SENAFTI
SEMINAR NASIONAL MAHASISWA
FAKULTAS TEKNOLOGI INFORMASI

5th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
7 September 2024 – Jakarta, Indonesia
Volume 3, Nomor 2, September 2024 - ISSN 2962-8628 (*online*)

PENERAPAN ALGORITMA RSA PADA TANDA TANGAN DIGITAL DALAM SURAT KETERANGAN PENGANTAR ONLINE DI LINGKUNGAN RT.05/RW.04 PERUMAHAN BUANA GARDENIA PINANG KOTA TANGERANG

Riznandjaya Shafahad[1*], Mufti[2]

[1,2]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta Selatan, Indonesia

Email: [1*]2011500549@student.budiluhur.ac.id, [2*]mufti_hayat@yahoo.com
(* : corresponding author)

Abstrak- Surat pengantar adalah dokumen resmi yang dikeluarkan oleh Ketua Rukun Tetangga (RT) untuk memberikan penjelasan terkait keperluan administratif seperti pengajuan izin, mengurus administrasi kependudukan, atau sebagai syarat dalam proses atau pengurusan kegiatan tertentu. Pada lingkungan RT.05/RW.04 Perumahan Buana Gardenia Pinang Kota Tangerang, peneliti mengidentifikasi sebuah permasalahan, yaitu masih diterapkannya sistem pembuatan surat keterangan pengantar secara manual. Padahal kondisi yang ada saat ini sebagian besar warga memiliki kesibukan yang tinggi, termasuk Ketua RT. Jadi antara warga dengan Ketua RT sulit mempunyai kesempatan untuk bertemu secara langsung, sehingga menjadi suatu kendala apabila warga memiliki keperluan terhadap Ketua RT, khususnya keperluan yang mendesak. Untuk mengatasi permasalahan tersebut, lingkungan RT.05/RW.04 Perumahan Buana Gardenia Pinang Kota Tangerang membutuhkan sistem pembuatan surat keterangan pengantar berbasis *website*. Dengan kehadiran dan penerapan sistem ini diharapkan dapat menghemat waktu dan tenaga bagi warga yang mengajukan, Ketua RT yang memverifikasi, serta Ketua RW yang memvalidasi surat, karena sistem ini dapat diakses kapanpun dan dimanapun. Maka peneliti memutuskan untuk membuat sistem pembuatan surat keterangan pengantar berbasis *website* dengan menerapkan algoritma kriptografi RSA dan hash MD5 dalam pembentukan tanda tangan digital berupa *QR Code* yang tertera pada surat tersebut. Rata-rata kecepatan proses *hashing* yang dihasilkan adalah 0.04112 detik, sedangkan rata-rata kecepatan proses enkripsi yang dihasilkan adalah 0.18365 detik. Selanjutnya, hasil yang didapat dari penerapan kombinasi kedua algoritma ini adalah keaslian dokumen yang dihasilkan dapat dibuktikan, yaitu dengan memindai *QR Code* yang sebelumnya dihasilkan sebagai tanda tangan digital. Pemindaian *QR Code* tersebut kemudian akan menghasilkan *link URL*, yang ketika dibuka di *browser* akan menampilkan halaman hasil validasi dokumen yang status keasliannya sedang dibuktikan. Rata-rata kecepatan dekripsi yang dihasilkan adalah 0.163 milidetik.

Kata Kunci: Surat Keterangan Pengantar, Tanda Tangan Digital, Algoritma *Rivest Shamir Adleman* (RSA), *Hash Message Digest* 5 (MD5).

APPLICATION OF THE RSA ALGORITHM TO DIGITAL SIGNATURES IN ONLINE INTRODUCTION LETTER IN THE NEIGHBORHOOD OF RT.05/RW.04 RESIDENTIAL BUANA GARDENIA PINANG KOTA TANGERANG

Abstract- *A cover letter is an official document issued by the Head of the Neighborhood Unit to provide explanations regarding administrative needs such as applying for permits, managing population administration, or as a requirement in the process or management of certain activities. In the neighborhood of RT.05/RW.04 Buana Gardenia Pinang Housing, Tangerang City, researchers identified a problem, namely that the system for making introductory certificates manually is still implemented. Despite the current conditions, most residents are very busy, including the Head of the Neighborhood Association. It is difficult for residents and the Head of the Neighborhood Association to have the opportunity to meet in person, so it becomes an obstacle if residents have a need for the Head of the Neighborhood Unit, especially an urgent need. To overcome this problem, the neighborhood of RT.05/RW.04 Buana Gardenia Pinang Housing, Tangerang City requires a website-based system for creating introductory certificates. With the presence and implementation of this system, it is hoped that it will save time and energy for the residents who apply, the Head of the Neighborhood Association who verifies, and the Head of the Neighborhood Association who validates the letter, because this system can be accessed anytime and anywhere. The researchers decided to create a system for creating website-based introductory certificates by applying the RSA cryptographic algorithm and MD5 hash in forming a digital signature in the form of a QR Code printed on the letter. The average speed of the resulting hashing process is 0.04112 seconds, while the average speed of the resulting encryption process is 0.18365 seconds. Furthermore, the result obtained from applying the combination of these two algorithms is that the authenticity of the resulting document can be proven, namely by scanning the QR Code that was previously generated as a digital signature. Scanning the QR Code will then produce a URL link, which when opened in a browser will display a page of document validation results whose authenticity status is being proven. The average decryption speed produced was 0.163 milliseconds.*

Keywords:*Introductory Statement Letter, Digital Signature, Rivest Shamir Adleman (RSA) Algorithm, Hash Message Digest 5 (MD5).*

1. PENDAHULUAN

Surat pengantar adalah dokumen formal yang memungkinkan satu pihak berkomunikasi dengan pihak lain secara tertulis. Data ini dapat berupa pemberitahuan, laporan, ide, sanggahan, dan banyak lagi. Surat lamaran adalah jenis komunikasi formal yang disusun dan dikeluarkan atas nama individu dalam jabatan tertentu, seperti yang dikemukakan oleh Atmosudirdjo, S. Prajudi [1].

Optimalisasi pelayanan administrasi kepada masyarakat dilakukan melalui penerapan digitalisasi pelayanan publik secara meluas dengan memanfaatkan teknologi sistem informasi. Pelayanan pemerintah desa kini menjadi lebih cepat, responsif, dan disertai dengan informasi yang benar berkat digitalisasi pelayanan publik, yang berdampak positif secara langsung kepada masyarakat [2].

Masyarakat RT.05/RW.04 Perumahan Buana Gardenia Pinang, Kota Tangerang masih menggunakan pendekatan manual dalam membuat surat pengantar. Dalam prosedur berbasis kertas ini, warga harus terlebih dahulu mendatangi Ketua RT untuk mendapatkan formulir surat pengantar, yang kemudian harus mereka isi dan serahkan untuk ditandatangani oleh Ketua RT dan Ketua RW. Masalah muncul ketika Ketua RT sering tidak ada di tempat atau sulit mendapatkan waktu yang tepat untuk bertemu secara langsung dengan warga. Sehingga menjadikan pembuatan surat pengantar ini menyita banyak waktu dan sangat melelahkan, sedangkan di sisi lain tidak sedikit warga yang membutuhkan surat pengantar ini dengan segera. Maka dari itu, hal ini menjadi penghalang bagi pelayanan administrasi yang lebih baik di tingkat RT dan RW, karena warga belum mendapatkan pelayanan yang cepat dari pihak RT dan RW, maka diperlukan solusi kreatif untuk menghilangkannya.

Berdasarkan data penelitian yang dilakukan peneliti, rata-rata kondisi perekonomian warga RT.05/RW.04 Perumahan Buana Gardenia Pinang Kota Tangerang adalah kalangan menengah ke atas. Sebab seluruh kepala keluarga (atau yang mewakilinya) di lingkungan ini adalah pekerja, 60% di antaranya adalah pegawai swasta, 30% wiraswasta, dan 10% adalah PNS. Oleh karena itu, warga di lingkungan ini dapat dikategorikan sebagai orang-orang yang mampu, berkecukupan, dan paham teknologi.

Maka berawal dari permasalahan tersebut, serta ditambah dengan kondisi lingkungan yang mendukung, peneliti memutuskan untuk membuat sistem pembuatan surat keterangan pengantar *online* berbasis *website*. Sistem ini akan menerapkan algoritma RSA yang dikombinasikan dengan *hash* MD5 dalam pembentukan tanda tangan digital berupa *QR Code* yang ada pada surat tersebut.

Status keaslian dokumen dapat diketahui dengan memindai *QR Code* yang sebelumnya dihasilkan sebagai tanda tangan digital. Pemindaian *QR Code* tersebut kemudian akan menghasilkan *link URL*, yang ketika dibuka di *browser* akan menampilkan halaman hasil validasi dokumen yang status keasliannya sedang dibuktikan. Dengan adanya proses validasi dokumen, maka dimungkinkan untuk mendeteksi dokumen palsu yang dipalsukan oleh pihak yang tidak bertanggung jawab.

Oleh karena itu, kehadiran dan penerapan sistem pembuatan surat keterangan pengantar *online* berbasis website di lingkungan RT.05/RW.04 Perumahan Buana Gardenia Pinang Kota Tangerang ini diharapkan dapat memudahkan warga dalam membuat surat keterangan pengantar, terlebih ketika dibutuhkan dalam keadaan mendesak. Sistem ini juga dapat menghemat waktu dan tenaga bagi warga yang mengajukan, Ketua Rukun Tetangga (RT) yang memverifikasi, serta Ketua Rukun Warga (RW) yang memvalidasi surat, karena sistem ini dapat diakses kapan dan dimana saja.

Sebuah penelitian yang diterbitkan dalam jurnal *peer-review* berjudul "Implementasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritme Elgamal pada Dokumen di Balai Pendidikan dan Pelatihan Penerbangan (BP3) Curug Berbasis Web" [3].

Kaitan penelitian ini dengan penelitian pada jurnal tersebut yaitu terdapat pada proses memproteksi atau mengamankan *file* dokumen dalam tanda tangan digital dengan cara enkripsi dan dekripsi. Sedangkan perbedaan dengan penelitian pada jurnal tersebut adalah fungsi *hash* yang digunakan untuk perancangan tanda tangan digital pada penelitian ini menggunakan algoritma MD5, sedangkan penelitian pada jurnal tersebut menggunakan algoritma SHA-256.

Kontribusi peneliti dalam penelitian ini terletak pada hasil penyisipan tanda tangan digital yang disisipkan dalam bentuk *QR Code*, serta proses verifikasi dokumen yang dilakukan dengan cara memindai *QR Code* yang dihasilkan untuk melihat status keaslian dokumen.

Sumber daya *online* yang biasanya dapat diakses melalui *World Wide Web* dikenal sebagai situs *web*. Kemampuan untuk mengaksesnya dari mana saja di seluruh dunia kapan saja bergantung pada konektivitasnya ke internet. Halaman *web* secara teknis adalah halaman yang merupakan bagian dari domain atau subdomain tertentu [4].

Tanda tangan digital adalah metode kriptografi untuk menandatangani dokumen elektronik. Prosesnya melibatkan pembuatan nilai hash (ringkasan pesan) dari dokumen, lalu mengenkripsinya dengan kunci pribadi pengirim. Dokumen yang sudah dienkripsi ini menjadi tanda tangan digital. Tanda tangan digital memberikan keandalan, keaslian, dan integritas dokumen, mirip dengan tanda tangan kertas pada dokumen fisik [5].

Kriptografi adalah bidang keilmuan yang berhubungan dengan teknik enkripsi. Teknik ini melibatkan pengacakan informasi asli, yang dikenal sebagai *plaintext*, menggunakan kunci enkripsi untuk menghasilkan teks acak yang disebut *ciphertext. Ciphertext* ini dirancang untuk menjadi tantangan bagi orang yang tidak berwenang untuk menguraikannya, karena mereka tidak memiliki kunci dekripsi. Masalah ini diselesaikan melalui penggunaan kunci yang digunakan dalam proses enkripsi dan dekripsi [6].

Pada tahun 1970-an, Whitfield Diffie dan Martin Hellman memperkenalkan enkripsi asimetris, menggunakan pasangan kunci satu untuk enkripsi dan satu untuk dekripsi. Kunci publik dapat digunakan untuk mendekripsi pesan, tetapi hanya penerima dengan kunci rahasia yang dapat membaca pesan tersebut. Penemuan ini meningkatkan keamanan komunikasi digital dan menjadi dasar bagi protokol keamanan internet modern seperti SSL/TLS. Kontribusi Diffie dan Hellman sangat penting dalam perkembangan teknologi informasi dan komunikasi [7].

MD5 (*Message-Digest algorithm* 5) adalah fungsi hash kriptografi yang menghasilkan nilai *hash* 128-bit dan dirancang oleh Ronald Rivest pada tahun 1991 sebagai pengganti MD4. MD5 mengubah pesan dengan panjang berbeda menjadi *output* 128-bit melalui pemrosesan blok 512-bit dalam 4 putaran. Meskipun awalnya populer untuk pemeriksaan integritas *file* dan keamanan internet, kerentanan signifikan ditemukan pada tahun 1996 dan 2004, yang mengurangi keandalannya dan mendorong penggunaan algoritma alternatif seperti SHA-1. *Hash* MD5 biasanya direpresentasikan sebagai angka heksadesimal 32 digit [8].

Algoritma RSA dikembangkan oleh Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1970-an, Untuk menghormati pembuatnya, metode ini menggunakan namanya. Metode ini berbeda dengan penyelesaian algoritma diskrit karena bergantung pada tingkat kesulitan faktorisasi bilangan bulat. Prosedur pengangkatan hanya digunakan oleh RSA. Enkripsi asimetris digunakan oleh RSA, sebuah teknik kriptografi, yang menggunakan pasangan kunci publik dan kunci privat [9]

2. METODE PENELITIAN

2.1 Metode Pengumpulan Data

Berdasarkan masalah yang diidentifikasi pada langkah sebelumnya, langkah ini melibatkan pengumpulan data. Selama proses ini, kami melakukan hal-hal seperti:

a. Studi Literatur, Untuk mengatasi masalah yang ada-khususnya implementasi tanda tangan digital dengan menggunakan algoritma RSA dan *Hash* MD5-para peneliti melakukan tinjauan literatur, yang meliputi pengumpulan, analisis, dan pembacaan referensi dari berbagai macam sumber, termasuk buku, jurnal, makalah, internet, dan lain-lain.
b. Wawancara, Melakukan wawancara dengan Ketua RT.05/RW.04 Perumahan Buana Grdenia Pinang Kota Tangerang untuk mendapatkan informasi dan dokumen yang dibutuhkan dalam menyelesaikan permasalahan yang ada.
c. Observasi, Melihat langsung keadaan lingkungan terkait yang diriset dalam penelitian ini, melihat alur proses dokumen, serta mempelajari dokumen yang digunakan untuk mengumpulkan data perancangan sistem.

2.2 Tahapan Penerapan Fungsi Hash MD5

Algoritma MD5 menerima nilai dengan panjang berapa pun sebagai masukan dan mengembalikan hasil 128-bit. Menggunakan nilai masukan yang beragam untuk menghasilkan hasil keluaran yang sama secara komputasi tidak mungkin dilakukan. Kecepatan algoritme ini dioptimalkan untuk digunakan dengan tanda tangan digital dan kompatibel dengan komputer berarsitektur 32-bit. Sebuah peningkatan dari pendahulunya, metode MD4, algoritma MD5 tidak membutuhkan tabel substitusi yang besar. Beberapa fase membentuk algoritma MD5, termasu:

a. *Append Padding Bit,* Jika panjang setiap blok pesan tidak sama dengan 448 modulo512, maka panjang pesan akan bertambah. Dengan menambahkan bit 1 dan 0, panjang pesan dinaikkan ke tingkat yang kompatibel dengan 448 modulus 512. Jumlah total bit yang ditambahkan adalah antara satu hingga lima ratus lima puluh satu.
b. *Append Lenght,* Pada bilangan bulat biner 64-bit, jumlah panjang pesan sebelum bit padding keluar. Bila panjang pesan melebihi 264 bit, maka 64 bit dari urutan terendah yang digunakan.
c. *Initialize MD Buffer*, Untuk penghitungan ini, empat buffer 32-bit (A, B, C, dan D) digunakan. Berikut ini tabel 1 adalah angka heksadesimal yang digunakan untuk menginisialisasi keempat buffer:

Tabel 1. *Initialize MD Buffer*

No.	Angka Heksadesimal
A	01234567
B	89ABCDEF
C	FEDCBA98
D	76543210

d. *Process Message in 16-Word Blocks*, Menentukan empat fungsi lain yang mengambil argumen 32-bit dan mengembalikan hasil 32-bit. Pada tabel 2 adalah simbol yang digunakan untuk mewakili fungsi tambahan:

Tabel 2. *Process Message in 16-Word Blocks*

No.	Fungsi
1	F(X,Y,Z) = (X ^ Y) v (~X ^ Z)
2	G(X,Y,Z) = (X ^ Z) v (Y ^ ~Z)
3	H(X,Y,Z) = (X □ Y □ Z)
4	I(X,Y,Z) = Y □ (X v ~Z)

Mirip dengan fungsi F, fungsi G, H, dan I menghasilkan *output* X, Y, dan Z secara paralel bitwise. Ini berarti bahwa jika bit X, Y, dan Z independen dan tidak bias, maka setiap bit dari *output* G, H, dan I juga independen dan tidak bias. Pada tahap ini, fungsi sinus digunakan untuk menghasilkan tabel T 64 elemen. Berikut ini adalah Tabel 3 yang berisi elemen T dan pemisalan notasinya pada Tabel 4.

Tabel 3. Tabel Elemen T

D76AA478	E8C7B756	242070DB	C1BDCEEE	F57C0FAF	X4787C62A	A8304613	FD469501
698098D8	8B44F7AF	FFFF5BB1	895CD7BE	6B901122	FD987193	A679438E	49B40821
F61E2562	C040B340	265E5A51	E9B6C7AA	D62F105D	02441453	D8A1E681	E7D3FBC8
21E1CDE6	C33707D6	F4D50D87	455A14ED	A9E3E905	FCEFA3F8	676F02D9	8D2A4C8A
FFFA3942	8771F681	6D9D6122	FDE5380C	A4BEEA44	4BDECFA9	F6BB4B60	BEBFBC70
289B7EC6	EAA127FA	D4EF3085	04881D05	D9D4D039	E6DB99E5	1FA27CF8	C4AC5665
F4292244	432AFF97	AB9423A7	FC93A039	655B59C3	8F0CCC92	FFEFF47D	85845DD1
6FA87E4F	FE2CE6E0	A3014314	4E0811A1	F7537E82	BD3AF235	2AD7D2BB	EB86D391

Tabel 4. Permisalan Notasi

No.	Notasi
1	Ronde 1: Misalkan [abcd k s i] dinotasikan sebagai berikut: a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s)
2	Ronde 2: Misalkan [abcd k s i] dinotasikan sebagai berikut: a = b + ((a + G(b,c,d) + X[k] + T[i]) <<< s)
3	Ronde 3: Misalkan [abcd k s i] dinotasikan sebagai berikut: a = b + ((a + H(b,c,d) + X[k] + T[i]) <<< s)
4	Ronde 4: Misalkan [abcd k s i] dinotasikan sebagai berikut: a = b + ((a + I(b,c,d) + X[k] + T[i]) <<< s).
5	Langkah selanjutnya adalah menambahkan empat register dengan nilai sebelum operasi pada blok ini dimulai: A = A+AA, B = B+BB, C = C+CC, D = D+DD

e. *Output*, Nilai A, B, C, dan D terdiri dari *Message Digest* yang dihasilkan sebagai *output*. Dimulai dengan *byte* dengan urutan terendah (A) dan diakhiri dengan *byte* dengan urutan tertinggi (D) [10].

2.3 Tahapan Penerapan Algoritma RSA

Algoritma RSA terdiri dari 3 proses, yaitu:

a. Pembangkit Kunci, Proses pembentukan atau pembangkitan kunci algoritma RSA yaitu:
   1. Pilih dua bilangan prima acak ukuran besar, p dan q.
   2. Hitung modulus sistem pada persamaan (1).

$$\mathbf{n = p * q} \quad (1)$$

   3. Cari persamaan (2) *Totient* Φ (n)

$$\mathbf{\Phi(n) = (p-1)(q-1)} \quad (2)$$

   4. Pilih persamaan (3) dimana kunci enkripsi e secara acak

Dimana 1 < e < Φ (n), gcd (e, Φ (n)) = 1 (3)

5. Selesaikan rumus (4) berikut untuk menentukan kunci dekripsi d.

d ≡ e-1 (mod Φ(n)) (4)

dimana ekivalen dengan persamaan (5):

e * d ≡ 1 (mod Φ(n)), dimana 0 ≤ d ≤ n (5)

sehingga dihasilkan:

1. *Private key* = (d, n), Bersifat sangat rahasia, dan hanya penerima pesan yang boleh mengetahuinya.
2. *Public key* = (e, n), Bersifat tidak rahasia, dan boleh disebarkan dengan bebas.

b. Enkripsi, Secara umum proses enkripsi dengan RSA dilakukan dengan rumus (6) sebagai berikut:

$$C_i = P_i^{e} \bmod n \quad (6)$$

Tetapi pada penelitian ini, enkripsi dilakukan dengan menggunakan *private key*, bukan dengan *public key*, kebalikan dari proses enkripsi secara umum dengan RSA. Hal ini bertujuan agar hanya pengirim pesan yang dapat membangkitkan *digital signature* dari data yang dikirim. Jika saat proses pengiriman *intruder* melakukan *modification* atau *fabrication* terhadap data, maka *intruder* tidak akan dapat membangkitkan *digital signature* yang sesuai dikarenakan intruder tidak memiliki *private key* yang sesuai [9].
Sehingga proses enkripsi pada penelitian ini sesuai persamaan (7) berikut:

$$C_i = P_i^{d} \bmod n \quad (7)$$

c. Dekripsi, Secara umum proses dekripsi dengan RSA dilakukan dengan rumus (8) sebagai berikut:

$$P_i = C_i^{d} \bmod n \quad (8)$$

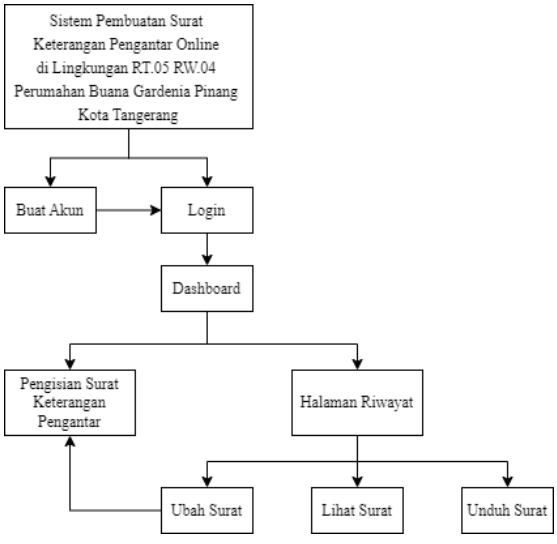
Tetapi pada penelitian ini, proses deskripsi menggunakan *public key*, bukan *private key*. Hal ini dimaksudkan agar setiap penerima dapat menguji keaslian *file*. Sehingga proses deskripsi pada penelitian ini sesuai persamaan (9) berikut:

$$P_i = C_i^{e} \bmod n \quad (9)$$

2.4 Rancangan Menu

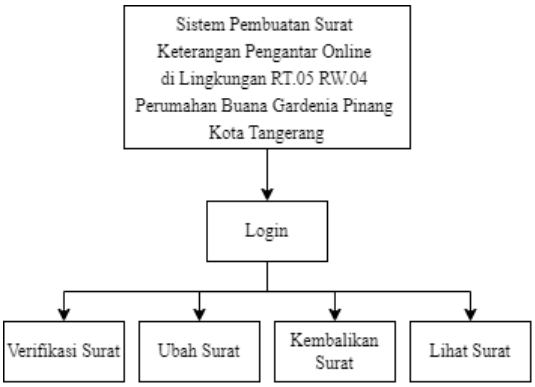
Rancangan menu pada sistem pembuatan surat keterangan pengantar *online* untuk lingkungan RT.05/RW.04 Perumahan Buana Gardenia Pinang Kota Tangerang dengan menerapkan algoritma RSA adalah seperti gambar 1 - gambar 3 berikut.

a. Rancangan Menu *User* Warga. Rancangan menu untuk *user* warga ditunjukkan pada gambar 1.



Gambar 1. Rancangan Menu *User* Warga

b. Rancangan Menu *User* RT. Rancangan menu untuk *user* RT ditunjukkan pada gambar 2.



Gambar 2. Rancangan Menu *User* RT

c. Rancangan Menu *User* RW. Rancangan menu untuk *user* RW ditunjukkan pada gambar 3.

Gambar 3. Rancangan Menu *User* RW

3. HASIL DAN PEMBAHASAN

Waktu yang ditawarkan untuk menyelesaikan seluruh proses pembuatan surat keterangan pengantar *online* menggunakan sistem ini adalah 15 sampai 30 menit. Sedangkan apabila menggunakan sistem yang lama membutuhkan waktu beberapa jam bahkan sampai hitungan hari.

3.1 Tahapan Pembuatan Kunci

Pada tahap pembentukan kunci bertujuan untuk membangkitkan kunci privat dan kunci publik. Kunci privat digunakan dalam pembentukan tanda tangan digital, sedangkan kunci publik digunakan untuk verifikasi. Pada proses ini menggunakan algoritma RSA. Contoh implementasi tahapan-tahapan untuk pembuatan kuncinya adalah sebagai berikut.

a. P = 7, q= 11
b. N = p x q = 7 x 11 = 77
c. $\phi(n)=(p-1)(q-1)=(7-1)(11-1)=6\times10=60$
d. Kunci privat (d,n) = (29,77)
e. Kunci publik (e,n) = (3,77)

3.2 Tahapan Proses Pembentukan Tanda Tangan Digital

a. *Hashing*, Teknik MD5 digunakan untuk mengubah file teks menjadi *message digest*, yang merupakan langkah pertama dalam membuat tanda tangan digital. Hasil *message digest* dari teks *file* dapat dilihat pada tabel 5 berikut.

Tabel 5. *Message Digest* Teks Dokumen

Teks pada Dokumen	***Message Digest***
Teks pada dokumen surat 009	dfca64b89ad6d472c6466ddf6a03d114

b. *Enkripsi*, Untuk membuat tanda tangan digital, intisari pesan Tabel 6 harus dienkripsi terlebih dahulu dengan kunci privat RSA yang telah dibuat sebelumnya.

Tabel 6. Konversi *Message Digest*

Message Digest	dfca64b89ad6d472c6466ddf6a03d114
***Message Digest* Menjadi Nilai Desimal**	223 202 100 184 154 214 212 114 198 70 109 223 106 3 209 20

Kemudian tanda tangani *hash* tersebut dengan kunci privat (*d*,*n*) menggunakan rumus enkripsi yaitu $C = P^d \bmod n$ sesuai tahapan pada Tabel 7. Dimana Tabel 8 merupakan hasil *C* adalah tanda tangan digital.

Tabel 7. Proses Enkripsi

Kunci Privat	$d = 29$
	$n = 77$
Rumus Enkripsi	$C = P^d \bmod n$
Proses Enkripsi	Menghitung $223202100184154214212114198701092231063209^{29} \bmod 77$ $223202100184154214212114198701092231063209 \bmod 77 = 43$ Menghitung $43^{29} \bmod 77$ Mengubah 29 ke bentuk biner: $29_{10} = 11101_2$ Menghitung pangkat: $43^1 = 43 \bmod 77$ $43^2 = 43 \times 43 = 1849 \bmod 77 = 6$ $43^4 = 62 = 36 \bmod 77 = 36$ $43^8 = 362 = 1296 \bmod 77 = 25$ $43^{16} = 252 = 625 \bmod 77 = 9$ Gabungkan berdasarkan biner 11101: $43^{29} = 43^{16} \times 43^8 \times 43^4 \times 43^1$ Menghitung: $9 \times 25 = 225 \bmod 77 = 55$ $55 \times 36 = 1980 \bmod 77 = 31$ $31 \times 43 = 1333 \bmod 77 = 26$ $223202100184154214212114198701092231063209^{29} \bmod 77 = 26$

Tabel 8. Hasil Tanda Tangan Digital

Hasil Enkripsi	sdRyaP0bmt2KwcXUNUeatOwi7AKclaxgh/yZ2G T8mSAFvPk8VboeaRchBI9z3nSAQB3nIWIq1U3 v5O/QvjZkXkch8HXOdzl+o5tv7pW8gmajmqrww ExNYbpY5M3ZZVwjCVWldsLphGXTVXHjCY p6hCZnKSd8zdKNvRcy3gmJqixiGgzX8TZIDb8 KZvMT3wMlWK4xb9/poK4SQ9JCXufNa9+kY NwMl2BnWhQCoyZ6GLHMAZ/moKCdayzGcL 6E+da+XgoBevcbHz9hN77kxsPbXsY9DShOQX QZYUtjrWzc+phdDRo3psnYJ/0IHYeRsl18c/wb9 Z7Mm/fm1DitTyTR4Q==

3.3 Tahapan Proses Verifikasi

Untuk memastikan bahwa data tersebut asli, prosedur verifikasi dijalankan. Langkah-langkah untuk memverifikasi tanda tangan digital adalah sebagai berikut.

a. *Hashing file* yang diterima, Teks *file* yang diterima kembali dilakukan *hashing* dengan algoritna MD5 untuk menghasilkan *message digest*. Hasil *hash* dari teks *file* dapat dilihat pada tabel 9.
b. Dekripsi, menggunakan kunci publik RSA dan rumus P = C e mod n untuk menguraikan tanda tangan digital. Setelah mendekripsi tanda tangan digital, sebuah intisari pesan dihasilkan. Intisari Tabel 10 ini dibandingkan dengan intisari pesan file asli.

Tabel 9. Proses Dekripsi

Kunci Publik	$e = 3$
	$n = 77$
Rumus Dekripsi	$P = C^{e} \bmod n$
Proses Dekripsi	Menghitung 26^3 $26^1 = 26$ $26^2 = 26 \times 26 = 676$ $676 \bmod 77 = 61$ Kemudian dikalikan lagi dengan 26: $26^3 = 26^2 \times 26 \equiv 61 \times 26$ Menghitung: $61 \times 26 = 1586$ $1586 \bmod 77 \equiv 37$ Hasil Akhir: $26^3 \bmod 77 = 37$

Tabel 10. Hasil Dekripsi

Hasil Dekripsi	3031300d060960864801650304020105000420f2e caece37be9c543f80163aff737c5d2d7de811f977e3 ea237505488afc6304

c. Perbandingan *message digest*, Akhirnya, keabsahan dokumen telah diperiksa. Kita sekarang memiliki dua intisari pesan: satu dari *hashing* file teks yang diterima dan satu lagi dari dekripsi tanda tangan digital menggunakan kunci publik.

Tabel 11. Hasil Verifikasi

***Message Digest* Teks pada dokumen**	dfca64b89ad6d472c6466ddf6a03d114
***Message Digest* Hasil Dekripsi**	dfca64b89ad6d472c6466ddf6a03d114

Keabsahan dari dokumen yang diterima telah dikonfirmasi oleh temuan verifikasi pada Tabel 11. Untuk alasan sederhana, mendekripsi *message digest* menghasilkan hasil yang sama dengan *message digest* file teks asli.

3.4 Pengujian Enkripsi dan Dekripsi Algoritma RSA

Pengujian pada penelitian ini bertujuan untuk memastikan bahwa sistem yang dibuat dapat bekerja seperti yang diharapkan. Dari 10 contoh pengujian enkripsi dokumen menggunakan algoritma RSA dan *hash* MD5 yang telah dilakukan, maka dihasilkan rata-rata kecepatan proses *hashing*-nya yaitu sebesar 0.04112 detik. Sedangkan rata-rata kecepatan enkripsinya yaitu sebesar 0.18365 detik. Kemudian juga dari 10 contoh pengujian dekripsi dokumen dengan melakukan pemindaian *QR Code*, maka dihasilkan rata-rata kecepatan proses dekripsinya yaitu sebesar 0.163 milidetik.

4. KESIMPULAN

Dari hasil studi serta pembahasan yang sudah dilaksanakan, peneliti meyimpulkan bahwa sistem pembuatan surat keterangan pengantar *online* berbasis *website* sangat bermanfaat bagi warga RT.05/RW.04 Perumahan Buana Gardenia Pinang Kota Tangerang dengan mempercepat pelayanan dari pihak RT dan RW. Kombinasi algoritma RSA dan hash MD5 efektif dalam membuat tanda tangan digital berupa *QR Code*, dengan kecepatan *hashing* rata-rata 0.04112 detik dan enkripsi 0.18365 detik. Selain itu, kedua algoritma ini juga efektif dalam validasi dokumen, dengan rata-rata kecepatan dekripsi 0.163 milidetik, serta mampu menjaga keaslian dokumen dari pemalsuan. Kekurangan dari sistem ini antara lain belum adanya petunjuk cara penggunaan dan alur kerja aplikasi, belum adanya notifikasi terkait perkembangan proses surat yang muncul pada perangkat masing-masing pengguna, sehingga masing-masing pengguna harus mengeceknya secara manual, serta aplikasi ini belum dikembangkan dalam versi *mobile*. Oleh karena itu, saran dari peneliti untuk mengembangkan sistem ini adalah agar semua kekurangan yang telah disebutkan dapat direalisasikan.

DAFTAR PUSTAKA

[1] E. Setyawati, Suyudi, F. A. Gunantara, and H. Wijoyo, "Sistem Informasi Pelayanan Administrasi Surat Pengantar Berbasis Website dengan Framework Codeigniter Guna Meningkatkan Kualitas Pelayanan pada Desa Tambaksari Kidul Kabupaten Banyumas," *Jurnal Informasi dan komputer (JIK) STMIK Dian Cipta Cendikia Kotabumi*, vol. 9, no. 1, pp. 22–31, 2021.

[2] F. Vauzia, N. W. Kirana, P. P. Rosulindo, U. Wusqo, and M. Akmal, "Pembuatan dan Pelatihan Penggunaan Aplikasi Permohonan Surat Keterangan Berbasis Website Di Desa Sariwangi," *SEWAGATI, Jurnal Pengabdian Kepada Masyarakat*, vol. 8, no. 1, pp. 1116–1125, 2024.

[3] V. H. Zulian and P. Purwanto, "Implementasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritme Elgamal pada Dokumen di Balai Pendidikan dan Pelatihan Penerbangan (BP3) Curug Berbasis Web," Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI), vol. 1, no. 1, pp. 386–393, Sep. 2022.

[4] M. H. Romadhon, Y. Yudhistira, and Mukrodin, "Sistem Informasi Rental Mobil Berbsasis Android dan Website Menggunakan Framework Codeigniter 3 Studi Kasus : Cv Kopja Mandiri," *Jurnal Sistem Informasi Dan Teknologi Peradaban (JSITP)*, vol. 2, no. 1, pp. 30–36, 2021.

[5] Y. Anshori, A. Y. E. 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, May 2019.

[6] H. Mursid, J. Supardi, and M. Q. Rizkie, "Pengujian Integritas File Operasi Tanda Tangan Digital Menggunakan Kombinasi Hash MD5, RSA dan Skema QR-Cod," *Jurnal Generic*, vol. 14, no. 2, pp. 30–37, Jul. 2022, doi: 10.18495/generic.v14i2.135.

[7] Muh. Taufiqurrahman, Irawan, and I. Syamsuddin, "Perancangan Sistem Tanda Tangan Digital (Digital Signature)," Prosiding Seminar Nasional Teknik Elektro dan Informatika (SNTEI) 2020, pp. 60–65, Oct. 2020.

[8] M. H. Santoso, N. D. Girsang, H. Siagian, A. Wahyudi, and B. A. Sitorus, "Perbandingan Algoritma Kriptografi Hash MD5 Dan SHA-1," Prosiding Seminar Nasional Teknologi Informatika (SEMANTIKA), vol. 2, no. 1, pp. 54–59, Nov. 2019.

[9] B. K. Hutasuhut, S. Efendi, and Z. Situmorang, "Digital Signature Untuk Menjaga Keaslian Data dengan Algoritma MD5 dan Algoritma RSA," *InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan)*, vol. 3, no. 2, pp. 164–169, Mar. 2019, doi: 10.30743/infotekjar.v3i2.1019.

[10] I. Saputra and S. D. Nasution, "Perbandingan Performa Algoritma MD5 dan SHA-256 dalam Membangkitkan Identitas File," *Jurnal Sains Komputer dan Informatika (J-SAKTI)*, vol. 6, no. 1, pp. 172–187, Mar. 2022.