertujuan untuk mengatasi masalah ini dengan menerapkan fasilitas tanda tangan digital dalam administrasi surat menyurat dan mendukung penerapan keamanan dalam proses administratif. Penelitian ini menggunakan metode observasi yang meliputi tahap identifikasi masalah, pengumpulan data, perancangan sistem, implementasi, dan tahap pengujian. Algoritma RSA dipilih untuk implementasi tanda tangan digital dalam penelitian ini. Meskipun algoritma RSA memiliki keamanan yang tinggi, namun menghasilkan kode tanda tangan yang panjang. Untuk mengatasi masalah ini, penelitian juga menggunakan skema QR Code sebagai metode untuk menampung kode tanda tanda tangan digital yang panjang sehingga dapat disisipkan pada dokumen surat. Hasil dari penelitian ini bermanfaat untuk menyederhanakan proses tanda tangan pada dokumen surat dengan menggunakan tanda tangan digital. Selain itu, sistem ini juga dapat menjaga keaslian dokumen surat. Dalam hasil pengujian, pemindaian QR Code terenkripsi terhadap 15 data QR Code berhasil, sehingga dapat mengenali seluruh data.

Kata kunci*— Kriptografi, Algoritma RSA, Tanda Tangan Digital, QR Code, Surat.*

Abstract

The correspondence administration system at Parit Baru Village Office is already computerized. However, there are existing deficiencies in the current system. One significant drawback is the absence of digital signature facilities, leading to reliance on conventional signatures for letter signing. This study aims to rectify this issue by introducing digital signature facilities to the correspondence administration system, thereby enhancing security in administrative processes. The research methodology includes observation methods involving problem identification, data collection, system design, implementation, and testing stages. The RSA algorithm is selected for digital signature implementation in this study. Despite its high security, the RSA algorithm produces lengthy signature codes. To address this, the study employs a QR Code scheme to accommodate the lengthy digital signature codes, allowing them to be embedded in letters. The results of this research are valuable for simplifying the letter signing process using digital signatures while ensuring document authenticity. Testing results indicate successful encryption scans of 15 QR Code data, thereby recognizing all data.

Keywords— *Cryptography, RSA Algorithm, Digital Signature, QR Code, Letters.*

1. PENDAHULUAN

Proses administratif di Kantor Desa Parit Baru sudah memanfaatkan teknologi informasi. Terdapat banyak tujuan yang muncul dalam implementasi teknologi informasi tersebut, di antaranya adalah peningkatan tingkat efektivitas dan bahkan merubah sistem pelayanan administratif di Kantor Desa Parit Baru. Pada saat ini pelayanan administratif di Kantor Desa Parit Baru memerlukan inovasi berbasis teknologi informasi untuk penerapan *Smart* RT berbasis digital. Pelayanan administratif yang umum dilakukan adalah penandatanganan dokumen, oleh karena itu perlu dilakukan upaya untuk memastikan keabsahan suatu dokumen surat.

Dalam penerapannya saat ini, penandatanganan surat menyurat di Kantor Desa Parit Baru masih terdapat kekurangan. Kekurangannya yaitu tidak adanya sistem penandatanganan secara digital untuk dokumen surat dan proses penandatanganan dokumen masih dengan tanda tangan konvensional. Tanda tangan digunakan sebagai identifikasi keaslian dan bukti seorang penandatangan sudah mengetahui dan sepakat terhadap dokumen surat yang ditandatangani [1]. Terdapat perbedaan antara tanda tangan konvensional dan tanda tangan digital dalam penggunaannya. Pada tanda tangan konvensional rentan diduplikasi secara langsung ataupun dengan cara *scanning* digital yang dapat disalahgunakan secara berulang. Untuk tanda tangan digital memiliki informasi yang berbeda pada setiap dokumen yang ditandatangani, hal ini dikarenakan setiap dokumen memiliki identitas informasi yang berbeda pada setiap dokumen suratnya [2].

Dokumen digital masih memiliki kerentanan terhadap perubahan isi dan pembuktian keaslian dokumen. Dengan menerapkan tanda tangan digital sebagai jaminan keamanan data dokumen digital permasalahan tersebut dapat diselesaikan. Pada saat transmisi, pesan yang bertandatangan digital dapat dipastikan bahwa pesan tersebut adalah pesan yang asli tanpa adanya perubahan. Hal ini disebabkan adanya proses enkripsi pada tanda tangan digital, dimana dokumen asli tidak diterapkan enkripsi, sehingga dokumen tetap dapat terbaca oleh banyak pihak [3]. Keaslian pesan dapat diketahui dengan memverifikasi tanda tangan digital, *message digest* dari dokumen asli dan *plaintext* dari hasil verifikasi tanda tangan digital kemudian dibandingkan. Jika hasil *message digest* dari dokumen asli sama dengan *plaintext* dari hasil verifikasi, dapat dipastikan dokumen terjamin keasliannya [4].

Keamanan data pada surat yang ditandatangani dengan digital tergantung pada panjang kunci dan metode kriptografi yang digunakan. Dalam penelitian ini algoritma RSA digunakan untuk mengamankan tanda tangan digital. Pada algoritma RSA panjang kode tangan (*ciphertext*) yang dihasilkan cukup panjang. Oleh karena itu, penelitian ini akan memanfaatkan skema *QR Code* sebagai penyimpanan kode tanda tangan digital yang cukup panjang agar mudah disisipkan di dokumen surat [5].

Sebelumnya, pada sebuah penelitian yang telah dilakukan mengenai pengamanan tanda tangan digital. Dalam penelitian tersebut informasi pada tanda tangan digital diamankan menggunakan metode RSA. Hasil dari penelitian ini, diketahui pada program yang telah diterapkan algoritma RSA dapat mengenkripsi *plaintext* dan menghasilkan *output ciphertext* yang tidak dapat dipahami oleh pihak luar yang ingin melihat informasi dari pesan yang telah dienkripsi. Penelitian menggunakan pemograman *python*, inputan pada aplikasi hanya *support* format teks dan belum *support* format Docx, *output* dari aplikasi hanya *ciphertext* dan tidak menerapkan skema *QR Code* [6]. Pada penelitian ini telah menggunakan PHP, inputan pada aplikasi telah *support* format Docx, menerapkan skema *QR Code* pada tanda tangan digital, dan melakukan studi kasus penelitian di Kantor Desa Parit Baru.

Pada studi penelitian lainnya sudah berhasil membuat aplikasi penandatangan dokumen secara digital dengan menggunakan algoritma kriptografi yang telah menerapkan *QR Code* sebagai solusi untuk menyimpan tanda tangan digital dalam bentuk kode (*ciphertext*) yang cukup

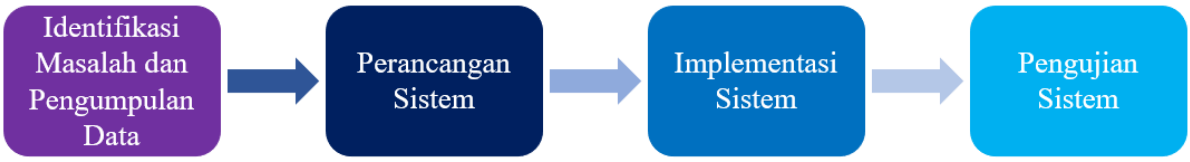
panjang. Dari penelitain ini didapatkan hasil data pada tanda tangan digital yang di enkripsi dan diterapkan ke dalam *QR Code* terbukti dapat menguatkan keabsahan terhadap suatu dokumen yang ditandatangani karena informasi telah terlindungi dan tidak dapat terdeteksi apabila di *scan* menggunakan aplikasi lain selain aplikasi yang menerbitkan tanda tangan tersebut. Penelitian menggunakan algoritma dari *Advanced Encryption Standard* (AES) untuk melakukan enkripsi tanda tangan digital, aplikasi hanya *support* format PDF dan belum Docx. [7]. Pada penelitian ini menggunakan algoritma dari *Rivest Shamir Adleman* (RSA), dan inputan pada aplikasi telah *support* format Docx.

Penelitian terkait lainnya pernah dilakukan untuk mengamankan tanda tangan digital pada kuitansi digital. Dalam penelitain ini, algoritma RSA diterapkan pada *website* khusus untuk menandatangani kuitansi secara digital. Hasil dari penelitian ini, data pada tanda tangan digital yang dienkripsi berupa nomor kuitansi, nama pelaku transaksi pertama dan pelaku transaksi kedua berhasil diamankan dan terbukti dapat menguatkan keabsahan kuitansi digital pada proses transaksi karena informasi telah terlindungi dan tidak akan terdeteksi apabila di *scan* dengan aplikasi lain. Pada penelitian aplikasi yang dibuat hanya *support* format teks dan belum *support* format Docx, tidak memiliki lokasi penelitian, dan data yang dienkripsi yaitu nomor kuitansi, nama pelaku transaksi pertama dan pelaku transaksi kedua [8]. Pada penelitian ini inputan pada aplikasi telah *support* format Docx, melakukan studi kasus penelitian di Kantor Desa Parit Baru, dan data yang dienkripsi adalah informasi dari tanda tangan digital *QR Code.*

Berdasarkan pemaparan masalah dari penelitian terdahulu, penelitian ini mengembangkan suatu sistem tanda tangan digital yang diberi nama "E-RTSignParitBaru" yang menggunakan enkripsi dari algoritma RSA dan diterapkan dalam *QR Code* sebagai tanda tangan digital untuk keabsahan dokumen surat. Penelitian ini diharapkan dapat memberikan manfaat pada peningkatan keamanan dokumen surat dengan menggunakan algoritma RSA untuk enkripsi dan menyimpan tanda tangan dalam *QR Code*, efisiensi dan keterbacaan proses penandatanganan dokumen surat yang lebih mudah dipahami serta *QR Code* yang cepat terbaca dan diverifikasi.

2. METODE PENELITIAN

Melalui penggunaan aplikasi berbasis *web*, penelitian ini memusatkan perhatian pada implementasi sistem keamanan tanda tangan digital dalam *QR Code* dengan menggunakan Metode RSA. Diagram alir penelitian pada Gambar 1 menunjukkan tahapan metode penelitian sebagai berikut.



Gambar 1. Diagram Alir Penelitian

Pada Gambar 1 memaparkan rangkaian tahapan dalam metode penelitian, mencakup identifikasi permasalahan dan pengumpulan data, perancangan sistem, implementasi sistem, serta pengujian sistem.

2.1 Identifikasi Masalah dan Pengumpulan Data

Pada tahap penelitian ini, metode untuk mengumpulkan data yang diterapkan adalah metode observasi. Proses observasi ini melibatkan penghimpunan informasi dan data secara langsung di Kantor Desa Parit Baru dan bagaimana sistem bekerja di Kantor Desa Parit Baru. Data yang dipergunakan dalam penelitian ini adalah surat pengantar RT tiruan dan akan dibuat data warga seperti yang sudah pernah melakukan layanan administrasi surat menyurat di Kantor Desa Parit Baru. Data yang dihimpun berjumlah 15 surat pengantar RT. Data yang diperoleh dari

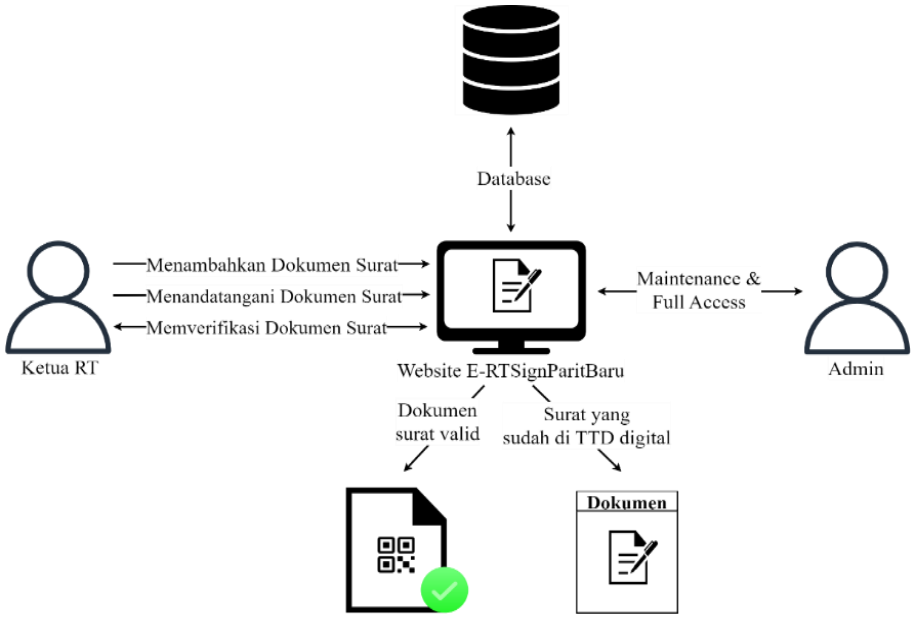
proses pengumpulan informasi ini dimanfaatkan untuk mengevaluasi efektivitas algoritma yang terintegrasi dalam sistem yang dikembangkan dalam penelitian ini.

2.2 Perancangan Sistem

Tahapan perancangan sistem memiliki tujuan untuk merinci keperluan sistem dan menyampaikan representasi terstruktur dari sistem yang sedang dibuat. Meskipun Kantor Desa Parit Baru telah mengadopsi sistem administrasi surat menyurat terkomputerisasi, namun masih terdapat kekurangan, seperti ketiadaan fasilitas tanda tangan digital. Penelitian ini mengimplementasikan proses penandatanganan digital dengan algoritma kriptografi RSA. *Ciphertext* yang dihasilkan dari proses enkripsi RSA memiliki kode yang cukup panjang, dan guna mempermudah integrasi sebagai tanda tangan digital, penelitian ini juga menggunakan metode *QR Code*.

2.2.1 *Arsitektur Sistem*

Sistem arsitektur E-RTSignParitBaru memiliki dua pengguna, yaitu Admin dan Ketua RT. Ketua RT dapat mengakses *website* dan menambahkan dokumen surat, yang akan disimpan dalam basis data untuk diproses dengan tanda tangan digital *QR Code* menerapkan enkripsi RSA. Proses verifikasi dapat diakses oleh Ketua RT dan Admin. Rancangan struktur sistem yang dibuat terlihat pada Gambar 2.



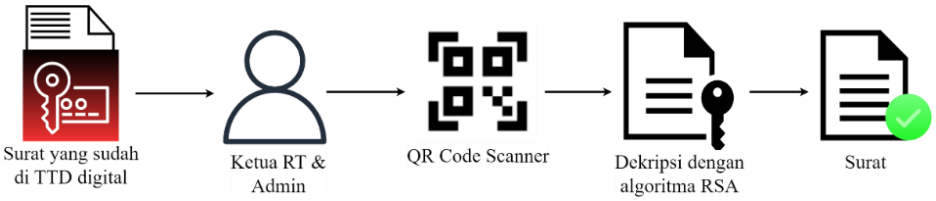
Gambar 2. Struktur Sistem

Berikut adalah penjelasan lebih lanjut dari struktur sistem, secara umum terdapat dua tahap utama dalam struktur sistem ini. Tahap pertama melibatkan penerapan tanda tangan digital pada sistem surat-menyurat RT/RW di Desa Parit Baru, sementara tahap kedua mencakup proses validasi surat yang telah mendapatkan tanda tangan digital. Penciptaan tanda tangan digital pada dokumen surat dimulai dengan pembuatan surat oleh Ketua RT, diikuti oleh proses pengolahan surat untuk mendapatkan tanda tangan digital menggunakan algoritma RSA, sebagaimana tergambar pada Gambar 3.

Gambar 3. Proses *Generate* Tanda Tangan Digital

Untuk proses verifikasi surat yang telah mendapatkan tanda tangan digital, Ketua RT dan Administrator memiliki kewenangan untuk melakukan verifikasi dengan memindai *QR Code*

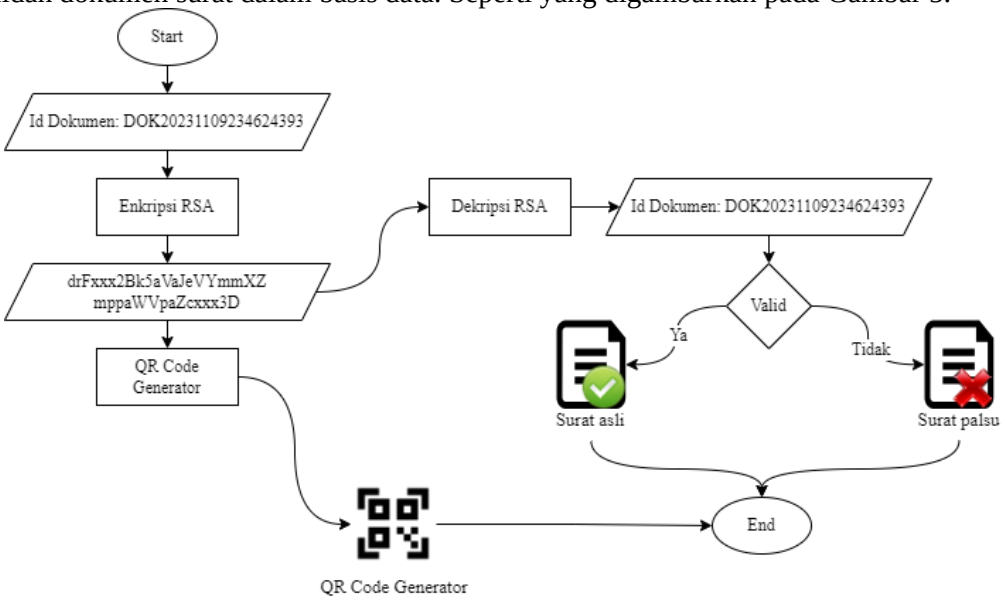
yang telah dienkripsi pada dokumen tersebut. Selanjutnya, sistem akan menjalankan proses dekripsi menggunakan algoritma RSA. *Output* dari proses enkripsi berupa kode *plaintext*, akan dibandingkan dengan data dalam basis data. Jika terdapat kecocokan atau kesesuaian, dokumen surat dianggap valid. Sebaliknya, jika tidak maka dianggap tidak valid. Ilustrasi proses ini dapat dilihat pada Gambar 4.



Gambar 4. Proses Verifikasi Dokumen Surat yang Telah Ditandatangan

2.2.2 Rancangan Tanda Tangan Digital

Data yang akan dienkripsi pada setiap dokumen surat adalah Id Dokumen, yang digunakan sebagai *plaintext*. *Plaintext* ini akan mengalami proses enkripsi dengan algoritma RSA, dan hasil enkripsi tersebut akan dihasilkan dalam bentuk *QR Code* sebelum disematkan pada dokumen surat. Inklusi kode *QR Code* pada setiap dokumen surat menandakan bahwa dokumen tersebut telah diberikan tanda tangan digital. Proses validasi surat yang telah ditandatangani melibatkan penggunaan pemindai *QR Code*. Selanjutnya, dilakukan proses dekripsi menggunakan algoritma RSA untuk menghasilkan *plaintext*. *Plaintext* tersebut kemudian diurai untuk mendapatkan Id Dokumen surat, yang selanjutnya digunakan untuk memverifikasi kevalidan dokumen surat dalam basis data. Seperti yang digambarkan pada Gambar 5.



Gambar 5. Desain Tanda Tangan Digital dengan Penerapan Algoritma RSA

2.3 Rivest Shamir Adleman (RSA)

Metode *Rivest Shamir Adleman* (RSA) merupakan salah satu algoritma kriptografi *modern* dengan kategori kunci asimetris, di mana kunci yang digunakan dalam proses enkripsi berbeda dengan kunci yang diterapkan dalam proses dekripsi. Pada proses enkripsi, kunci publik digunakan, sedangkan untuk dekripsi, kunci privat diaplikasikan [9]. Algoritma RSA memiliki keunggulan karena kesulitan dalam faktorisasi bilangan besar menjadi faktor prima. Hingga saat ini, algoritma RSA mempertahankan tingkat keamanan yang tinggi, karena belum terdapat mesin atau metode lain yang mampu dengan cepat mendekripsi data yang telah dienkripsi oleh algoritma tersebut. Keamanan algoritma ini dipengaruhi oleh panjang kunci, di mana semakin besar panjang bitnya, semakin sulit untuk melakukan dekripsi karena faktorisasi dua bilangan prima acak yang

digunakan dalam pembentukan kunci menjadi semakin sulit [10]. Langkah-langkah pembentukan kunci publik dan kunci privat pada algoritma *Rivest Shamir Adleman* (RSA) dijelaskan sebagai berikut: [5].

a. Menentukan dua bilangan prima secara acak yang disimbolkan sebagai p dan q, dengan syarat $p \neq q$, dan keduanya saling terpisah.
b. Menghitung nilai N sebagai hasil dari perkalian dua bilangan prima, yaitu
$$N = p.q \quad (1)$$
c. Menentukan nilai Φ yaitu
$$\Phi = (p - 1) * (q - 1) \quad (2)$$
d. Memilih bilangan bulat (integer) dalam rentang satu hingga Φ, dengan syarat $(1 < e < \Phi)$, yang juga merupakan bilangan koprima terhadap Φ. e akan digunakan sebagai kunci publik.
e. Menentukan nilai d
$$e * d \bmod \Phi = 1 \quad (3)$$
alternatifnya, nilai d dapat juga dihitung menggunakan rumus
$$d = (1+k\Phi)/e = \text{bilangan bulat} \quad (4)$$
Nilai k diperoleh melalui eksperimen dengan menjalankan nilai sekuensial dari 1,2,3, . . .dst, sehingga dapat menghasilkan nilai d yang berupa bilangan bulat. Nilai d ini nantinya akan digunakan sebagai kunci privat.
f. Kunci publik terdiri dari pasangan (e, N), sementara kunci privat terdiri dari pasangan (d, N).

Proses enkripsi dan dekripsi dalam RSA melibatkan langkah-langkah sebagai berikut ini:

a. Enkripsi pesan (P) menggunakan kunci publik (e, N) dengan rumus
$$C = \textit{Plaintext}\ e \bmod N \quad (5)$$
b. Dekripsi *ciphertext* (C) menggunakan kunci privat (d, N) dengan rumus
$$P = \textit{Chipertext}\ d \bmod N \quad (6)$$

2.4 Implementasi

Pada tahap implementasi, E-RTSignParitBaru sistem tanda tangan digital, akan diterapkan dengan bahasa pemrograman *Hypertext Preprocessor* (PHP). Pengelolaan data surat dilakukan melalui basis data *MySQL*. Sistem yang telah dikembangkan akan diinstalasikan pada *server cloud* untuk memungkinkan aksesibilitas yang fleksibel dari berbagai lokasi dan waktu.

2.5 Pengujian

Guna menguji tingkat keamanan dari sistem tanda tangan digital yang telah dikonseptualkan, dilakukan pengujian pengenkripsian dan pendekripsian data pada *QR Code*.

3. HASIL DAN PEMBAHASAN

Sistem penandatanganan surat menyurat E-RTSignParitBaru adalah suatu platform berbasis situs *web* yang dapat diakses dari berbagai lokasi. Pengembangan sistem terkomputerisasi untuk manajemen surat menyurat di Desa Parit Baru, E-RTSignParitBaru, melibatkan implementasi fitur tanda tangan digital pada setiap dokumen yang dikeluarkan oleh Desa Parit Baru, khususnya untuk surat pengantar RT. Selain itu, juga dikembangkan fitur untuk melakukan verifikasi keaslian dokumen surat untuk keperluan lainnya.

3.1 Pembangkitan Kunci RSA

Pilih dua bilangan prima secara acak, p dan q, yang berbeda satu sama lain. Misal: p = 557 dan q = 757. Hitung hasil perkalian dari kedua bilangan prima: $n = p \times q = 557 \times 757 = 421649$. Hitung nilai fungsi Euler dari n, yaitu $\Phi(n) = (p - 1) \times (q - 1) = 556 \times 756 = 420336$. Kemudian pilih bilangan e sebagai kunci publik yang relatif prima terhadap $\Phi(n)$, dalam contoh ini e = 11. Selanjutnya temukan bilangan d (kunci privat) yang merupakan invers modular dari e

terhadap Φ(n) dengan menggunakan algoritma *Extended Euclidean* atau formula $d = \frac{(1+k\,\Phi(n))}{e}$, dimana *k* adalah bilangan bulat. Misalnya, dengan memilih *k* = 8, maka *d* = 305699.

3.2 Proses Enkripsi RSA

Pada perhitungan proses enkripsi ini digunakan data *plaintext* berupa id dokumen, misal *P* = DOK2023100. *Plaintext* dikonversi ke dalam nilai ASCII (*Decimal*) agar dapat digunakan untuk proses selanjutnya, data yang telah diubah dapat dilihat pada Tabel 1.

Tabel 1. Konversi *Ciphertext* ke Nilai ASCII (*Decimal*)

No.	*Plaintext*	Bentuk ASCII
1.	D	68
2.	O	79
3.	K	75
4.	2	50
5.	0	48
6.	2	50
7.	3	51
8.	1	49
9.	0	48
10.	0	48

Setelah dikonversi, selanjutnya data *plaintext* di enkripsi menggunakan kunci publik (*e*) dengan menggunakan persamaan berikut.

$C = P^e$ (*mod* n)

$C_1 = 68^{11}$ (*mod* 421649) = 400027
$C_2 = 79^{11}$ (*mod* 421649) = 379792
$C_3 = 75^{11}$ (*mod* 421649) = 213841
$C_4 = 50^{11}$ (*mod* 421649) = 306912
$C_5 = 48^{11}$ (*mod* 421649) = 153250
$C_6 = 50^{11}$ (*mod* 421649) = 306912
$C_7 = 51^{11}$ (*mod* 421649) = 357184
$C_8 = 49^{11}$ (*mod* 421649) = 98977
$C_9 = 48^{11}$ (*mod* 421649) = 153250
$C_{10} = 48^{11}$ (*mod* 421649) = 153250

Jadi, Ciphertext yang dihasilkan dari proses enkripsi RSA adalah

C = 400027.379792.213841.306912.153250.306912.357184.98977.153250.153250

3.2.1 Proses Dekripsi RSA

Pada perhitungan proses dekripsi ini menggunakan kunci privat (*d*) dengan menggunakan persamaan berikut.

$P = C^d$ (*mod* n)

$P_1 = 400027^{305699}$ (*mod* 421649) = 68
$P_2 = 379792^{305699}$ (*mod* 421649) = 79
$P_3 = 213841^{305699}$ (*mod* 421649) = 75
$P_4 = 306912^{305699}$ (*mod* 421649) = 50
$P_5 = 153250^{305699}$ (*mod* 421649) = 48
$P_6 = 306912^{305699}$ (*mod* 421649) = 50
$P_7 = 357184^{305699}$ (*mod* 421649) = 51
$P_8 = 98977^{305699}$ (*mod* 421649) = 49
$P_9 = 153250^{305699}$ (*mod* 421649) = 48
$P_{10} = 153250^{305699}$ (*mod* 421649) = 48

Setelah data *ciphertext* di dekripsi, selanjutnya mengkonversi hasil ke dalam nilai ASCII (Karakter) untuk mendapatkan bentuk *plaintext* seperti semula, data yang telah diubah dapat dilihat pada Tabel 2.

Tabel 2. Konversi *Ciphertext* ke Nilai ASCII (Karakter)

No.	Bentuk ASCII	*Plaintext*
1.	68	D
2.	79	O
3.	75	K
4.	50	2
5.	48	0
6.	50	2
7.	51	3
8.	49	1
9.	48	0

No.	Bentuk ASCII	*Plaintext*
10.	48	0

Jadi, hasil *Ciphertext* yang di dekripsi kembali pada proses dekripsi RSA adalah
P = 68 79 75 50 48 50 51 49 48 48
P = DOK2023100

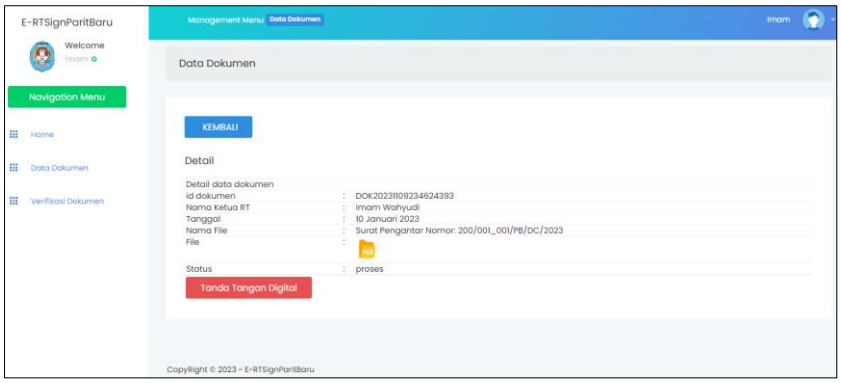
3.3 Proses Tanda Tangan Digital

Proses penerapan tanda tangan digital dimulai dengan administrator Kantor Desa Parit Baru menambahkan data Ketua RT baru ke dalam *website* E-RTSignParitBaru, sistem kemudian membangkitkan kunci *public* dan *private* 4096-bit untuk Ketua RT baru dan menyimpannya di dalam *database*. Setelah pembentukan kunci, Ketua RT bisa mengakses *website* E-RTSignParitBaru sebagai Ketua RT. Proses ini diawali dengan Ketua RT melengkapi informasi pada formulir surat pengantar RT yang diperlukan oleh warga. Kemudian, surat tersebut diunggah ke *web* E-RTSignParitBaru untuk mendapatkan tanda tangan digital. Informasi yang akan dienkripsi pada setiap dokumen surat adalah identitas dokumen (id dokumen), yang akan dijadikan sebagai *plaintext*. *Plaintext* tersebut kemudian dienkripsi menggunakan algoritma RSA. Hasil enkripsi dari algoritma RSA dibuat dalam bentuk *QR Code* sebelum ditempatkan pada dokumen surat. Penggabungan *QR Code* pada dokumen surat menandakan bahwa surat tersebut telah menerima tanda tangan digital. Contoh dari proses enkripsi tanda tangan digital dapat diilustrasikan dalam Tabel 3.

Tabel 3. Hasil Proses Enkripsi dan Pembentukan *QR Code*

Id Dokumen	Hasil Enkripsi RSA	*QR Code*
DOK20231109234624393	drFxxx2Bk5aVaJeVYmm XZmppaWVpaZcxxx3D	

Dalam serangkaian langkah untuk menerapkan tanda tangan digital pada dokumen surat Pengantar RT, Ketua RT akan menjalankan proses validasi terhadap dokumen surat yang telah diinput ke dalam *web* E-RTSignParitBaru. Sebelum memberikan tanda tangan digital, Ketua RT diwajibkan untuk menyertakan informasi terlebih dahulu untuk tanda tangan digital menyesuaikan surat yang akan ditanda tangan. Setelah memasukkan data informasi untuk tanda tangan digital dan menyimpannya, dokumen siap untuk mengikuti tahap Tanda Tangan Enkripsi. Ketua RT kemudian menginisiasi proses Tanda Tangan Enkripsi, yang melibatkan proses enkripsi RSA. Hasil dari enkripsi RSA akan dihasilkan dalam bentuk *QR Code* sebelum ditempatkan pada dokumen surat. Halaman proses tanda tangan digital oleh Ketua RT dapat ditemukan pada Gambar 6.

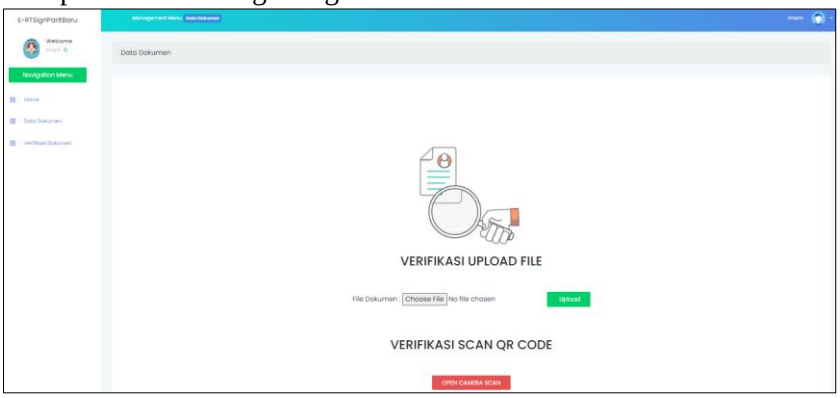


Gambar 6. Halaman Proses Tanda Tangan Digital

3.4 Proses Verifikasi Tanda Tangan Digital

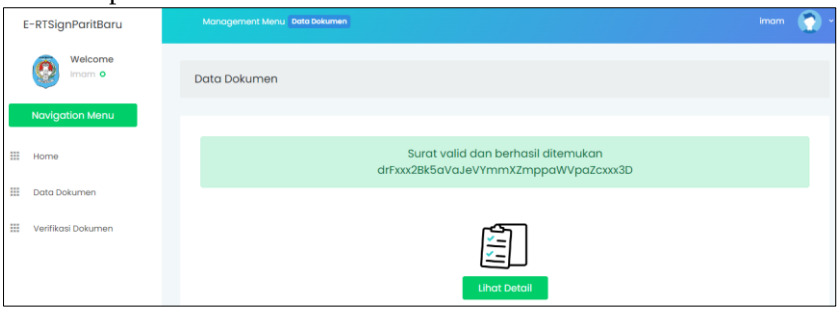
Proses verifikasi tanda tangan digital berperan dalam memverifikasi keaslian dokumen surat yang dikeluarkan oleh Kantor Desa Parit Baru melalui situs *web* E-RTSignParitBaru. Setiap

dokumen surat yang diterbitkan dan telah mendapatkan tanda tangan digital memiliki suatu kode unik yang dihasilkan melalui enkripsi menggunakan algoritma RSA. Kode unik hasil enkripsi tersebut kemudian dimasukkan ke dalam sebuah gambar berformat *QR Code*. Untuk membaca kode yang tersemat dalam *QR Code*, dapat dilakukan dengan menggunakan pembaca *QR Code*. Gambar 7 menunjukkan halaman yang digunakan untuk melakukan verifikasi dokumen surat yang telah mendapatkan tanda tangan digital.

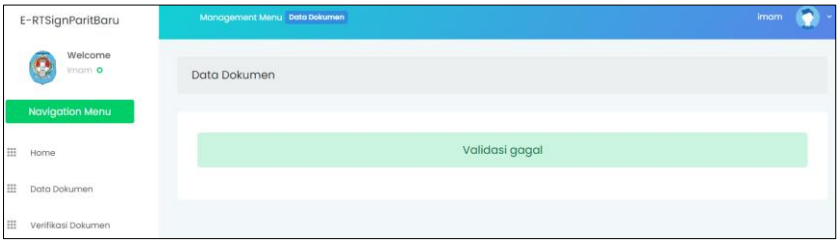


Gambar 7. Halaman Verifikasi Dokumen Surat

Sesudah meng*upload file* dokumen surat atau mens*can QR Code* pada dokumen surat, sistem akan menjalankan proses dekripsi menggunakan algoritma RSA. *Output* dari proses dekripsi akan diurai untuk mengambil Id dokumen, yang kemudian digunakan sebagai parameter dalam pencarian dokumen surat dalam sistem. Jika dokumen surat ditemukan dalam sistem, itu menandakan bahwa dokumen surat tersebut memiliki keabsahan dan telah mendapatkan tanda tangan digital. Sebaliknya, jika tidak ditemukan maka dokumen surat dianggap tidak valid. Gambar 8 dan 9 merupakan halaman hasil verifikasi dokumen valid dan tidak valid.



Gambar 8. Halaman Verifikasi Hasil Keabsahan Dokumen dengan Tanda Tangan Digital



Gambar 9. Halaman Verifikasi Hasil Ketidakvalidan Dokumen

3.5 Hasil Tanda Tangan Digital

Setiap surat yang berhasil mendapatkan tanda tangan digital akan dilengkapi dengan *QR Code* yang dihasilkan melalui proses enkripsi menggunakan algoritma RSA. Penggunaan *QR Code* dipilih untuk menyematkan informasi tanda tangan digital guna mengoptimalkan proses penyisipan hasil enkripsi algoritma RSA [5], mengingat algoritma RSA menghasilkan tanda

tangan digital dengan panjang yang cukup besar, sehingga mempersulit penyisipan kode pada dokumen surat. Ilustrasi 10 menampilkan contoh dokumen surat yang telah mendapatkan tanda tangan digital melalui algoritma RSA.

Gambar 10. Dokumen Surat dengan Tanda Tangan Digital

3.6 Hasil Pengujian Enkripsi dan Dekripsi Metode RSA

Pengujian enkripsi dan dekripsi metode RSA dilakukan untuk mengetahui sistem E-RTSignParitBaru yang dibuat dapat menandatangani dokumen surat dengan algoritma RSA yang dibubuhkan dalam *QR Code* dan memverifikasi dokumen yang dihasilkan oleh sistem E-RTSignParitBaru. Terdapat 15 data yang digunakan untuk menilai keberhasilan proses enkripsi dan dekripsi. Tabel 4 memuat hasil dari pengujian proses enkripsi.

Tabel 4. Hasil Pengujian Proses Enkripsi ke dalam *QR Code*

No.	Id Dokumen	Hasil Enkripsi RSA	Hasil Konversi Ke Dalam *QR Code*	Berhasil? (Ya / Tidak)
1.	DOK20231109234624393	drFxxx2Bk5aVaJeVYmmXZmppaWVpaZcxxx3D		Ya
2.	DOK20231009073401347	drFxxx2Bk5aVaJeUYmmVamlnZ2JpZJsxxx3D		Ya
3.	DOK20231009073538851	drFxxx2Bk5aVaJeUYmmVamloamluZZUxxx3D		Ya
4.	DOK20231009073652599	drFxxx2Bk5aVaJeUYmmVamlpbGNraZ0xxx3D		Ya
5.	DOK20231009073917159	drFxxx2Bk5aVaJeUYmmVamlsaGhnZZ0xxx3D		Ya
6.	DOK20231009074125584	drFxxx2Bk5aVaJeUYmmVampkaWZraJgxxx3D		Ya
7.	DOK20231009074234472	drFxxx2Bk5aVaJeUYmmVamplamVqZ5Yxxx3D		Ya
8.	DOK20231009074430662	drFxxx2Bk5aVaJeUYmmVampnamFsZpYxxx3D		Ya

No.	Id Dokumen	Hasil Enkripsi RSA	Hasil Konversi Ke Dalam *QR Code*	Berhasil? (Ya / Tidak)
9.	DOK20231009074628789	drFxxx2Bk5aVaJeUYmmVamppaWltaJ0xxx3D		Ya
10.	DOK20231009074746860	drFxxx2Bk5aVaJeUYmmVampqa2duZpQxxx3D		Ya
No.	**Id Dokumen**	**Hasil Enkripsi RSA**	**Hasil Konversi Ke Dalam *QR Code***	**Berhasil? (Ya / Tidak)**
11.	DOK20231009074900844	drFxxx2Bk5aVaJeUYmmVampsZ2FuZJgxxx3D		Ya
12.	DOK20231009075056900	drFxxx2Bk5aVaJeUYmmVamtjbGdvYJQxxx3D		Ya
13.	DOK20231009075218625	drFxxx2Bk5aVaJeUYmmVamtlaGlsYpkxxx3D		Ya
14.	DOK20231009075339482	drFxxx2Bk5aVaJeUYmmVamtmampqaJYxxx3D		Ya
15.	DOK20231009075651629	drFxxx2Bk5aVaJeUYmmVamtpbGJsYp0xxx3D		Ya

Berdasarkan Tabel 4 hasil pengujian proses enkripsi ke dalam *QR Code* yang dilakukan dari 15 data asli yang di enkripsi menunjukkan 15 data percobaan berhasil sehingga akurasi sistem dapat mengenali seluruh data. Tabel 5 menggambarkan hasil dari pengujian proses dekripsi.

Tabel 5. Hasil Pengujian Proses Dekripsi *QR Code*

No.	*QR Code*	Konversi ke Kode Enkripsi RSA	Kode Enkripsi RSA yang asli	Sesuai? (Ya / Tidak)	Dekripsi Kode Enkripsi RSA Menjadi Id Dokumen	Id Dokumen yang asli	Sesuai? (Ya / Tidak)
1.		drFxxx2Bk5aVaJeVYmmXZmppaWVpaZcxxx3D	drFxxx2Bk5aVaJeVYmmXZmppaWVpaZcxxx3D	Ya	DOK20231109234624393	DOK2023110921092346243 93	Ya
2.		drFxxx2Bk5aVaJeUYmmVamlnZ2JpZJsxxx3D	drFxxx2Bk5aVaJeUYmmVamlnZ2JpZJsxxx3D	Ya	DOK20231009073401347	DOK2023109073401347	Ya
3.		drFxxx2Bk5aVaJeUYmmVamloamluZZUxxx3D	drFxxx2Bk5aVaJeUYmmVamloamluZZUxxx3D	Ya	DOK20231009073538851	DOK2023109073538851	Ya
4.		drFxxx2Bk5aVaJeUYmmVamlpbGNraZ0xxx3D	drFxxx2Bk5aVaJeUYmmVamlpbGNraZ0xxx3D	Ya	DOK20231009073652599	DOK2023109073652599	Ya
5.		drFxxx2Bk5aVaJeUYmmVamlsaGhnZZ0xxx3D	drFxxx2Bk5aVaJeUYmmVamlsaGhnZZ0xxx3D	Ya	DOK20231009073917159	DOK2023109073917159	Ya
6.		drFxxx2Bk5aVaJeUYmmVampkaWZraJgxxx3D	drFxxx2Bk5aVaJeUYmmVampkaWZraJgxxx3D	Ya	DOK20231009074125584	DOK2023109074125584	Ya

No.	*QR Code*	Konversi ke Kode Enkripsi RSA	Kode Enkripsi RSA yang asli	Sesuai? (Ya / Tidak)	Dekripsi Kode Enkripsi RSA Menjadi Id Dokumen	Id Dokumen yang asli	Sesuai? (Ya / Tidak)
7.		drFxxx2Bk5aVaJeUYmmVamplamVqZ5Yxxx3D	drFxxx2Bk5aVaJeUYmmVamplamVqZ5Yxxx3D	Ya	DOK20231009074234472	DOK2023100907423447 2	Ya
8.		drFxxx2Bk5aVaJeUYmmVampnamFsZpYxxx3D	drFxxx2Bk5aVaJeUYmmVampnamFsZpYxxx3D	Ya	DOK20231009074430662	DOK2023100907443066 2	Ya
9.		drFxxx2Bk5aVaJeUYmmVamppaWltaJ0xxx3D	drFxxx2Bk5aVaJeUYmmVamppaWltaJ0xxx3D	Ya	DOK20231009074628789	DOK2023100907462878 9	Ya
10.		drFxxx2Bk5aVaJeUYmmVampqa2duZpQxxx3D	drFxxx2Bk5aVaJeUYmmVampqa2duZpQxxx3D	Ya	DOK20231009074746860	DOK2023100907474686 0	Ya
11.		drFxxx2Bk5aVaJeUYmmVampsZ2FuZJgxxx3D	drFxxx2Bk5aVaJeUYmmVampsZ2FuZJgxxx3D	Ya	DOK20231009074900844	DOK2023100907490084 4	Ya
12.		drFxxx2Bk5aVaJeUYmmVamtjbGdvYJQxxx3D	drFxxx2Bk5aVaJeUYmmVamtjbGdvYJQxxx3D	Ya	DOK20231009075056900	DOK2023100907505690 0	Ya
13.		drFxxx2Bk5aVaJeUYmmVamtlaGlsYpkxxx3D	drFxxx2Bk5aVaJeUYmmVamtlaGlsYpkxxx3D	Ya	DOK20231009075218625	DOK2023100907521862 5	Ya
14.		drFxxx2Bk5aVaJeUYmmVamtmampqaJYxxx3D	drFxxx2Bk5aVaJeUYmmVamtmampqaJYxxx3D	Ya	DOK20231009075339482	DOK2023100907533948 2	Ya
15.		drFxxx2Bk5aVaJeUYmmVamtpbGJsYp0xxx3D	drFxxx2Bk5aVaJeUYmmVamtpbGJsYp0xxx3D	Ya	DOK20231009075651629	DOK2023100907565162 9	Ya

Berdasarkan Tabel 5 hasil pengujian dekripsi *QR Code* ke data asli yang dilakukan dari 15 data *QR Code* (hasil enkripsi) yang di dekripsi menunjukkan 15 data percobaan berhasil sehingga akurasi sistem dapat mengenali seluruh data.

4. KESIMPULAN

Dari penelitian yang telah dilakukan, dapat ditarik kesimpulan sebagai berikut:

1. Proses pengamanan data dalam konteks tanda tangan digital *QR Code*, melalui hasil pengujian pada 15 data, menunjukkan bahwa data *plaintext* berhasil dienkripsi, dan data *ciphertext* yang ditampilkan kembali di *website* berhasil didekripsikan. Hal ini menandakan bahwa proses pengamanan data menggunakan Algoritma Kriptografi RSA berjalan dengan baik.
2. Akurasi sistem dalam men-*scan QR Code* yang terenkripsi, dengan hasil pengujian terhadap 15 data *QR Code* (hasil enkripsi) berhasil di *scan QR Code* dan menampilkan data asli *QR Code* terenkripsi, sehingga akurasi sistem dapat mengenali seluruh data.

5. SARAN

Berikut adalah beberapa saran untuk penelitian yang dapat dilakukan selanjutnya:

1. Sistem dapat dikembangkan untuk dapat menandatangani format selain Docx, seperti PDF atau format lain yang umum digunakan dalam proses administrasi surat-menyurat.
2. Untuk pengembangan selanjutnya, implementasi sistem berbasis *mobile* dapat dipertimbangkan guna meningkatkan fleksibilitas sistem secara keseluruhan.

UCAPAN TERIMA KASIH

Penulis ingin menyampaikan rasa syukur kepada Allah SWT atas kesuksesan penyelesaian penelitian ini. Terima kasih juga disampaikan kepada orang tua dan teman-teman yang telah memberikan dukungan, baik dalam bentuk motivasi maupun dukungan finansial, selama proses penelitian ini.

DAFTAR PUSTAKA

[1] W. K. Sandy, A. W. Widodo and Y. A. Sari, "Penentuan Keaslian Tanda Tangan Menggunakan *Shape Feature Extraction Techniques* Dengan Metode Klasifikasi *K Nearest Neighbor* dan *Mean Average Precision*," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer,* Vols. Vol. 2, No. 3, pp. 1083-1091, 2018.

[2] R. A. Azdy, "Tanda tangan Digital Menggunakan Algoritme *Keccak* dan RSA," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI),* pp. 184-191, 2016.

[3] D. P. Precilia and A. Izzuddin, "Aplikasi Tanda Tangan Digital (*Digital Signature*) Menggunakan Algoritma *Message Digest* 5 (MD5)," *Precilia, D. P., & Izzuddin, A. (2015). Aplikasi Tanda Tangan DigitaEnergy-Jurnal Ilmiah Ilmu-Ilmu Teknik,* vol. Vol. 5 No. 1, pp. 14-19, 2015.

[4] Y. Anshori, A. Y. E. Dodu dan D. M. P. M. P. Wedananta, "Implementasi Algoritma Kriptografi *Rivest Shamir Adleman* (RSA) pada Tanda Tangan Digital," *Tecno.Com,* pp. 110-121, 2019.

[5] I. B. G. Sarasvananda and I. B. A. I. Iswara, "Tanda Tangan Elektronik Menggunakan Algoritma *Rivest Shamir Adleman* (RSA) pada Sistem Informasi Surat Menyurat LPIK INSTIKI," *Jurnal SISFOKOM (Sistem Informasi dan Komputer),* pp. 289-296, 2022.

[6] I. S. E. Jatri and P. H. Utomo, "Pengaplikasian Kriptosistem *Rivest Shamir Adleman* (RSA) Pada Tanda Tangan Elektronik," *(PROSIDING) Seminar Nasional Matematika dan Sains,* pp. 112-121, 2021.

[7] M. F. Andrika dan A. Fitriansyah, "Aplikasi Penandatanganan Dokumen Secara Digital Menggunakan Metode *Advanced Encryption Standard* (AES) (Studi Kasus : Fmipa Universitas Riau)," *Jurnal Aplikasi Komputer,* pp. 1-12, 2021.

[8] F. Ariyanto and S. , "Implementasi *Digital Signature* Dan *Quick Response Code* Pada Aplikasi Kuitansi Digital," *JIKO (Jurnal Informatika dan Komputer),* pp. 125-131, 2022.

[9] L. Wicaksono, "Ketahanan Algoritma RSA Terhadap *Brute Force Attack*," *Doctoral dissertation, Universitas Islam Negeri Maulana Malik Ibrahim,* 2013.

[10] F. D. I. Mulyana, A. P. Heryani and V. Khoirunnisa, "Implementasi *Metode Rivest Shamir Adleman* untuk Enkripsi dan Dekripsi," *Jurnal Informatika dan Teknologi Komputer (J-ICOM),* pp. 32-39, 2022.