JDSP
Jurnal Data Science Penusa

Implementasi Digital Signature Menggunakan Algoritma Rivest Shamir Adleman Pada Dokumen Elektronik

Kicky Maulana[1)*], Anita Sindar Ros Maryana Sinaga [2)]
[1)] STMIK Pelita Nusantara, [2)]STMIK Pelita Nusantara
[1)]kickymaulana@gmail.com, [2)]nitamaryana76@gmail.com

Received: 15 Agustus 2024 Accepted: 27 September 2024 Published: 27 Desember 2024
Pp. 842-850

OPEN ACCESS

***Penulis Koresponden**

Kata Kunci: Tanda Tangan Digital, Metode RSA, PDF

JDSP: Jurnal Data Science Penusa is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Abstrak : Kemajuan teknologi komputer telah memberikan banyak kemudahan dalam berbagai aspek kehidupan, namun juga membawa tantangan baru, terutama terkait keamanan dokumen elektronik. Salah satu tantangan utama adalah meningkatnya kasus pemalsuan dokumen digital, terutama yang menggunakan format Portable Document Format (PDF). Format ini menjadi pilihan populer untuk berbagai jenis dokumen karena sifatnya yang universal dan kemampuannya dalam mempertahankan tata letak asli. Namun, dengan kemudahan akses dan penggunaan PDF, muncul risiko pemalsuan dokumen, penambahan teks, hingga pemalsuan tanda tangan, yang dapat mengakibatkan penipuan dan pencurian identitas. Untuk mengatasi masalah ini, kriptografi menawarkan solusi dengan melindungi integritas dan keaslian dokumen. Algoritma Rivest-Shamir-Adleman (RSA) merupakan salah satu metode kriptografi kunci publik yang digunakan untuk enkripsi dan dekripsi data. Algoritma ini dirancang untuk menghasilkan pasangan kunci yang berbeda antara proses enkripsi dan dekripsi, sehingga hanya pihak yang memiliki kunci dekripsi yang dapat membaca pesan asli. Dalam penelitian ini, implementasi tanda tangan digital menggunakan algoritma RSA diterapkan pada dokumen elektronik dalam format PDF. Hasil penelitian menunjukkan bahwa penggunaan algoritma RSA dapat meningkatkan keamanan dokumen digital, mengurangi risiko pemalsuan, dan memastikan keaslian dokumen.

1. PENDAHULUAN

Kemajuan teknologi komputer telah membawa banyak perubahan dan dampak bagi kehidupan manusia. Teknologi komputer mempermudah komunikasi, akses informasi, pendidikan, ekonomi, kesehatan, dan mengakses informasi dengan cepat. Selain itu teknologi komputer juga memberi dampak negatif seperti kemudahan memalsukan dokumen.

Peningkatan penggunaan dokumen elektronik dalam era teknologi 4.0 telah menjadi hal yang umum karena efisiensi yang ditawarkan, baik dari segi waktu maupun biaya (Rifauddin., 2019). Berbagai instansi, perusahaan, dan organisasi memanfaatkan format dokumen elektronik seperti .docx, .xls, .pptx, dan .pdf (Krismayani., 2019) untuk menyimpan serta menyajikan informasi dengan lebih baik.

Di antara format tersebut, PDF menjadi pilihan populer karena kemampuannya untuk menjaga konsistensi data dan tampilan di berbagai perangkat, baik komputer maupun smartphone. Format file PDF banyak dipergunakan sebab dapat mengkonversi berjenis-jenis file (.jpg, exel, ppt). Meskipun PDF menawarkan banyak keuntungan, format ini mudah dipalsukan. Oknum tak bertanggung jawab dapat mengubah isi, menambahkan teks, dan memalsukan tanda tangan, penipuan dan pencurian identitas, maka diperlukan pengamanan dokumen dengan algoritma enkripsi.

Kriptografi dapat melindungi informasi melalui penggunaan algoritme kode, hash, dan tanda tangan. Algoritma Rivest-Shamir-Adleman (RSA) bagian dari kriptografi merupakan algoritma untuk enkripsi kunci

publik (public-key encryption). Algoritma kriptografi RSA didesain sesuai fungsinya menghasilkan kunci yang digunakan untuk enkripsi berbeda dari kunci yang digunakan untuk dekripsi pesan (Syahputra, 2021)

2. TINJAUAN LITERATUR

Kriptografi (cryptograpy) berasal dari bahasa Yunani yaitu dari kata "cryptos" dan "graphein" yang berarti tulisan rahasia. Sedangkan, definisi kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data (Chyan, 2018).

Tujuan Kriptografi merupakan empat aspek mendasar dari keamanan informasi (Putro, 2022), yaitu:

a. Kerahasiaan (confidentiality)

Kerahasiaan adalah layanan yang bertujuan untuk menjaga kerahasiaan pesan agar tidak dapat dibaca oleh pihak-pihak yang tidak berhak yang direalisasikan dengan mengubah pesan menjadi cipherteks.

b. Integritas data (data integrity)

Integritas data adalah layanan yang bertujuan untuk menjaga pesan dari perbuatan atau manipulasi oleh orang yang tidak berhak. Layanan integritas data diimplementasikan melalui tanda-tangan digital.

c. Otentikasi (authentication)

Otentikasi merupakan layanan yang bertujuan untuk mengidentifikasi informasi, baik informasi mengenai user yang berkomunikasi, maupun mengidentifikasi sumber informasi. Otentikasi juga diimplementasikan dengan tanda-tangan digital.

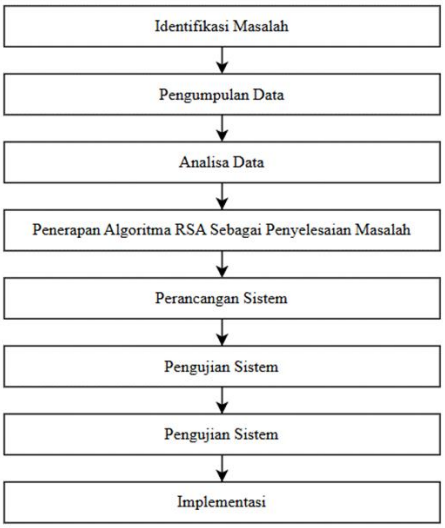
d. Nir penyangkalan (non-repudiation)

Nir penyangkalan merupakan layanan untuk mencegah adanya penyangkalan oleh pihak yang memberikan informasi maupun pihak yang menerima informasi. Nir penyangkalan juga diimplementasikan dengan tandan-tangan digital untuk mencegah penyangkalan oleh pihak pemberi informasi (Chafid, 2022).

Secara umum, fungsi hash merupakan suatu fungsi matematika yang dapat mengubah suatu data menjadi nilai integer yang relatif kecil. Dalam kriptografi, fungsi hash juga disebut fungsi hash kriptografi yang memiliki definisi yaitu fungsi yang menerima inputan string dengan panjang sembarang dan mengubahnya menjadi string yang panjangnya tetap.

METODE PENELITIAN

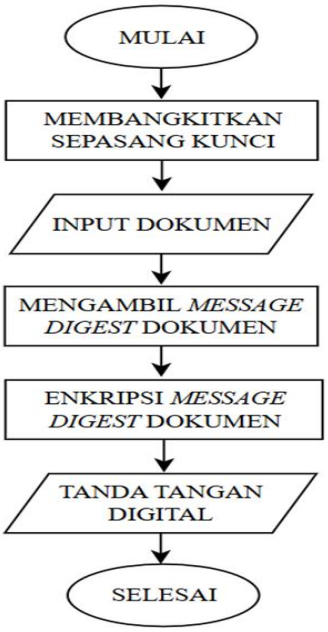
Untuk memperjelas metodologi penelitian, diperlukan sebuah kerangka kerja yang sistematis. Kerangka kerja ini menggambarkan langkah-langkah sistem yang akan diteliti dan bertujuan untuk memberikan arah pada penelitian. Prosesnya mencakup pengamatan hubungan sistem, penemuan solusi untuk masalah yang muncul, pemecahan masalah, analisis ulang sistem, dan penentuan kelayakan penerapan sistem dalam industri teknologi. Adapun kerangka kerja yang dibuat untuk penelitian ini dapat dilihat pada Gambar 1.



Gambar 1 Kerangka Kerja

HASIL PENELITIAN

Metode yang digunakan untuk mengimplementasikan tanda tangan digital pada suatu dokumen elektronik adalah Algoritma RSA. Algoritma RSA menerapkan proses enkripsi dan dekripsi yang membutuhkan kunci pubik dan kunci privat. Berikut merupakan proses pembentukan algoritma RSA yang di tunjukkan flowchart pada Gambar 2.



Gambar 2 Pembentukan Algoritma Rsa

Berikut merupakan proses enkripsi dan deskripsi dalam algoritma RSA berikut ini:

a. Menginputkan file berformat ekstensi .pdf. Contoh file berformat ekstensi .pdf ditunjukkan pada Gambar 3.



SURAT PERJANJIAN SEWA MENYEWA

Gambar 3 Contoh File Berekstensi .pdf

b. Mengenkripsi message digest dengan kriptografi algoritma RSA

Tabel 1 Enkripsi Kode ASCII Dari Message Digest Menggunkan Excel

No.	SHA-256	Formula Excel	ASCII	Privat d	Privat n	Rumus VBA	Enkripsi
1	b	=CODE(char)	98	13	299	=ModExp(ascii,d,n)	59
2	2	=CODE(char)	50	13	299	=ModExp(ascii,d,n)	154
3	9	=CODE(char)	57	13	299	=ModExp(ascii,d,n)	109
4	1	=CODE(char)	49	13	299	=ModExp(ascii,d,n)	101

5	2	=CODE(char)	50	13	299	=ModExp(ascii,d,n)	154
No.	SHA-256	Formula Excel	ASCII	Privat d	Privat n	Rumus VBA	Enkripsi
6	a	=CODE(char)	97	13	299	=ModExp(ascii,d,n)	136
7	8	=CODE(char)	56	13	299	=ModExp(ascii,d,n)	199
8	6	=CODE(char)	54	13	299	=ModExp(ascii,d,n)	41
9	0	=CODE(char)	48	13	299	=ModExp(ascii,d,n)	165
10	a	=CODE(char)	97	13	299	=ModExp(ascii,d,n)	136
11	a	=CODE(char)	97	13	299	=ModExp(ascii,d,n)	136
12	0	=CODE(char)	48	13	299	=ModExp(ascii,d,n)	165
13	c	=CODE(char)	99	13	299	=ModExp(ascii,d,n)	112
14	b	=CODE(char)	98	13	299	=ModExp(ascii,d,n)	59
15	4	=CODE(char)	52	13	299	=ModExp(ascii,d,n)	13
16	b	=CODE(char)	98	13	299	=ModExp(ascii,d,n)	59
17	a	=CODE(char)	97	13	299	=ModExp(ascii,d,n)	136
18	d	=CODE(char)	100	13	299	=ModExp(ascii,d,n)	87
19	d	=CODE(char)	100	13	299	=ModExp(ascii,d,n)	87
20	1	=CODE(char)	49	13	299	=ModExp(ascii,d,n)	101
21	6	=CODE(char)	54	13	299	=ModExp(ascii,d,n)	41
22	9	=CODE(char)	57	13	299	=ModExp(ascii,d,n)	109
23	1	=CODE(char)	49	13	299	=ModExp(ascii,d,n)	101
24	0	=CODE(char)	48	13	299	=ModExp(ascii,d,n)	165
25	a	=CODE(char)	97	13	299	=ModExp(ascii,d,n)	136
26	c	=CODE(char)	99	13	299	=ModExp(ascii,d,n)	112
27	e	=CODE(char)	101	13	299	=ModExp(ascii,d,n)	127
28	1	=CODE(char)	49	13	299	=ModExp(ascii,d,n)	101
29	0	=CODE(char)	48	13	299	=ModExp(ascii,d,n)	165
30	b	=CODE(char)	98	13	299	=ModExp(ascii,d,n)	59
31	b	=CODE(char)	98	13	299	=ModExp(ascii,d,n)	59
32	7	=CODE(char)	55	13	299	=ModExp(ascii,d,n)	81
33	3	=CODE(char)	51	13	299	=ModExp(ascii,d,n)	90
34	f	=CODE(char)	102	13	299	=ModExp(ascii,d,n)	245
35	e	=CODE(char)	101	13	299	=ModExp(ascii,d,n)	127
36	e	=CODE(char)	101	13	299	=ModExp(ascii,d,n)	127
37	9	=CODE(char)	57	13	299	=ModExp(ascii,d,n)	109
38	b	=CODE(char)	98	13	299	=ModExp(ascii,d,n)	59
39	9	=CODE(char)	57	13	299	=ModExp(ascii,d,n)	109
40	a	=CODE(char)	97	13	299	=ModExp(ascii,d,n)	136
41	e	=CODE(char)	101	13	299	=ModExp(ascii,d,n)	127
42	4	=CODE(char)	52	13	299	=ModExp(ascii,d,n)	13
43	7	=CODE(char)	55	13	299	=ModExp(ascii,d,n)	81
44	2	=CODE(char)	50	13	299	=ModExp(ascii,d,n)	154
45	c	=CODE(char)	99	13	299	=ModExp(ascii,d,n)	112
46	b	=CODE(char)	98	13	299	=ModExp(ascii,d,n)	59
47	9	=CODE(char)	57	13	299	=ModExp(ascii,d,n)	109

48	2	=CODE(char)	50	13	299	=ModExp(ascii,d,n)	154
No.	SHA-256	Formula Excel	ASCII	Privat d	Privat n	Rumus VBA	Enkripsi
49	6	=CODE(char)	54	13	299	=ModExp(ascii,d,n)	41
50	3	=CODE(char)	51	13	299	=ModExp(ascii,d,n)	90
51	0	=CODE(char)	48	13	299	=ModExp(ascii,d,n)	165
52	d	=CODE(char)	100	13	299	=ModExp(ascii,d,n)	87
53	7	=CODE(char)	55	13	299	=ModExp(ascii,d,n)	81
54	e	=CODE(char)	101	13	299	=ModExp(ascii,d,n)	127
55	3	=CODE(char)	51	13	299	=ModExp(ascii,d,n)	90
56	7	=CODE(char)	55	13	299	=ModExp(ascii,d,n)	81
57	a	=CODE(char)	97	13	299	=ModExp(ascii,d,n)	136
58	f	=CODE(char)	102	13	299	=ModExp(ascii,d,n)	245
59	5	=CODE(char)	53	13	299	=ModExp(ascii,d,n)	66
60	6	=CODE(char)	54	13	299	=ModExp(ascii,d,n)	41
61	8	=CODE(char)	56	13	299	=ModExp(ascii,d,n)	199
62	9	=CODE(char)	57	13	299	=ModExp(ascii,d,n)	109
63	c	=CODE(char)	99	13	299	=ModExp(ascii,d,n)	112
64	7	=CODE(char)	55	13	299	=ModExp(ascii,d,n)	81

c. Deskripsi atau verifikasi algoritma RSA
File yang diterima dengan format .txt atau bisa disebut juga sebagai file tanda tangan dipecah dengan pemisah tanda titik terlebih dahulu ke dalam bentuk tabel seperti yang ditunjukkan pada Tabel 2.

Tabel 2 Deskripsi File Tanda Tangan

No.	Enkripsi	Publik e	Publik n	Rumus VBA	ASCII	Rumus Excel	SHA-256
1	59	61	299	=ModExp(enkripsi,e,n)	98	=CHAR(char)	b
2	154	61	299	=ModExp(enkripsi,e,n)	50	=CHAR(char)	2
3	109	61	299	=ModExp(enkripsi,e,n)	57	=CHAR(char)	9
4	101	61	299	=ModExp(enkripsi,e,n)	49	=CHAR(char)	1
5	154	61	299	=ModExp(enkripsi,e,n)	50	=CHAR(char)	2
6	136	61	299	=ModExp(enkripsi,e,n)	97	=CHAR(char)	a
7	199	61	299	=ModExp(enkripsi,e,n)	56	=CHAR(char)	8
8	41	61	299	=ModExp(enkripsi,e,n)	54	=CHAR(char)	6
9	165	61	299	=ModExp(enkripsi,e,n)	48	=CHAR(char)	0
10	136	61	299	=ModExp(enkripsi,e,n)	97	=CHAR(char)	a
11	136	61	299	=ModExp(enkripsi,e,n)	97	=CHAR(char)	a
12	165	61	299	=ModExp(enkripsi,e,n)	48	=CHAR(char)	0
13	112	61	299	=ModExp(enkripsi,e,n)	99	=CHAR(char)	c
14	59	61	299	=ModExp(enkripsi,e,n)	98	=CHAR(char)	b
15	13	61	299	=ModExp(enkripsi,e,n)	52	=CHAR(char)	4
16	59	61	299	=ModExp(enkripsi,e,n)	98	=CHAR(char)	b
17	136	61	299	=ModExp(enkripsi,e,n)	97	=CHAR(char)	a
18	87	61	299	=ModExp(enkripsi,e,n)	100	=CHAR(char)	d
19	87	61	299	=ModExp(enkripsi,e,n)	100	=CHAR(char)	d

20	101	61	299	=ModExp(enkripsi,e,n)	49	=CHAR(char)	1
21	41	61	299	=ModExp(enkripsi,e,n)	54	=CHAR(char)	6
22	109	61	299	=ModExp(enkripsi,e,n)	57	=CHAR(char)	9
No.	Enkripsi	Publik e	Publik n	Rumus VBA	ASCII	Rumus Excel	SHA-256
23	101	61	299	=ModExp(enkripsi,e,n)	49	=CHAR(char)	1
24	165	61	299	=ModExp(enkripsi,e,n)	48	=CHAR(char)	0
25	136	61	299	=ModExp(enkripsi,e,n)	97	=CHAR(char)	a
26	112	61	299	=ModExp(enkripsi,e,n)	99	=CHAR(char)	c
27	127	61	299	=ModExp(enkripsi,e,n)	101	=CHAR(char)	e
28	101	61	299	=ModExp(enkripsi,e,n)	49	=CHAR(char)	1
29	165	61	299	=ModExp(enkripsi,e,n)	48	=CHAR(char)	0
30	59	61	299	=ModExp(enkripsi,e,n)	98	=CHAR(char)	b
31	59	61	299	=ModExp(enkripsi,e,n)	98	=CHAR(char)	b
32	81	61	299	=ModExp(enkripsi,e,n)	55	=CHAR(char)	7
33	90	61	299	=ModExp(enkripsi,e,n)	51	=CHAR(char)	3
34	245	61	299	=ModExp(enkripsi,e,n)	102	=CHAR(char)	f
35	127	61	299	=ModExp(enkripsi,e,n)	101	=CHAR(char)	e
36	127	61	299	=ModExp(enkripsi,e,n)	101	=CHAR(char)	e
37	109	61	299	=ModExp(enkripsi,e,n)	57	=CHAR(char)	9
38	59	61	299	=ModExp(enkripsi,e,n)	98	=CHAR(char)	b
39	109	61	299	=ModExp(enkripsi,e,n)	57	=CHAR(char)	9
40	136	61	299	=ModExp(enkripsi,e,n)	97	=CHAR(char)	a
41	127	61	299	=ModExp(enkripsi,e,n)	101	=CHAR(char)	e
42	13	61	299	=ModExp(enkripsi,e,n)	52	=CHAR(char)	4
43	81	61	299	=ModExp(enkripsi,e,n)	55	=CHAR(char)	7
44	154	61	299	=ModExp(enkripsi,e,n)	50	=CHAR(char)	2
45	112	61	299	=ModExp(enkripsi,e,n)	99	=CHAR(char)	c
46	59	61	299	=ModExp(enkripsi,e,n)	98	=CHAR(char)	b
47	109	61	299	=ModExp(enkripsi,e,n)	57	=CHAR(char)	9
48	154	61	299	=ModExp(enkripsi,e,n)	50	=CHAR(char)	2
49	41	61	299	=ModExp(enkripsi,e,n)	54	=CHAR(char)	6
50	90	61	299	=ModExp(enkripsi,e,n)	51	=CHAR(char)	3
51	165	61	299	=ModExp(enkripsi,e,n)	48	=CHAR(char)	0
52	87	61	299	=ModExp(enkripsi,e,n)	100	=CHAR(char)	d
53	81	61	299	=ModExp(enkripsi,e,n)	55	=CHAR(char)	7
54	127	61	299	=ModExp(enkripsi,e,n)	101	=CHAR(char)	e
55	90	61	299	=ModExp(enkripsi,e,n)	51	=CHAR(char)	3
56	81	61	299	=ModExp(enkripsi,e,n)	55	=CHAR(char)	7
57	136	61	299	=ModExp(enkripsi,e,n)	97	=CHAR(char)	a
58	245	61	299	=ModExp(enkripsi,e,n)	102	=CHAR(char)	f
59	66	61	299	=ModExp(enkripsi,e,n)	53	=CHAR(char)	5
60	41	61	299	=ModExp(enkripsi,e,n)	54	=CHAR(char)	6
61	199	61	299	=ModExp(enkripsi,e,n)	56	=CHAR(char)	8
62	109	61	299	=ModExp(enkripsi,e,n)	57	=CHAR(char)	9

63	112	61	299	=ModExp(enkripsi,e,n)	99	=CHAR(char)	c
64	81	61	299	=ModExp(enkripsi,e,n)	55	=CHAR(char)	7

Sesuaikan dengan salah satu daftar kunci publik seperti yang ditunjukkan pada Tabel 3

Tabel 3 Daftar Kunci Publik

No.	Nama	Kunci Publik	
		E	N
1	Wancara Siregar, S.Kom.	99	134
2	Antonius Pangaribuan	72	60
3	Kicky Maulana	61	299
4	Supran Manggala	77	27
5	Gojek Salman	99	80
6	Hani Anjeli	88	234

Sesuaikan hasil deskripsi dengan hasil pengubahan dari Kode ASCII ke karakter untuk melihat apakah nilainya sama atau tidak. Jika sama, maka file benar-benar ditandatangani oleh pemilik file dan belum pernah diubah oleh orang lain. Hal tersebut menandakan file tersebut asli. Sementara jika tidak sama, maka file tersebut tidak asli dan tidak valid. Contoh kesesuaian antara Kode Hashing dari file .pdf dan perubahan Kode ASCII ke karakter SHA-256 ditunjukkan pada Tabel 4.

Tabel 4 Perbandingan Antara Kode dari File .pdf dan Perubahan Kode ASCII

Kode Hashing Fungsi SHA-256 dari File .pdf	Kode Hasil Perubahan dari Kode ASCII ke Karakter SHA-256
"b2912a860aa0cb4badd16910ace10bb73fee9b9ae472cb92630d7e37af5689c7"	"b2912a860aa0cb4badd16910ace10bb73fee9b9ae472cb92630d7e37af5689c7"

PEMBAHASAN

Tahap ini berkaitan dengan hasil sistem yang telah dibagun, berikut ini adalah hasil dari sistem yang telah dibangun.

a. Tampilan Login

Halaman login digunakan untuk masuk ke aplikasi, pengguna harus memasukkan username dan password yang sesuai pada form tersebut, halaman login juga digunakan agar mencegah pengguna yang menyalahgunakan aplikasi. Tampilan halaman login ditunjukkan pada Gambar 4.



Gambar 4 Tampilan Halaman Login

b. Tampilan Pembangkit Kunci
Dalam tampilan pembangkit kunci berisi informasi mengenai nilai bilangan p dan q, setelah nilai di inputkan maka dapat di hitung dengan menggunakan rumus setelah itu pilih nilai e nya agar dapat menghitung nilai d nya. Adapun tampilan halaman pembangkit kunci ditunjukkan pada Gambar 5.



Gambar 6 Tampilan Halaman Pembangkit Kunci

c. Tampilan Penandatanganan Dokumen
Pada tampilan tandatanganin dokumen terlebih dahulu pilih dokumen yang diinginkan. Setelah itu isikan nilai bilangan d dan bilangan n nya. Lalu pilih menu tandatangani dokumen



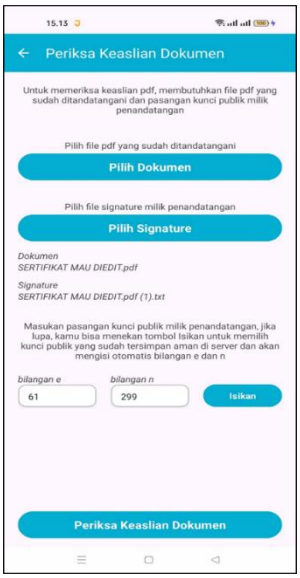
Gambar 7 Tampilan Halaman Penandatanganan Dokumen

d. Tampilan Periksa Keaslian Dokumen
Pada tampilan periksa keaslian dokumen terlebih dahulu pilih dokumen setelah dokumen terpilih pilih menu signature setelah itu isikan bilangan e dan bilangan n. Setelah pilih pilih menu periksa keaslian dokumen.

KESIMPULAN

Adapun kesimpulan yang didapat dari penelitian ini adalah sebagai berikut:
a. Telah diterapkan algoritma RSA pada dokumen elektronik dan mampu mengenkripsi suatu file yang telah ditandatangani;
b. Telah dirancang dan dibangun sistem Digital Signature dengan menggunakan algoritma RSA berbasis Android dan dapat menjamin keamanan dokumen yang ditandatanganinya dalam aspek integrity,

authentication, dan non-repudiation; dan
c. Pembangkitan kunci pada algoritma RSA memastikan bahwa hanya pasangan kunci yang digunakan untuk proses enkripsi, yang dapat digunakan pada proses dekripsinya.



Gambar 8 Tampilan Halaman Periksa Keaslian Dokumen

REFERENCES

Carles Andi Saputra G, C. A. (2023). Analisis Perbandingan Algoritma Kriptografi Data Encryption Standard Dan Advanced Encryption Standard Pada Proses Enkripsi Dan Dekripsi File Dokumen. *(Doctoral Dissertation, Universitas Dehasen Bengkulu)*. .

Chafid, N. (2022). Impelementasi Algoritma Kriptografi Klasik Caesar Untuk Rancang Bangun Aplikasi E-Voting Berbasis Web. . *Jurnal Ilmiah Sains Dan Teknologi*, 136-137.

Chyan, P. (2018). Penerapan Sistem Kriptografi Enkripsi Jamak Dan Tanda Tangan Digital Dalam Mendukung Keamanan Informasi. *Tematika: Jurnal Penelitian Teknik Informatika Dan Sistem Informasi*, 39-46.

Krismayani., A. G. (2019). "Penerimaan Aplikasi E-Dokumen Di Pt Pelindo Iii Cabang Tanjung. . *Jurnal Ilmu Perpustakaan,,,* 261–270.

Putro, S. S. (2022). Peranan Kriptografi Dalam Keamanan Data Pada Jaringan Komputer. *Jurnal Ilmiah Kursor, 3(2)*. .

Rifauddin., M. (2019). Pengelolaan Arsip Elektronik Berbasis Teknologi. *Khizanah Al-Hikmah: Jurnal Ilmu,*, 168–178.

Syahputra, A. (2021). Implementasi Algoritma Freivlds Untuk Pembangkitan Kunci Algoritma Rsa Pada Pengamanan Data Video. . *Pelita Informatika: Informasi Dan Informatika*, 70-77.

Toresa, D. P. (2023). Pelatihan Dasar Jaringan Komputer Untuk Siswa Teknik Komputer Dan Jaringan (Tkj) Smk Migas Inovasi Riau. *J-COSCIS: Journal of Computer Science Community Service, 3(1),*, 27-32.

Wirawan, L. S. (2020). Implementasi Digital Signature Menggunakan Algoritma Rsa Dan Fungsi Hash Md5 Untuk Aplikasi Sms Di Handphone Berbasis Java. *Karya Ilmiah*, 23-80.