Implementasi Algoritma RSA Untuk Keamanan Data Pasien Menggunakan Teknologi *QR CODE*

Implementation of RSA Algorithm For Securing Patient Data using QR Code Technology

Adi Fajaryanto Cobantoro[1)], Fadhlullah Yoga Wicahyono[2)], Ismail Abdurrozzaq Z[3)]

[1), 2), 3)] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Ponorogo
Email : adifajaryanto@umpo.ac.id[1)], fadhlullahyoga21@gmail.com[2)], ismail@umpo.ac.id[3)]

Abstrak

Perkembangan teknologi digital menuntut peningkatan sistem keamanan, terutama dalam perlindungan data pribadi pengguna. Salah satu sektor yang sangat bergantung pada kerahasiaan data adalah sektor kesehatan, di mana informasi pasien harus dilindungi dari potensi kebocoran dan penyalahgunaan. Penelitian ini bertujuan untuk mengimplementasikan algoritma kriptografi RSA (Rivest-Shamir-Adleman) dalam sistem registrasi pasien di praktik dokter gigi Regunawati Cahyaningsih. RSA dipilih karena sifatnya yang asimetris dan kemampuannya dalam menjaga keamanan data melalui penggunaan pasangan kunci publik dan privat. Selain itu, penelitian ini juga menggabungkan QR Code sebagai media akses terhadap data terenkripsi, guna mempercepat dan menyederhanakan proses otorisasi data. Proses enkripsi dilakukan pada informasi penting seperti NIK, nama, alamat, nomor telepon, dan rekam medis sebelum disimpan dalam database. Berdasarkan hasil pengujian, sistem menunjukkan performa yang sangat baik dari sisi fungsionalitas, akurasi algoritma, dan kecepatan tampilan. Pengujian Whitebox memastikan keakuratan implementasi algoritma RSA dengan akurasi 100%. Pengujian performa dengan metrik Largest Contentful Paint (LCP) menunjukkan waktu muat yang sangat cepat, antara 0.5 hingga 2.3 milidetik, dengan skor performa 100, sehingga sistem dinilai responsif dan optimal dari sisi pengalaman pengguna. Dengan demikian, RSA terbukti efektif dalam meningkatkan keamanan data pasien dan menjaga kerahasiaan informasi dalam sistem informasi klinik berbasis web.

Kata kunci: *Algoritma Rivest-Shamir-Adleman, Keamanan Data Pasien, Pengujian Whitebox, QR Code*

Abstract

The advancement of digital technology demands improved security systems, especially in protecting users' personal data. One sector that heavily relies on data confidentiality is the healthcare sector, where patient information must be safeguarded from potential leaks and misuse. This study aims to implement the RSA (Rivest-Shamir-Adleman) cryptographic algorithm in the patient registration system at the dental clinic of Regunawati Cahyaningsih. RSA was chosen for its asymmetric nature and its ability to ensure data security through the use of public and private key pairs. Additionally, this study integrates QR Code technology as a medium for accessing encrypted data, streamlining and accelerating the data authorization process. The encryption process is applied to important information such as NIK, name, address, phone number, and medical records before being stored in the database. Based on the testing results, the system demonstrated excellent performance in terms of functionality, algorithm accuracy, and display speed. Whitebox testing confirmed the accuracy of the RSA algorithm implementation with 100% accuracy. Performance testing using the Largest Contentful Paint (LCP) metric showed very fast load times, ranging from 0.5 to 2.3 milliseconds, with a performance score of 100, making the system highly responsive and optimal in terms of user experience. Therefore, RSA is proven to be effective in enhancing patient data security and maintaining confidentiality within a web-based clinical information system.

Keywords: *Rivest-Shamir-Adleman Algorithm, Patient Data Security, Whitebox Testing, QR Code*

1. PENDAHULUAN

Perkembangan ilmu pengetahuan dan teknologi di Indonesia telah membawa dampak signifikan terhadap kehidupan masyarakat, terutama dalam bidang keamanan siber[1]. Menurut [2], keamanan siber berperan penting dalam melindungi data dan sistem teknologi dari ancaman, serangan, serta akses tidak sah guna menjaga integritas, kerahasiaan, dan ketersediaan informasi. Hal serupa diungkapkan oleh [3], yang menambahkan bahwa perlindungan tersebut juga mencakup upaya menjaga privasi data pribadi, melindungi keberlanjutan operasional bisnis, serta memastikan stabilitas dan keandalan infrastruktur vital, seperti jaringan data[4]. Sejalan dengan itu, [5] menekankan bahwa keamanan siber tidak hanya menjadi fondasi dalam pengembangan

teknologi yang lebih maju tetapi juga berperan dalam meningkatkan kesadaran masyarakat mengenai pentingnya perlindungan data pribadi. Berdasarkan pendapat para ahli, dapat disimpulkan bahwa keamanan siber memiliki peran yang sangat penting dalam melindungi data dan sistem teknologi dari berbagai ancaman, serangan, serta akses tidak sah. Keamanan siber tidak hanya menjaga integritas, kerahasiaan, dan ketersediaan informasi, tetapi juga memastikan privasi data pribadi, keberlanjutan operasional bisnis, serta stabilitas infrastruktur vital. Selain itu, keamanan siber berperan sebagai dasar pengembangan teknologi yang lebih maju dan meningkatkan kesadaran masyarakat terhadap pentingnya perlindungan data.

Kebocoran data menjadi isu serius yang sering terjadi di Indonesia[6]. Berdasarkan data dari perusahaan keamanan siber *Surfshark*, Indonesia berada di peringkat ketiga dunia untuk kasus kebocoran data terbanyak pada tahun 2022, dengan lebih dari 12 juta akun terdampak. Salah satu contoh adalah kebocoran data pengguna Tokopedia yang terjadi pada 20 Maret 2020, seperti dilaporkan oleh CNN Indonesia. Dalam insiden ini, seorang peretas bernama "*whysodank*" berhasil mencuri data sekitar 91 juta pengguna, termasuk nomor telepon, email dengan *hash password*, dan nama pengguna, yang kemudian dijual di *dark web* seharga 74 juta[7]. Kasus serupa terjadi di sektor perbankan pada Bank Syariah Indonesia (BSI), yang diretas oleh seorang peretas asal Rusia pada 8 Mei 2023[8]. *Hacker* tersebut berhasil mencuri dan mengakses sekitar 1,5 *gigabyte* data pribadi pengguna, termasuk nama lengkap, nomor telepon, lokasi, saldo rekening, riwayat transaksi, detail pembukaan rekening, informasi pekerjaan, dan data lainnya. Data nasabah BSI ini kemudian diperjualbelikan di pasar gelap atau *dark web*. Kejadian serupa terjadi pada BPJS Kesehatan, badan hukum pemerintah yang mengelola jaminan kesehatan masyarakat. Pada akhir Mei 2021, BPJS Kesehatan mengalami kebocoran data peserta, meliputi NIK, nama, alamat, nomor telepon, email, hingga 20 juta data yang dilengkapi foto peserta[9]. Data ini juga dilaporkan dijual di *dark web*. Kebocoran tersebut menimbulkan dampak serius, baik secara materiil maupun immateriil, serta mengurangi kepercayaan masyarakat terhadap keamanan pengelolaan data oleh instansi pemerintah maupun swasta.

Kasus-kasus ini menunjukkan adanya kerentanan tinggi terhadap privasi dan keamanan data pribadi, serta lemahnya perlindungan pada institusi yang menjadi target. Kerentanan ini terjadi karena sistem keamanan data yang belum memadai sehingga mudah ditembus oleh pihak-pihak yang tidak bertanggung jawab. Dampak kebocoran data bisa memicu pencurian identitas, manipulasi mata uang, atau bahkan penyalahgunaan data untuk tujuan kriminal[3]. Selain itu, data yang tidak akurat dapat merusak reputasi perusahaan atau organisasi yang mengelolanya, karena pengguna mungkin kehilangan kepercayaan terhadapnya. Oleh karena itu, menjaga privasi menjadi semakin penting di era digital saat ini[10].

Untuk mengatasi masalah kebocoran data, penelitian ini mengimplementasikan enkripsi di tingkat database menggunakan algoritma RSA (*Rivest-Shamir-Adleman*), sebuah metode kriptografi asimetris yang menggunakan pasangan kunci publik dan privat. Kontribusi utama dari penelitian ini adalah penerapan algoritma kriptografi RSA pada sistem informasi pasien untuk mengenkripsi data sensitif di tingkat basis data, sehingga hanya dapat diakses oleh pihak yang memiliki kunci privat. Selain itu, penelitian ini mengintegrasikan QR Code sebagai media penyimpanan dan akses data terenkripsi guna mempercepat proses otorisasi informasi secara aman. Kombinasi antara RSA dan QR Code memberikan solusi konkret terhadap isu keamanan data pasien, memperkuat kepercayaan pengguna, serta mendukung penerapan standar perlindungan informasi di lingkungan praktik medis berbasis digital.

2. DASAR TEORI

2.1 Keamanan Data

Keamanan data adalah serangkaian praktik dan proses yang bertujuan melindungi data dari akses yang tidak sah, kerusakan, atau pencurian selama siklus hidupnya. Keamanan data sangat penting dalam dunia teknologi informasi, karena data yang tidak dilindungi dapat menyebabkan dampak buruk, seperti kerugian finansial, kerusakan reputasi, dan pelanggaran privasi[11].

2.2 Kriptografi

Kriptografi adalah ilmu yang digunakan untuk menjaga kerahasiaan dan keamanan informasi melalui teknik pengkodean atau enkripsi. Tujuan utamanya adalah memastikan bahwa data hanya dapat diakses oleh pihak yang berwenang, serta terlindung dari akses yang tidak sah. Kriptografi memungkinkan pesan, file, atau data digital untuk dienkripsi menggunakan algoritma tertentu, sehingga informasi tersebut tidak dapat dibaca oleh siapa pun selain penerima yang memiliki kunci dekripsi yang tepat. Di era digital ini, kriptografi menjadi penting dalam menjaga keamanan data yang ditransmisikan melalui jaringan, mencegah pencurian informasi, dan melindungi privasi pengguna[2].

2.3 RSA (*Rivest Shamir Adleman*)

RSA (*Rivest Shamir Adleman*) adalah algoritma kriptografi asimetris yang digunakan secara luas untuk mengamankan pengiriman data. Algoritma ini dikembangkan oleh Ron Rivest, Adi Shamir, dan Leonard Adleman di MIT pada tahun 1977[12].

Berikut Rumus Algoritma Kriptografi RSA untuk membangkitkan pasangan kunci RSA adalah sebagai berikut :

- Memilih dua buah bilangan prima sembarang p dan q. Nilai p dan q bersifat rahasia.
- Menghitung modulus n (*public key*) dengan rumus

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

  Hasil dari n tidak bersifat rahasia sebaiknya p # q jika p = q maka n = p^2 sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n [13].
- Menghitung Fungsi *Euler's Totient*

  $$\phi(n) = (p-1)(q-1) \quad \text{.....(2)}$$

  Fungsi Euler's Totient $\phi(n)$ menghitung jumlah bilangan bulat yang relative prima terhadap n. Dalam konteks RSA, digunakan untuk menentukan kunci publik dan privat. Mengurangi setiap bilangan prima dengan 1 dan kemudian mengalikan hasilnya memberikan jumlah bilangan yang relatif prima terhadap n [14].
- Menentukan nilai kunci umum(*publik*) adalah KP = (e, n)

  Dimana nilai e merupakan bilangan public yang digunakan untuk enkripsi. Nilai *e* dipilih dari bilangan bulat positif yang lebih kecil dari $\phi(n)$ dan prima terhadap $\phi(n)$. Pilih e relatif prima terhadap $\phi(n)$ artinya, e dan $\phi(n)$ factor pembagi terbesar keduanya adalah 1. Secara sistematis disebut *greatest common divisor* (gcd) $(e,\phi(n)) = 1$.
- Menemukan kunci pribadi (*privat*) adalah *Ks* = (*d, n)*

  Untuk membangkitkan kunci privat dengan menggunakan persamaan :

  $$e \cdot d \equiv 1 \pmod{\phi(n)} \quad \text{.....(3)}$$

  Perhatikan bahwa $e \cdot d \equiv 1 \pmod{\phi(n)}$ ekuivalen dengan e . d = 1+ k$\phi(n)$ di mana K elemen dari himpunan N sehingga d dapat dihitung dengan

  $$d = \frac{1 + k\,\phi(n)}{e} \quad \text{.....(4)}$$

  Nilai d merupakan bilangan privat yang digunakan untuk dekripsi. Artinya, *d* adalah bilangan yang, Ketika dikalikan dengan *e* hasilnya adalah 1 dalam *modulo* $\phi(n)$. Dalam algoritma RSA, *d* adalah bagian dari kunci *privat*, sedangkan *e* adalah bagian dari kunci *publik* [10].

  Hasil dari Kunci *Privat* (*Ks*) adalah bilangan bulat dengan mencoba nilai-nilai m (bilangan *integer*). Cara menghitung nilai *Ks* dengan mencoba nilai *integer m* dengan rumus :

  $$Ks = \frac{(m \times \varphi(n)) + 1}{Kp} \quad \text{.....(5)}$$

  Untuk menemukan Ks, kita mencari bilangan bulat m yang memenuhi persamaan. Dengan mencoba berbagai nilai integer m, kita dapat menemukan nilai Ks yang benar. Nilai Ks harus berupa bilangan bulat valid [10].

  Proses enkripsi dengan algoritma RSA adalah sebagai berikut :

  $$C = M^e \bmod n \quad \text{.....(6)}$$

  Keterangan:

  - *C* adalah teks terenkripsi

- *M* adalah teks asli yang akan dienkripsi
- *e* adalah kunci publik (eksponen enkripsi)
- *n* adalah modulus (produk dari dua bilangan prima yang besar).

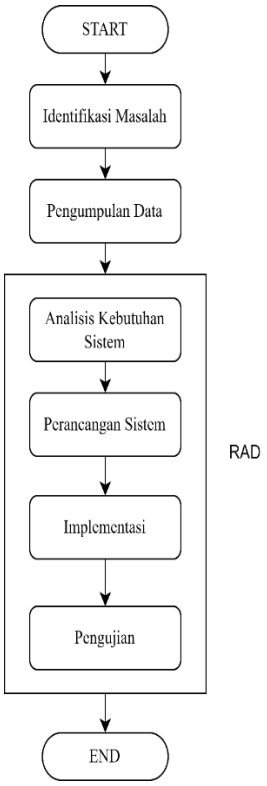
Proses enkripsi tersebut menghasilkan *encrypted* token yang akan dikirimkan bersamaan dengan *cipher text* dan *cipher text hash*, agar proses dekripsi dapat dilakukan [15].
Proses deskripsi dengan algoritma RSA adalah sebagai berikut :

$$M = C^d \ mod \ n \quad \text{.....(7)}$$

Keterangan :

- M adalah teks asli yang akan dienskripsi
- C adalah teks terenskripsi
- d adalah kunci *private* (eksponen enskripsi)
- n adalah modulus (produk dari dua bilangan prima yang besar).

3. METODOLOGI PENELITIAN



Gambar 1. *Tahapan Penelitian*

Berdasarkan gambar 1, tahapan penelitian meliputi identifikasi masalah, pengumpulan data, analisis kebutuhan sistem, perancangan, implementasi, dan pengujian dijelaskan sebagai berikut :

3.1 Identifikasi Masalah

Pada tahap ini, proses identifikasi masalah bertujuan untuk memperjelas permasalahan yang akan diteliti, dengan fokus pada penerapan algoritma RSA (*Rivest-Shamir-Adleman*) sebagai metode pengamanan data pasien di praktik dokter gigi Regunawati Cahyaningsih. Saat ini, data pada database masih menggunakan format asli (*plaintext*), sehingga rentan terhadap risiko keamanan dan potensi akses tidak sah. Selain itu, untuk mengkaji tantangan dan permasalahan yang mungkin muncul dalam penerapan metode keamanan tersebut pada data pasien.

3.2 Pengumpulan Data

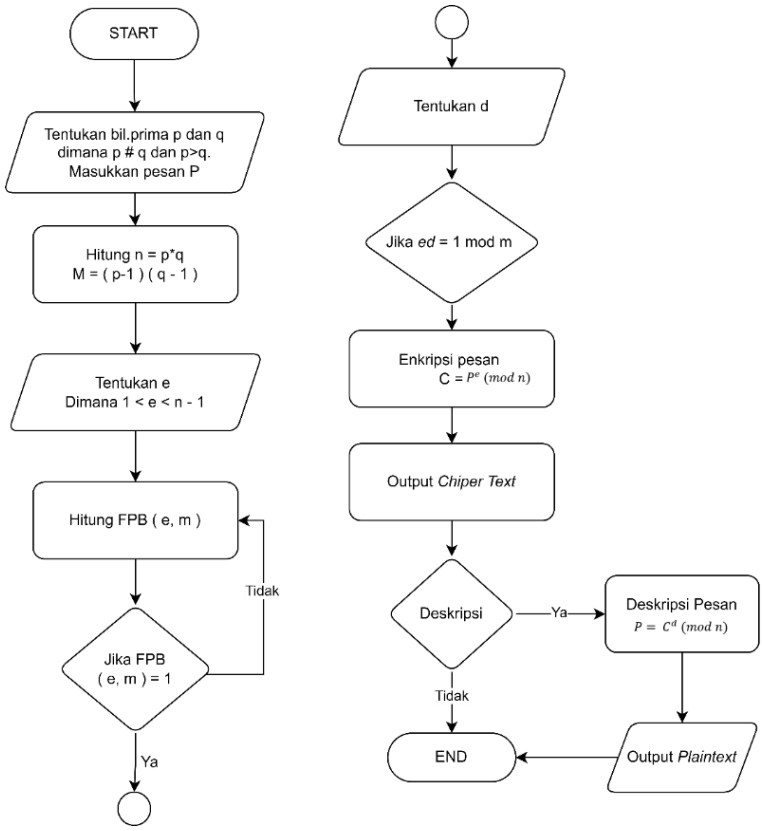
Data dikumpulkan menggunakan dua metode utama. Pertama, studi literatur dilakukan

untuk memahami konsep, cara kerja, dan penerapan algoritma RSA dalam sistem keamanan informasi dari sumber-sumber ilmiah dan terpercaya. Kedua, wawancara langsung dilakukan dengan drg. Regunawati Cahyaningsih untuk menggali kebutuhan sistem, memahami alur operasional registrasi dan pengelolaan data pasien, serta mengetahui tantangan keamanan yang dihadapi secara nyata di lapangan.

3.3 Analisis Kebutuhan Sistem

Analisis kebutuhan sistem merupakan tahap awal dalam pengembangan sistem, yang mencakup identifikasi kebutuhan pengguna seperti admin dan pasien. Admin memerlukan fitur untuk mengelola data pasien, penjadwalan, validasi pendaftaran, serta sistem keamanan berupa hak akses dan log aktivitas. Sementara itu, pasien membutuhkan fitur *login*, pendaftaran pemeriksaan, pengecekan nomor antrian, dan *logout*, dengan perlindungan data pribadi melalui sistem login yang aman dan penyimpanan data terenkripsi.

3.4 Perancangan Sistem



Gambar 2. *Flowchart Algoritma RSA*

Gambar 2 menggambarkan tahapan proses enkripsi dan dekripsi menggunakan algoritma RSA yang dimulai dengan pemilihan dua bilangan prima berbeda, yaitu p dan q, sebagai dasar pembentukan kunci. Selanjutnya dihitung nilai n sebagai hasil perkalian p dan q, serta nilai m sebagai hasil perkalian (p-1) dan (q-1). Setelah itu, dipilih nilai e yang saling prima dengan m dan berada dalam rentang 1 hingga n-1, dilanjutkan dengan validasi menggunakan perhitungan Faktor Persekutuan Terbesar (FPB) antara e dan m, yang harus menghasilkan nilai 1. Kemudian ditentukan nilai d sebagai kunci privat yang memenuhi persamaan ed ≡ 1 mod m. Setelah proses validasi selesai, pesan plaintext P dienkripsi menggunakan rumus C = P^e mod n untuk menghasilkan chipertext C, dan proses dekripsi dilakukan dengan rumus P = C^d mod n untuk mengembalikan pesan ke bentuk aslinya.

3.5 Implementasi

Setelah tahap perancangan desain sistem selesai langkah berikutnya adalah tahap implementasi, yang meliputi beberapa proses berikut:

a) Pengkodean

Pada tahap ini, pengembang mulai menulis kode program berdasarkan desain yang telah dirancang sebelumnya. Penulisan kode dilakukan dengan memperhatikan standar pengembangan perangkat lunak yang berlaku untuk memastikan kualitas dan keterbacaan program. Dalam penelitian ini, pengkodean dilakukan menggunakan perangkat lunak *Visual Studio Code*.

b) Implementasi Algoritma RSA

Proses enkripsi data menggunakan algoritma RSA dilakukan melalui beberapa langkah utama. Salah satu tahapan penting adalah pembangkitan dua jenis kunci, yaitu kunci publik (digunakan untuk mengenkripsi atau menyandikan data) dan kunci privat (digunakan untuk mendekripsi atau mengembalikan data ke bentuk aslinya). Proses pembangkitan ini menghasilkan dua kunci yang saling terkait. Setelah kedua kunci berhasil dibuat, langkah berikutnya adalah melaksanakan proses enkripsi untuk mengamankan data serta proses dekripsi untuk membaca kembali data terenkripsi sesuai kebutuhan.

3.6 Pengujian Sistem

Pengujian sistem dilakukan menggunakan *whitebox testing*. *Whitebox testing* berfokus pada pengujian logika internal kode program dengan mengidentifikasi unit yang diuji, menganalisis struktur kode, menentukan jalur uji (test cases), menjalankan unit testing, serta mengevaluasi hasil untuk memastikan tidak ada kesalahan dalam alur program. Selain itu, pengujian juga mencakup evaluasi performa melalui metrik *Largest Contentful Paint* (LCP), yang mengukur waktu render elemen terbesar di halaman sistem. Nilai LCP diklasifikasikan ke dalam tiga kategori: cepat (≤ 2.5 ms), sedang (2.6–4.0 ms), dan lambat (4.1–6.0 ms), untuk menilai kecepatan akses dan kenyamanan pengguna dalam menggunakan sistem.

4. PENGUJIAN DAN PEMBAHASAN

4.1 Implementasi Sistem

a. Struktur Data Pasien

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	id_pasien	bigint(20)		UNSIGNED	No	None		AUTO_INCREMENT	Change Drop More
2	no_rm	varchar(255)	utf8mb4_unicode_ci		Yes	NULL			Change Drop More
3	nama	text	utf8mb4_unicode_ci		No	None			Change Drop More
4	umur	int(11)			No	None			Change Drop More
5	no_telepon	text	utf8mb4_unicode_ci		Yes	NULL			Change Drop More
6	jenis_kelamin	enum('Laki-laki', 'Perempuan')	utf8mb4_unicode_ci		No	None			Change Drop More
7	alamat	text	utf8mb4_unicode_ci		No	None			Change Drop More
8	created_at	timestamp			Yes	NULL			Change Drop More
9	updated_at	timestamp			Yes	NULL			Change Drop More

Gambar 3. *Struktur Data Pasien*

Gambar 3 menampilkan struktur tabel data pasien dalam database yang mencakup kolom seperti ID pasien, nama, alamat, tanggal lahir, jenis kelamin, dan nomor telepon. Tabel ini berfungsi untuk menyimpan informasi identitas pasien secara lengkap dan terorganisir guna mendukung proses pelayanan medis serta pengelolaan data pasien di sistem informasi klinik.

b. Struktur Data Rekam Medis

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	id_rm	bigint(20)		UNSIGNED	No	None		AUTO_INCREMENT	Change Drop More
2	id_pasien	bigint(20)		UNSIGNED	No	None			Change Drop More
3	tanggal_pemeriksaan	date			No	None			Change Drop More
4	riwayat_penyakit	text	utf8mb4_unicode_ci		Yes	NULL			Change Drop More
5	dokter_pemeriksa	bigint(20)		UNSIGNED	No	None			Change Drop More
6	created_at	timestamp			Yes	NULL			Change Drop More
7	updated_at	timestamp			Yes	NULL			Change Drop More

Gambar 4. *Struktur Data Rekam Medis*

Gambar 4 menunjukkan struktur tabel rekam medis dalam database yang berisi kolom-

kolom penting seperti ID rekam medis, ID pasien, tanggal pemeriksaan, keluhan, diagnosis, tindakan, dan resep. Tabel ini dirancang untuk menyimpan riwayat medis setiap pasien secara terstruktur, sehingga memudahkan dalam pencatatan, pencarian, dan pengelolaan data pemeriksaan di sistem informasi klinik.

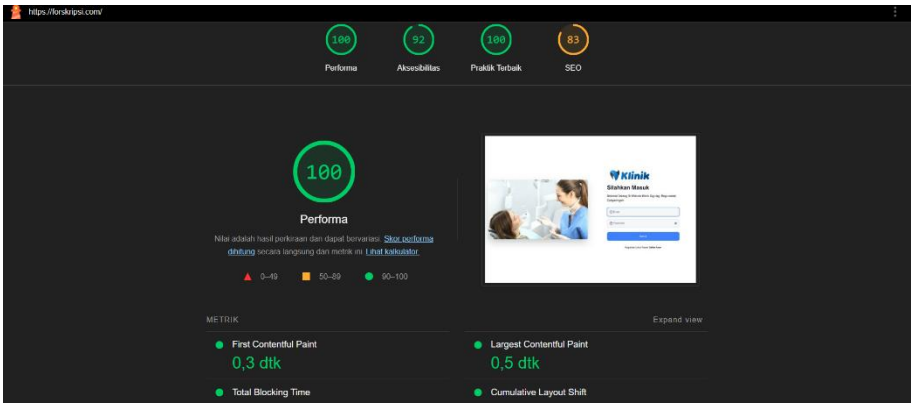
4.2 Pengujian Sistem

1) *Largest Contentful Paint (LCP) Testing*

Tabel 1. *Largest Contentful Paint (LCP) Testing*

No.	*Scenario Testing*	Rata-Rata LCP (*ms*)	Keterangan
1	Input data *Login* yang benar, lalu klik tombol 'Masuk'.	0.5	Berhasil *Login* tanpa error dan cepat
2	Melakukan enkripsi data pasien.	1.5	Data terenkripsi dengan benar tanpa error dan cepat
3	Melakukan dekripsi data pasien.	1.8	Data terdekripsi sesuai aslinya
4	Memindai *QR Code* untuk melihat data pasien.	1.0	*QR Code* berhasil terbaca
5	Memasukkan data pasien baru.	2.0	Data tersimpan dengan benar
6	Memperbarui data pasien.	2.3	Data berhasil diperbarui
7	Menghapus data pasien.	1.7	Data berhasil dihapus
8	Mencari data pasien berdasarkan nama.	1.4	Pencarian cepat dan akurat
9	Mencari data pasien berdasarkan ID.	1.6	Data ditemukan sesuai ID
10	Mengakses riwayat rekam medis pasien.	1.9	Riwayat tampil dengan benar
11	Mengakses daftar dokter.	1.3	Daftar dokter berhasil ditampilkan
12	Menambahkan diagnosis baru.	2.1	Diagnosis tersimpan dengan benar
13	Menampilkan daftar antrian pasien.	1.5	Daftar antrian tampil dengan benar
14	Menampilkan detail pasien melalui *QR Code*.	1.2	Informasi pasien sesuai

Berdasarkan Tabel 1, hasil pengujian *Largest Contentful Paint* (LCP) menunjukkan bahwa seluruh skenario memiliki waktu muat elemen terbesar yang cepat dan stabil, dengan rata-rata LCP sebesar 1.56 milidetik. Elemen penting seperti form login, data pasien, daftar dokter, hingga hasil pemindaian *QR Code* dapat dimuat dengan cepat, sebagian besar berada di bawah 2 ms. Aktivitas yang lebih kompleks seperti pembaruan data dan input diagnosis memiliki LCP sedikit lebih tinggi namun masih dalam batas optimal.



Gambar 5. *Hasil Testing LCP dengan Lighthouse*

Berdasarkan Gambar 5, evaluasi performa website https://forskripsi.com/ menunjukkan hasil yang sangat baik dengan skor 100 untuk performa, 92 aksesibilitas, 100 praktik terbaik, dan 83 SEO. Nilai *First Contentful Paint* 0,3 detik dan *Largest Contentful Paint* 0,5 detik menunjukkan kecepatan muat konten utama yang sangat cepat, serta Total *Blocking Time* dan

Cumulative Layout Shift yang rendah menandakan responsivitas dan stabilitas visual optimal. Meskipun skor SEO masih dapat ditingkatkan, secara keseluruhan *website* ini memiliki kinerja teknis yang sangat baik.

2) *Whitebox Testing*

Tabel 2. *Whitebox Testing*

Nama uji	Keterangan
Method dari *class* tb_pasien	*Create* ( )
Input data	Nama : Azizahratul No Telp : 0813456456789 Umur : 22 Alamat : Desa Manuk Siman
Method dari *Class* tb_pasien	*setAtribute* ()
Output Encrypt data	Nama : 234,151,365,151,202,13,166,202,246, 65,147 Umur : 22 Alamat : 68,374,145,202,280,116,202,384,65,81,280,73, 365,8,202,384 No Telp : 74,56,257,142,104,300,401,104,300,401,3,56, 398
Method dari *class* tb_pasien	*Save* ( )
Output descrypt data	Nama : Azizahratul No Telp : 0813456456789 Umur : 22 Alamat : Desa Manuk Siman
Expected result	Diharapkan data yang di inputkan pada database terenkripsi sesuai dengan yang diinginkan.
R*esult*	Data Terenskripsi pada database
Status	Valid

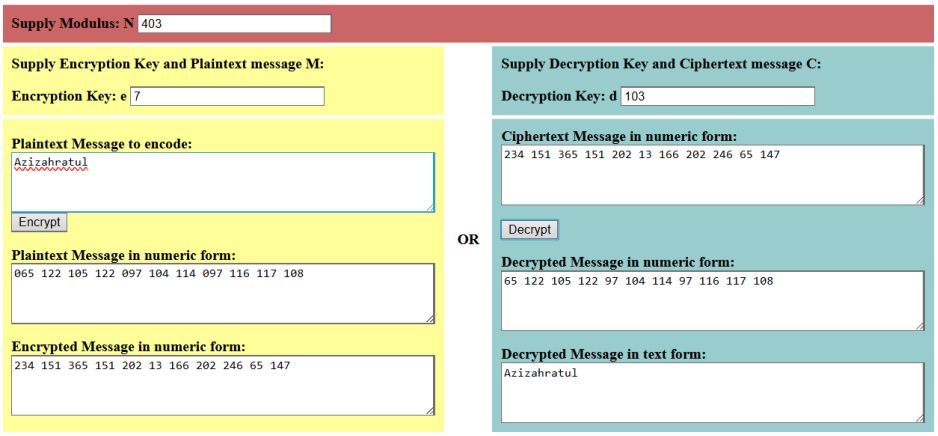
Berdasarkan hasil *whitebox testing* pada tabel 2 menunjukkan bahwa proses enkripsi dan dekripsi data pada class `tb_pasien` berjalan sesuai dengan spesifikasi. Data yang diinput seperti nama, nomor telepon, umur, dan alamat berhasil diproses melalui *method* `*setAtribute*()` dan dienkripsi dengan benar sebelum disimpan ke dalam database menggunakan *method* `*Save*()`. Setelah dilakukan dekripsi, data berhasil dikembalikan ke bentuk semula, yang membuktikan bahwa algoritma RSA diimplementasikan dengan tepat pada sistem. Dengan demikian, sistem berhasil melindungi data pasien secara menyeluruh dan status pengujian dinyatakan valid.

3) Pengujian Algoritma RSA

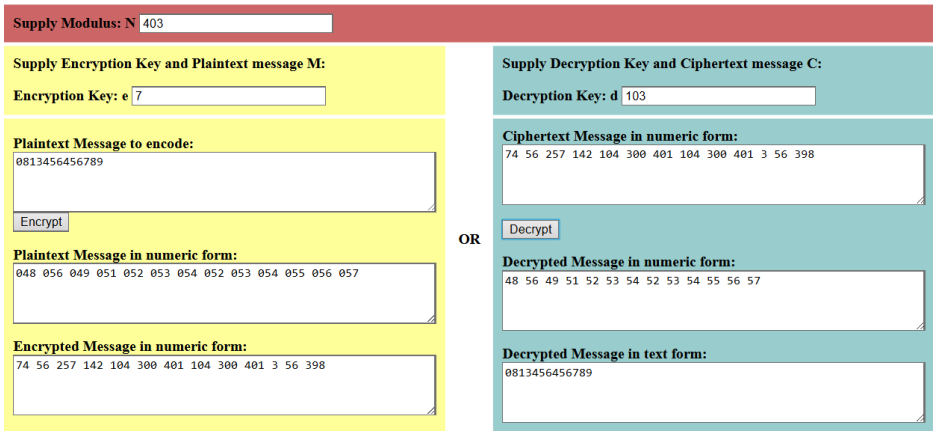
Tabel 3. *Hasil pengujian algoritma RSA*

No.	Input data	Hasil enkripsi	Hasil dekripsi	Kesimpulan	Keterangan
1.	Azizahratul	234,151,365,151 ,202,13,166,202, 246, 65,147	Azizahratul	Nama berhasil dienkripsi dan dikembalikan ke bentuk aslinya tanpa perubahan.	*Valid*
	0813456456789	74,56,257,142,1 04,300,401,104, 300,401,3,56,39 8	08134564567 89	No.telpon berhasil dienkripsi dan dikembalikan ke bentuk aslinya tanpa perubahan.	*Valid*
2.	Karang Gigi	270,202,166,202 ,384,51,280,72,3 65,51,365	Karang Gigi	Riwayat penyakit berhasil dienkripsi dan dikembalikan ke bentuk aslinya tanpa perubahan.	*Valid*

Pada Tabel 3, berbagai data sensitif—mulai dari nama “Azizahratul” hingga riwayat medis “Karang Gigi”—memulai sebuah perjalanan digital yang rahasia. Melalui algoritma RSA, informasi ini diubah wujudnya menjadi serangkaian angka yang tak bisa dimengerti, menyembunyikan makna aslinya dengan aman. Kemudian, dengan kunci yang tepat, angka-angka misterius itu dipanggil kembali. Ajaibnya, semua data kembali utuh ke bentuk semula, seolah tak pernah berubah. Tabel ini adalah saksi bisu perjalanan mereka, sebuah catatan yang membuktikan dengan status “Valid” bahwa sang algoritma adalah penjaga rahasia yang bekerja dengan sempurna. Berikut hasil pengujian algoritma RSA :



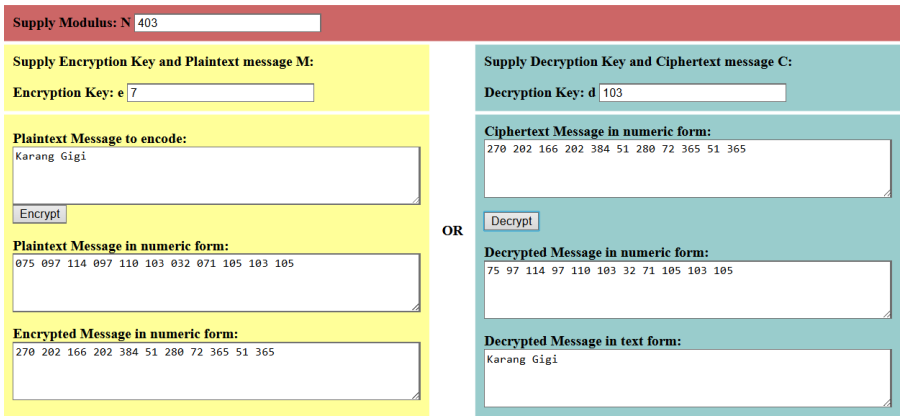
Gambar 6. *Hasil enkripsi dan deskripsi kolom Nama*



Gambar 7. *Hasil enkripsi dan deskripsi kolom No.telpon*

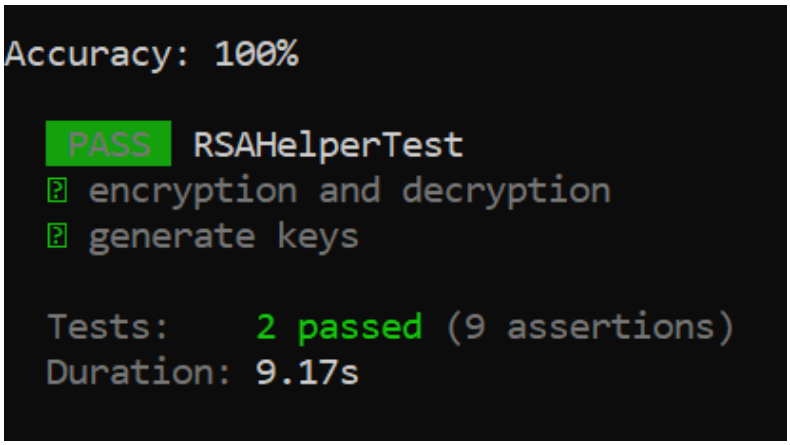
Gambar 6 menunjukkan hasil enkripsi dan dekripsi pada kolom Nama menggunakan algoritma RSA. Data “Azizahratul” dikonversi menjadi ciphertext dalam bentuk angka terenkripsi, yaitu “234 151 365 151 202 13 166 202 246 65 147”. Proses dekripsi dengan kunci yang sesuai berhasil mengembalikan ciphertext tersebut ke bentuk asli tanpa perubahan, membuktikan bahwa algoritma RSA berfungsi dengan baik dalam mengamankan data pasien.

Gambar 7 menunjukkan proses enkripsi dan dekripsi pada kolom No. Telepon menggunakan algoritma RSA. Data “0813456456789” dikonversi menjadi ciphertext dalam bentuk angka terenkripsi, yaitu “74 56 257 142 104 300 401 104 300 401 3 56 398”. Setelah dilakukan dekripsi menggunakan kunci yang sesuai, data berhasil dikembalikan ke bentuk aslinya tanpa perubahan. Hal ini membuktikan bahwa algoritma RSA dapat mengamankan dan mengembalikan data No. Telepon dengan benar.



Gambar 8. *Hasil enkripsi dan deskripsi kolom Riwayat Penyakit*

Gambar 8 menunjukkan proses enkripsi dan dekripsi pada kolom Riwayat Penyakit menggunakan algoritma RSA. Data "Karang Gigi" berhasil diubah menjadi *ciphertext* dalam bentuk angka terenkripsi, yaitu "270 202 166 202 384 51 280 72 365 51 365". Setelah dilakukan proses dekripsi menggunakan kunci yang sesuai, data kembali ke bentuk aslinya tanpa perubahan.



Gambar 9. *Hasil Akurasi Enkripsi dengan Algoritma RSA*

Gambar 9 menunjukan bahwa, sebuah proses krusial baru saja berakhir. Sebuah kode bernama RSAHelper, yang dirancang untuk tugas keamanan siber, telah menjalani serangkaian ujian berat. Selama 9.17 detik yang menegangkan, sistem secara otomatis menguji kemampuannya untuk membuat kunci (generate keys) dan melakukan enkripsi-dekripsi data. Akhirnya, layar menampilkan hasil yang ditunggu: sebuah kata "PASS" berwarna hijau terang. Dengan akurasi sempurna 100% dan 2 tes yang berhasil dilewati, ini adalah konfirmasi. Kode tersebut bekerja tanpa cela, membuktikan dirinya andal dan siap untuk menjalankan tugasnya dalam melindungi informasi digital.

5. KESIMPULAN

Dalam upaya meningkatkan keamanan data pasien, praktik drg. Regunawati Cahyaningsih telah sukses mengimplementasikan Algoritma Rivest-Shamir-Adleman (RSA). Sistem ini efektif mengenkripsi data sensitif menjadi _ciphertext_ yang hanya dapat diakses oleh pihak berwenang melalui kunci privat dan QR Code terenkripsi, memastikan integritas dan kerahasiaan data pasien terjaga. Pengujian fungsionalitas, akurasi algoritma (100% berhasil pada _unit test_ RSAHelperTest), dan kecepatan sistem (LCP 0,5-2,3 ms dengan skor performa 100) menunjukkan kinerja yang sangat baik, membuktikan RSA mampu mengenkripsi dan mengembalikan data secara akurat serta memberikan pengalaman pengguna yang optimal dalam lingkungan klinik.

DAFTAR PUSTAKA

[1] B. Anwar, N. B. Nugroho, J. Prayudha, and A. Azanuddin, "Implementasi Algoritma RSA Terhadap Keamanan Data Simpan Pinjam," Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer), vol. 18, no. 1, p. 30, Feb. 2019, doi: 10.53513/jis.v18i1.100. https://doi.org/10.53513/jis.v18i1.100

[2] S. Sutejo, "Implementasi Algoritma Kriptografi Rsa (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien," INTECOMS: Journal of Information Technology and Computer Science, vol. 4, no. 1, pp. 104–114, Jun. 2021, doi: 10.31539/intecoms.v4i1.2437. https://doi.org/10.31539/intecoms.v4i1.2437

[3] R. Zhang and Z. Wang, "Family cohesion moderates the inverted U-shaped curve between resting RSA and children's empathy," Psychoneuroendocrinology, vol. 172, p. 107231, Feb. 2025, doi: 10.1016/j.psyneuen.2024.107231. https://doi.org/10.1016/j.psyneuen.2024.107231

[4] Tarisa Auliya Ramadhani, A. Fajaryanto Cobantoro, and S. Sugianti, "Implementasi Algoritma Advanced Encryption Standard 128 untuk Pengamanan Database Sistem Registrasi Pasien," Jurnal Informatika Polinema, vol. 10, no. 4, pp. 521–526, Aug. 2024, doi: 10.33795/jip.v10i4.5619. https://doi.org/10.33795/jip.v10i4.5619

[5] Ni Kadek Sriyulianti, S. ngurah Ardhya, and M. jodi Setianto, "Kautsar, T. R. (2023). Kajian Literatur Terstruktur Terhadap Kebocoran Data Pribadi Dan Regulasi Perlindungan Data Pribadi. APJII. (2023). Survei APJII Pengguna Internet di Indonesia Tembus 215 Juta Orang. APJII. https://apjii.or.id/berita/d/survei-apjii-," Jurnal Ilmu Hukum Sui Generis, vol. 4, no. 3, Apr. 2025, doi: 10.23887/jih.v4i3.5035. https://doi.org/10.23887/jih.v4i3.5035

[6] I. Firdaus, "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan," Jurnal Rechten : Riset Hukum dan Hak Asasi Manusia, vol. 4, no. 2, pp. 23–31, Dec. 2022, doi: 10.52005/rechten.v4i2.98. https://doi.org/10.52005/rechten.v4i2.98

[7] A. R. Pradina, R. G. Tayibnafis, and V. Sevilla, "Signifikansi Informasi Isu Kebocoran Data Privasi Tokopedia Terhadap Perilaku Fandom," Jurnal Pustaka Komunikasi, vol. 5, no. 2, pp. 331–343, Sep. 2022, doi: 10.32509/pustakom.v5i2.2186. https://doi.org/10.32509/pustakom.v5i2.2186

[8] Vanesha Marcelliana et al., "Penerapan Perlindungan Konsumen Terhadap Nasabah PT. Bank Syariah Indonesia Dalam Kasus Kebocoran Data Nasabah," Deposisi: Jurnal Publikasi Ilmu Hukum, vol. 1, no. 2, pp. 180–194, Jun. 2023, doi: 10.59581/deposisi.v1i2.577. https://doi.org/10.59581/deposisi.v1i2.577

[9] A. H. Satria Nusantara, I. Kahirul Umam, and M. Lubis, "Jaminan Informasi dan Keamanan yang Lebih Baik: Studi Kasus BPJS Kesehatan," NUANSA INFORMATIKA, vol. 18, no. 2, pp. 120–127, Jul. 2024, doi: 10.25134/ilkom.v18i2.202. https://doi.org/10.25134/ilkom.v18i2.202

[10] D. Singh and S. Kumar, "Image authentication and encryption algorithm based on RSA cryptosystem and chaotic maps," Expert Syst Appl, vol. 274, p. 126883, May 2025, doi: 10.1016/j.eswa.2025.126883. https://doi.org/10.1016/j.eswa.2025.126883

[11] M. Rahmani, A. Nitaj, and M. Ziane, "A novel cryptanalytic attack on a family of RSA-like cryptosystems," Discrete Math, vol. 349, no. 1, p. 114660, Jan. 2026, doi: 10.1016/j.disc.2025.114660. https://doi.org/10.1016/j.disc.2025.114660

[12] H. Huang and Z. Han, "Computational ghost imaging encryption using RSA algorithm and discrete wavelet transform," Results Phys, vol. 56, p. 107282, Jan. 2024, doi: 10.1016/j.rinp.2023.107282. https://doi.org/10.1016/j.rinp.2023.107282

[13] A. F. Cobantoro, M. B. Setyawan, and H. Oktavianto, "Rekayasa Aplikasi Eposal Menggunakan Algoritma Base64 Untuk Menyimpan Data Pengguna," Jurnal Komtika (Komputasi dan Informatika), vol. 7, no. 1, pp. 31–38, May 2023, doi: 10.31603/komtika.v7i1.8711. https://doi.org/10.31603/komtika.v7i1.8711

[14] Y. Litanianda, D. April Riyanto, A. Prasetyo, A. Fajaryanto Cobantoro, and I. Abdurrozaq Zulkarnain, "Identifikasi Performa Algoritma Fuzzy Mamdani Sebagai Kendali Proses

Koagulasi pada Internet of Thing Pembuatan Tahu," bit-Tech, vol. 7, no. 2, pp. 608–617, Dec. 2024, doi: 10.32877/bt.v7i2.1972. https://doi.org/10.32877/bt.v7i2.1972

[15] H. Pramudya, A. Fajaryanto Cobantoro, and J. Karaman, "Implementasi Algoritma Selection Sort Dalam Sistem Absensi Siswa Untuk Pengurutan Keaktifan Berdasarkan Kehadiran," JATI (Jurnal Mahasiswa Teknik Informatika), vol. 9, no. 2, pp. 2887–2895, Mar. 2025, doi: 10.36040/jati.v9i2.13212. https://doi.org/10.36040/jati.v9i2.13212

[16] D. T. Tobing, "Implementasi Algoritma Rivest Shamir Adleman (RSA) Untuk Keamanan Data Rekam Medik Penyakit Pasien Rumah Sakit," Jurnal Kajian Ilmiah Teknologi Informasi dan Komputer, vol. 2, no. 2, pp. 65–73, May 2024, doi: 10.62866/jutik.v2i2.131. https://doi.org/10.62866/jutik.v2i2.131

[17] S. Kinney, "The RSA Encryption and Decryption Command Suite," in Trusted Platform Module Basics, Elsevier, 2006, pp. 207–221. doi: 10.1016/B978-075067960-2/50017-8. https://doi.org/10.1016/B978-075067960-2/50017-8