Journal of Information Technology and Computer Science (INTECOMS)
Volume 4 Nomor 1, Juni 2021
e-ISSN : 2614-1574
p-ISSN : 2621-3249

IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA (RIVEST SHAMIR ADLEMAN) UNTUK KEAMANAN DATA REKAM MEDIS PASIEN

IMPLEMENTATION OF RSA CRYPTOGRAPHY ALGORITHM (RIVEST SHAMIR ADLEMAN) FOR PATIENT MEDICAL RECORD DATA SECURITY

Sutejo
Universitas Lancang Kuning
sutejo@unilak.ac.id

ABSTRACT

Patient data security is very important for doctors and patients. Abuse from irresponsible parties to change or steal patient data can be avoided by the need for a mechanism to secure the data in the medical record system using encryption techniques in the database. In this study, the RSA cryptographic algorithm method is used to secure the patient's medical record data which contains notes and documents about the patient's identity, disease diagnosis, treatment, action and other services. RSA is an asymmetric cryptographic algorithm that uses a pair of keys, namely the public key and the private key. The security of the RSA algorithm lies in the difficulty of factoring prime numbers. In system testing using the blackbox method that focuses on the functional specifications of the software. The result of this research is a web-based medical record system that can help Citra Bunda Clinic to improve the safety of patient medical record data..

Keywords: Medical Records, RSA Algorithm, Data Security..

ABSTRAK

Keamanan data pasien sangatlah penting bagi dokter dan pasien. Penyalahgunaan dari pihak yang tidak bertanggung jawab untuk mengubah atau mencuri data pasien dapat dihindari dengan diperlukan mekanisme untuk mengamankan data yang ada pada sitem rekam medis menggunakan teknik enkripsi pada database. Dalam penelitian ini digunakan metode algoritma kriptografi RSA untuk mengamankan data rekam medis pasien yang berisikan catatan dan dokumen tentang identitas pasien, diagnosa penyakit, pengobatan, tindakan dan pelayanan lain. RSA merupakan algoritma kriptografi asimetris yang menggunakan sepasang kunci, yaitu kunci publik dan kunci pribadi. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan prima. Pada pengujian sistem menggunakan metode blackbox yang berfokus pada spesifikasi fungsional dari perangkat lunak. Hasil dari penelitian ini yaitu sistem rekam medis berbasis web yang dapat membantu Klinik Citra Bunda untuk meningkatkan keamanan data rekam medis pasien.

Kata Kunci: Rekam Medis, Algoritma RSA, Keamanan Data.

PENDAHULUAN

Dalam era kemajuan teknologi saat ini berbagai upaya dilakukan oleh manusia untuk mempercepat segala tindakan pekerjaan dengan memanfaatkan komputerisasi sehingga segala jenis pekerjaan dapat di selesaikan dengan mudah, cepat, akurat dan tepat guna (Setyawati, et. al., 2021). Dengan seiring perkembangan kemajuan teknologi masalah keamanan merupan salah satu aspek penting dari sebuah sistem informasi namun masalah keamanan seringkali kurang mendapat perhatian dari para pemilik dan prengelolah sistem informasi, salah satu contohnya adalah sistem informasi rekam medis yang ada di Klinik Citra Bunda, Jln. Sukaramai, Petapahan, kec. Tapung Hulu. Perkembangan teknologi informasi pada saat ini membuat setiap pemilik dan pengelolah sistem informasi harus dan wajib memikirkan bagaimana cara untuk melindungi keamanan sistem informasi yang dimilikinya agar terhindar dari berbagai resiko sehingga

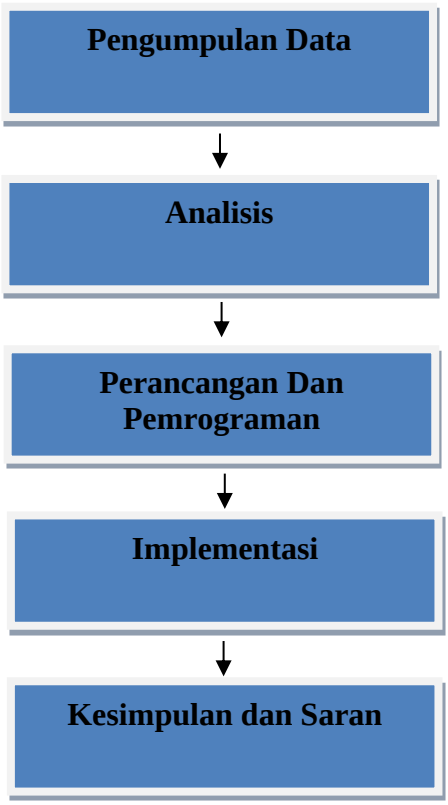
data tersebut tidak disalah gunakan oleh pihak-pihak tertentu yang tidak bertanggung jawab(Pabokory, et. al., 2016).

Rekam medis merupakan catatan riwayat pasien pengobatan serta dokumen yang berisi data pribadi, dianogsa riwayat penyakit yang di derita pasien, serta riwayat pengobatan pasien yang di keluarkan oleh pihak klinik. Informasi yang terdapat di dalam sebuah rekam medis pasien bersifat rahasia dan tidak dapat di baca oleh pihak yang tidak berkepentingan(Tohirin, 2020). Dari kasus permasalahan yang ada pada Klinik Citra Bunda belum adanya pengamanan data pada karena akan mengakibatkan tidak amannya dari pencurian data dalam sebuah sistem yang ada di database dan untuk menghindari perubahahan data di database di sistem informasi rekam medis Klinik Citra Bunda tersebut oleh pihak lain, banyak terdapat celah yang dapat di gunakan untuk memanipulasi hak akses pada database, misalnya teknik SQL injection contohnya serangan dengan melalui URL. Sebuah bahasa pemograman seperti PHP mengakses database melalui SQL query. Jika data yang langsung ke database dan tidak langsung di saring dengan benar, maka penyerang dapat menyisipkan perintah SQL nya sebagian dari input, database sebagai sumber data dan informasi tersebut perlu dilakukan proses pengamanan agar data dalam database tersebut lebih terjamin keamanannya(Anggraini & Juanita, 2018).

Terdapat banyak sekali teknik pengamanan data yang banyak digunakan, salah satu nya dengan menggunakan metode RSA (Rivest Shamir Adleman) dimana metode adalah satu metode kriptografi asimetri terbaik (Rakhman & Kurniawan, 2015, Yusrizal, 2019, Siringoringo, 2020, Haryanto, 2021). RSA menggunakan dua kunci public dan satu kunci private, proses enkripsi pada RSA menggunkan kunci private dan satu kunci publik, sedangkan untuk deskripsinya RSA menggunakan dua kunci publik(Ginting, et. al., 2015).

METODE

Berikut merupakan langkah-langkah dari penelitian :



Gambar 1. Tahapan Penelitian

Perencanaan

Merupakan tahapan yang di lakukan dalam penelitian. Yang mana tahapan inibertujuan untuk memberikan ketentuan bentuk masalah dan tujuan. Dalam proses perencanaan ada beberapa hal yang akan dilakukan yaitu menentukan masalah, tujuan penelitian, dan ruang lingkup.

a. Menentukan Masalah

   Hal pertama yang dilakukan penulis dalam penelitian ini adalah menentukan permasalahan yang ada

dan mengambil permasalahan tersebut menjadi topik penelitian.

b. Menentukan Tujuan
Setelah masalah ditentukan, maka penulis menentukan tujuan dari penelitian ini, yaitu untuk menyelesaikan masalah yang ada.

c. Menentukan Ruang Lingkup
Penulis menentukan ruang lingkup dengan alasan agar penelitian dapat teraarah dan tidak mengambang dari masalah yang telah ditentukan.

Pengumpulan Data

Tahapan selanjutnya merupakan termin pengumpulan data. Data diharapkan buat mempermudah peneliti melakukan penelitian. Kegiatan yg dilakukan pada termin pengumpulan data ini merupakan menjadi berikut :

a. Observasi Yaitu teknik yg dilakukan secara valid melalui pengamatan & penulisan terhadap hal diharapkan, bermaksud buat menerima data berdasarkan pengamatan pribadi.

b.Wawancara Bertujuan buat menerima keterangan secara pribadi melalui bertatap muka menggunakan Kepala Pengelolah Klinik Citra Bunda.

c.Studi Pustaka Sebagai acuan pada pada penelitian, baik berdasarkan *text book* juga berdasarkan keterangan-keterangan yg masih ada pada jurnal.

Analisis

Langkah analisis yang dilakukan adalah sebagai berikut :

a. Analisis Permasalahan
Analisis permasalahan adalah tahap yang dilakukan untuk mengetahui permasalahan apa yang sedang terjadi dan menentukan solusi yang dibutuhkan.

b. Usulan Sistem Baru
Dalam tahapan ini dibuat penjabaran gambaran umum sistem baru yang akan dibangun untuk mengatasi permasalahan pada Sistem Rekam Medis Data Pasien di Klinik Citra Bunda.

Perancangan dan Pemrograman

Dalam tahapan perancangan dan pemrograman terdapat kegiatan yang dilakukan, sebagai berikut:

a. Perancangan Sistem
Merupakan langkah yang dilakukan untuk membuat bentuk rancangan dari proses sistem. Peracangan ini menggunakan alat diagram UML yang dilakukan dalam bentuk pembuatan diagram.

b. Perancangan Interface
Pada tahap ini, setelah melakukan perancangan sistem dan perancangan interface dibuatlah program seperti yang telah dirancang.

Implementasi

Implementasi sistem adalah pengembangan dari tahap desain sistem. Tahap ini merupakan tahap yang paling penting karena harus mengimplementasikan sistem yang telah di rancang.

Kesimpulan dan Saran

Kesimpulan adalah hasil akhir penelitian yang dirumuskan berdasarkan data yang telah terkumpul, dan sejalan dengan rumusan masalah maupun langkah–langkah pemecahan masalah yang telah ditetapkan. Sedangkan saran merupakan usulan yang diajukan peneliti untuk dipertimbangkan agar permasalahan lain yang ada dapat dipecahkan sebaik-baiknya di waktu mendatang.

HASIL DAN PEMBAHASAN

Analisa Sistem

Tahap analisa sistem bertujuan sebagai dasar perancangan atau perbaikan sistem yang lama. Dari hasil analisis tersebut dapat dirancang atau diperbaiki menjadi sebuah sistem yang lebih efektif dan efisien. Untuk meningkatkan kecepatan dan keakuratan baik dalam penginputan data, pemrosesan data, keamanan data, serta hasil *output* nya maka klinik Citra Bunda memerlukan aplikasi yang lebih baik mengingat kemajuan teknologi yang semakin pesat untuk melindungi data yang dimilikinya agar terhindar dari berbagai resiko yang nantinya dapat membantu dalam melakukan pengamanan data rekam medis pasien.

Analisa sistem pada aplikasi ini merupakan penguraian dari suatu implementasi Algoritma Kriptografi RSA (*Rivest Shamir Adleman*) dimana algoritma ini adalah satu metode kriptografi asimetri terbaik. Prinsip kerja algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar bahkan sangat besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk mendapatkan kunci privat. Selama bilangan tersebut tidak dapat difaktorkan, selama itu pula keamanan algoritma RSA akan sangat tinggi.

Analisa Kebutuhan Sistem

Implementasi algoritma Kriptografi RSA data rekam medis pasien klinik Citra Bunda adalah digunakan untuk keamanan data pada database data rekam medis pasien. Analisa sistem pada aplikasi ini akan dibagi beberapa bagian, yakni sistem utama aplikasi akan dibahas mengenai proses utama dari aplikasi ini yaitu proses rekam medis pasien *input output* dan sistem algoritma akan membahas bagaimana algoritma kriptografi RSA bekerja sehingga data rekam medis pasien menjadi lebih aman.

Analisa Algoritma Kriptografi RSA

Dalam sistem algoritma kriptografi RSA terdapat proses utama, yaitu proses pembuatan kunci Privat dan kunci Publik dimana masing masing digunakan dalam proses enkripsi dan dekripsi, proses dekripsi adalah mengubah plainteks menjadi chipherteks dan dekripsi mengubah chipherteks menjadi plainteks(Andriani, 2017). Dalam algoritma RSA terdapat besaran-besaran yang penting yaitu sebagai berikut:

1. Nilai p dan q merupakan bilangan prima diambil secara acak atau lebih baiknya langsung dipilih oleh orang yang akan menerima data. Sifat dari kedua bilangan ini adalah rahasia, dimana hanya pengirim data dan penerima data yang dapat mengetahuinya.
2. Nilai N merupakan bersifat publik, karena Sifat N adalah tidak rahasia N=p.q.
3. φ(N)=(p-1)(q-1), sifat dari bilangan ini adalah rahasia.
4. e (kunci enkripsi), sifat bilangan kunci enkripsi tidak rahasia.
5. d (kunci dekripsi), kunci dekripsi bersifat rahasia.
6. m (plainteks), merupakan informasi awal yang bersifat rahasia.
7. C (Chipherteks), chipherteks merupakan infomasi yang telah di enkripsi yang bersifat tidak rahasia.

Pembangkitan Kunci Publik dan Kunci Privat

RSA (*Rivest Shamir Adleman*) merupakan algoritma yang menggunakan kunci yang berbeda pada proses enkripsi dan dekripsi. Algoritma kriptografi RSA menggunakan kunci asimetris. Pada proses enkripsi menggunakan kunci publik sedangkan dekripsi menggunakan kunci privat. *Generate* kunci atau pembangkitan kunci dilakukan pada awal sebelum melakukan proses enkripsi dimana

membutuhkan 2 bilangan (*integer*) prima secara acak, dalam hal ini diharuskan menggunakan sebuah pembangkit yang secara otomatis generasi bilangan tersebut dikarenakan angka-angka tersebut cukup besar dan banyak untuk memperoleh keamanan yang lebih tinggi dan lebih baik. Selanjutnya terdapat juga proses pengecekan apakah bilangan tersebut bilangan prima atau tidak sehingga akan terjadi *lopping* yang cukup lama sampai menemukan nilai prima yang sesuai dengan syarat.

Dalam proses keseluruhan pembangkitan kunci privat dan kunci publik diperoleh parameter-parameter yang dibutuhkan dalam proses selanjutnya yaitu proses enkripsi data (plainteks). kunci publik (e) digunakan untuk melakukan enkripsi, kunci private (d) digunakan untuk proses dekripsi, serta nilai modulo (N) akan selalu digunakan dalam proses enkripsi dan dekripsi. Berikut langkah-langkah proses pembangkitan kunci :

1. Proses pertama proses pembangkitan atau *generate* dua buah bilangan prima secara acak. Besaran itu adalah nilai *p* dan *q*.
2. Hitung nilai $N=p.q$ dan $\varphi(N) = (p-1)(q-1)$
3. Pilih satu kunci publik (e) dimana $1 < e < \varphi(N)$, yang disimbolkan dengan syarat dari pemilihan kunci ini adalah e harus relatif prima terhadap $\varphi(N)$.
4. Membangkitkan kunci privat (d) dengan persamaan e.d mod $\varphi(N)=1$.

Hasil dari proses diatas adalah kunci publik pasangan (e, N) sedangkan kunci privat pasangan (d, N).

Semisal nilai $p = 11$ dan $q = 13$ maka tentukan nilai $\varphi(N)$, *N dan e :*

$$N = P * Q = 11 * 13 = 143$$

$$\varphi(N) = (p-1)(q-1) = (11-1)(13-1) = 120$$

$$e.gcd(\varphi(N)) = e.gcd(120) = 7$$

b. Enkripsi

Sebelum melakukan enkripsi, *user* terlebih dahalu diminta mengisi semua inputan ke dalam *form* yang telah disediakan, lalu ketika *user* klik *submit*, maka dilakukan proses enkripsi pada inputan (plainteks) yang telah dibagi blok-blok yang kemudian akan dilakukan enkripsi.

Sebagai contoh, Perhitungan manual proses enkripsi untuk inputan pasien dengan nama "Fajar" oleh aplikasi diubah dalam bentuk ASCII sesuai dengan tabel ASCII yaitu 70 97 106 97 114.

Tabel 1. Ubah Teks Asli "Fajar" menjadi ASCII desimal

Karakter	F	a	j	a	r
ASCII (desc)	70	97	106	97	114

Setelah dilakukan perubahan kedalam bentuk ASCII maka *m* dalam desimal = 709710697114. Lakukan transformasi satu ke satu untuk *m* (terletak pada rentan $0 – (n – 1)$) hal ini dilakukan agar nilai enkripsi tidak terlampau besar Rentan setiap blok $m = 0 – (n – 1) = 0 – 142$. Maka blok yang terbentuk adalah :

$m_1 = 70$; $m_2 = 97$; $m_3 = 106$; $m_4 = 97$; $m_5 = 114$

Sebelumnya telah diketahui kunci publik adalah $e = 7$ dan $N = 143$ maka pesan M dapat dienkripsikan, yakni:

$c_1 = 70^7 \bmod 143 = 60$; $c_2 = 97^7 \bmod 143 = 59$

$c_3 = 106^7 \bmod 143 = 50$; $c_4 = 97^7 \bmod 143 = 59$

$c_5 = 114^7 \bmod 143 = 49$

Setelah proses enkripsi selesai, maka chiperteks yang dihasilkan adalah 60 59 50 59 49. Selanjutnya inputan yang telah di enkripsi tersebut disimpan kedalam *database*.

Langkah-langkah enkripsi adalah sebagai berikut :

1. Langkah pertama adalah mengambil nilai kunci publik (e) dan modulo (N) dari proses pembangkitan kunci.
2. Teks yang akan dienkripsi (plainteks).
3. Teks yang akan dienkripsi kemudian diubah kedalam bentuk ASCII sesuai dengan tabel ASCII.
4. Membagi teks tersebut menjadi beberapa blok (mi) dengan syarat mi < dengan length(mi) = (mi+1).
5. Setelah itu setiap blok dari teks akan dienkripsikan menggunakan pasangan kunci publik (e, N).

Dekripsi

Sebelum melakukan dekripsi, *user* meminta kepada sistem untuk menampilkan data yang dipilih sehingga memanggil perintah tampilkan data maka sistem melakukan dekripsi dahulu terhadap data (chipherteks) yang ada di *database* sehingga berubah ke bentuk data awal (plainteks) saat di inputkan lalu sistem akan menampilkan data kepada sistem.

Proses dekripsi dilakukan pada blok-blok bilangan yang diperoleh dari proses enkripsi sehingga menghasilkan bilangan baru yang apabila diubah kembali kedalam pengkodean ASCII akan menghasilkan karakter yang sama dengan plainteks sebelum dilakukan proses enkripsi. Proses dekripsi menggunakan pasangan kunci privat (d, N). Dalam proses dekripsi, jika kunci privat yang digunakan salah dan berbeda dari yang telah dibangkitkan maka proses dekripsi tidak akan berhasil.

Sebagai contoh, Perhitungan manual proses dekripsi dari 60 59 50 59 49 yang mana telah memiliki kunci privat (*d*,*N*) = (103, 143).

$m_1 = 60^{103} \bmod 143 = 70$; $m_2 = 59^{103} \bmod 143 = 97$

$m_3 = 50^{103} \bmod 143 = 106$; $m_4 = 59^{103} \bmod 143 = 97$

$m_5 = 49^{103} \bmod 143 = 114$

Maka Akan dihasilkan kembali m = 70 97 106 97 114 yang dalam pengkodean ASCII dapat dibaca sebagai “Fajar”.

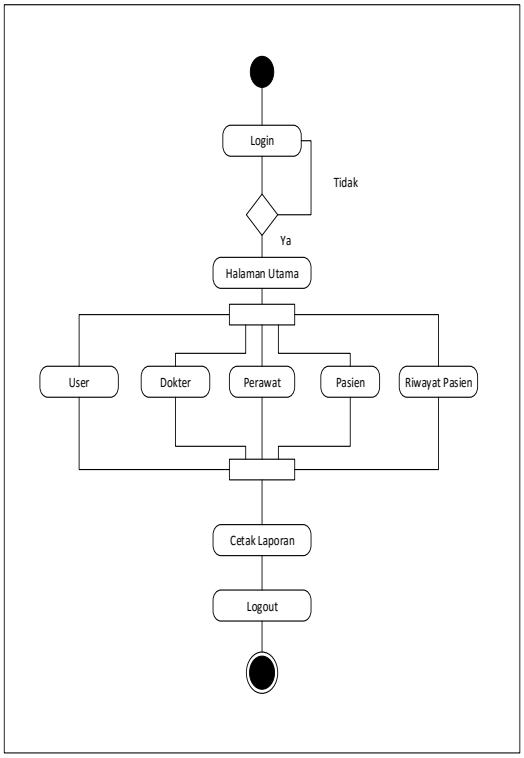
Langkah-langkah dekripsi adalah sebagai berikut :

1. Langkah pertama adalah mengambil nilai kunci privat (d) dan modulo (N).
2. Teks yang akan didekripsi (chipherteks)
3. Membagi teks tersebut menjadi beberapa blok (mi) dengan syarat mi < dengan length(mi) = (mi+1).
4. Kembalikan ke dalam bentuk ASCII , (karakter ASCII = mi ^ e (mod N))
5. Nilai ASCII diubah menjadi karakter sesuai dengan tabel ASCII
6. Karakter digabungkan menjadi satu blok.

Gambaran Sistem Yang Diusulkan

Perancangan sistem merupakan suatu kegiatan pengembangan serta perbaikan terhadap sebuah sistem yang berjalan. Pada tahap ini dilakukan upaya untuk memperbaiki sistem ataupun membangun dan menghasilkan sistem yang baru dengan memanfaatkan teknologi terbaru dan fasilitas yang tersedia.

UML (*Unified Modelling Language)* adalah metode pemodelan secara visual sebagai sarana untuk merancang dan membuat *software* berorientasi objek. Karena UML ini merupakan bahasa visual untuk pemodelan bahasa berorientasi objek, maka semua elemen dan diagram berbasiskan pada paradigma *object oriented*.a. Business Process

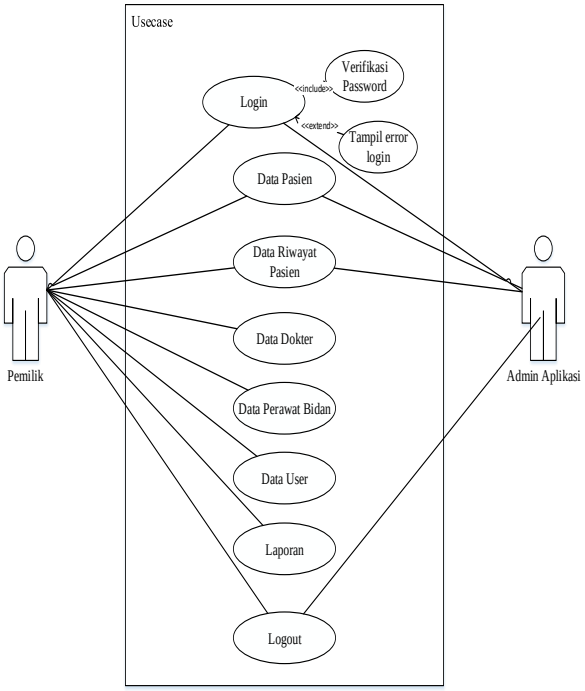


Gambar 2. Business Process

Pada Gambar 2. menjelaskan rancangan *Business Process Model*, Adapun kegunaan atau fungsi diagram ini adalah menjelaskan secara ringkas rancangan tentang aplikasi ini. Cara penggunaan aplikasi ini adalah user melakukan *login* dan jika *login* berhasil user akan masuk ke menu halaman utama lalu user dapat mengelola aplikasi.

Use Case Diagram

Use Case Diagram dibawah ini menggambarkan fungsionalitas yang diharapkan dari sebuah sistem, sebuah *use case* merepresentasikan sebuah interaksi antara aktor dengan sistem. Berikut adalah pemodelan *Use case* untuk pengamanan data rekam medis pasien sistem rekam medis klinik citra bunda.

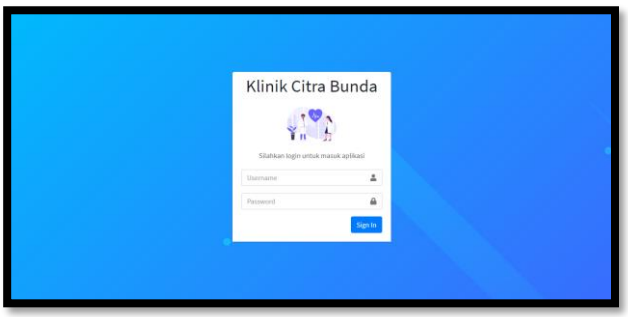


Gambar 3. Use Case Diagram

Gambar 3. *Use Case Diagram* menggambarkan apa saja peran dari aktor *pemilik*, dimana *pemilik* mendapat akses ke semua fitur sistem sedangkan *admin aplikasi* hanya sebagai pengelola sistem.

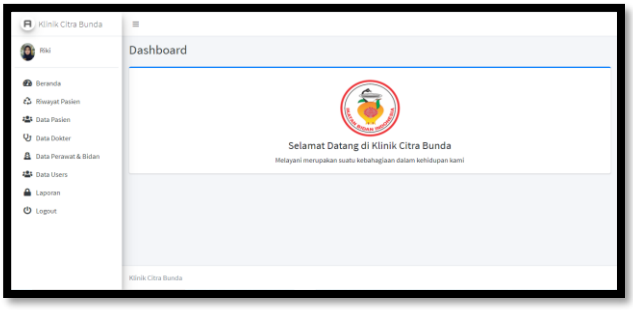
Implementasi

Tampilan Halaman Login



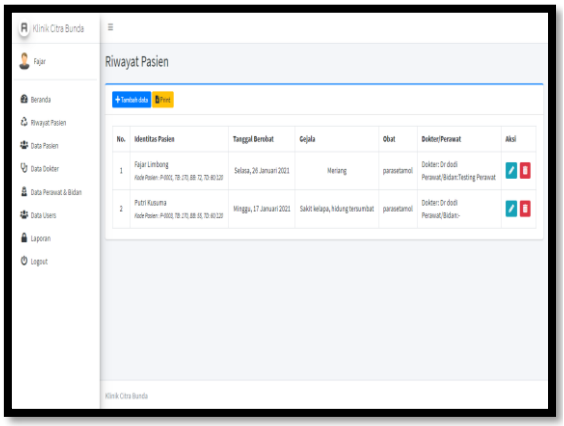
Gambar 4. Tampilan Halaman Login

Tampilan Halaman Utama



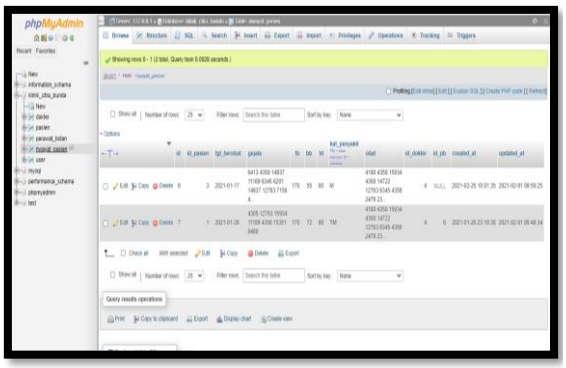
Gambar 5. Tampilan Halaman Utama

Tampilan Halaman Riwayat Pasien



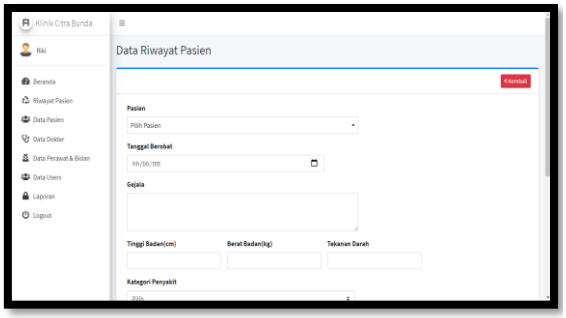
Gambar 6. Tampilan Halaman Riwayat Pasien

Tampilan Hasil Enkripsi Database Riwayat Pasien



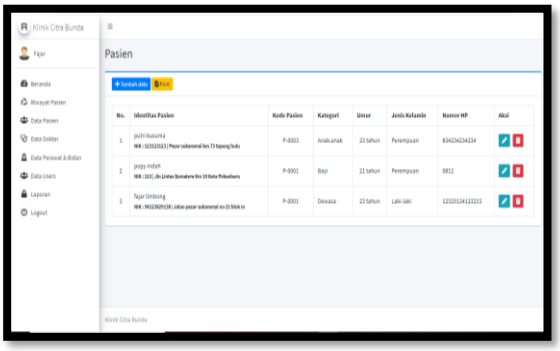
Gambar 7. Tampilan Hasil Enkripsi Database Riwayat Pasien

Tampilan Halaman Data Riwayat Pasien



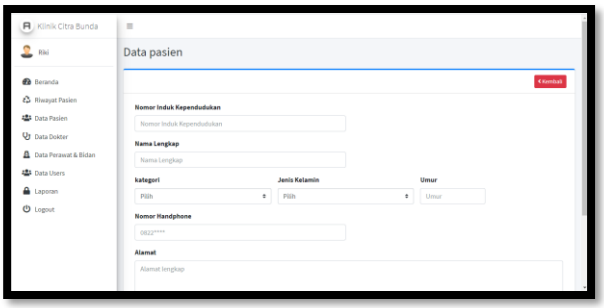
Gambar 8. Tampilan Data Halaman Riwayat Pasien

Tampilan Halaman Pasien



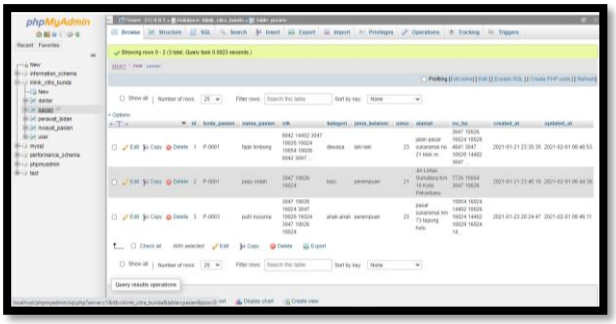
Gambar 9. Tampilan Halaman Pasien

Tampilan Halaman Data Pasien



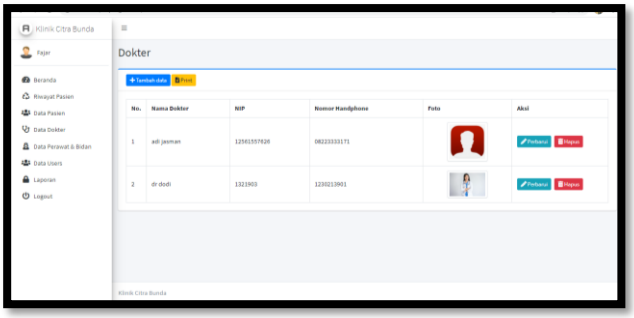
Gambar 10. Tampilan Halaman Data Pasien

Tampilan Hasil Enkripsi Database halaman Pasien



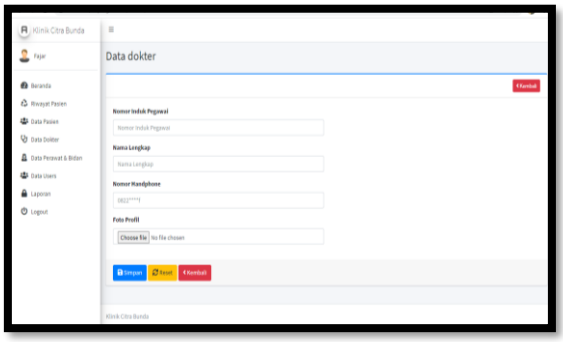
Gambar 11. Hasil Enkripsi Database halaman pasien

Tampilan Halaman Dokter



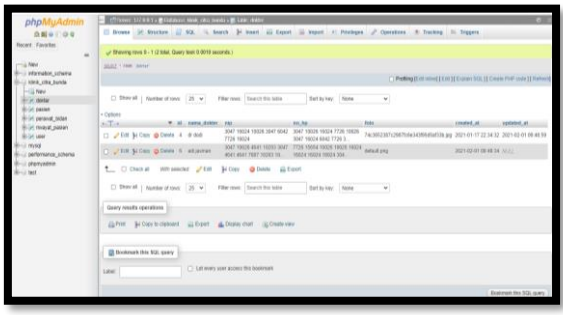
Gambar 12. Tampilan Halaman Dokter

Tampilan Halaman Tambah Data Dokter



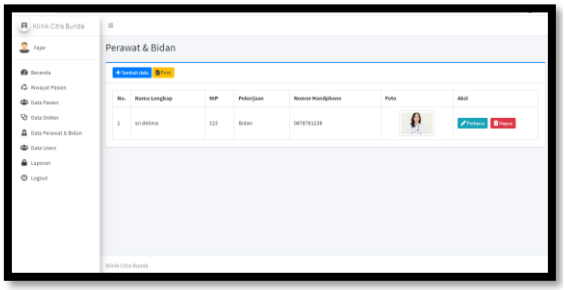
Gambar 13. Tampilan Halaman Tambah Data Dokter

Tampilan Hasil Enkripsi Database halaman Dokter



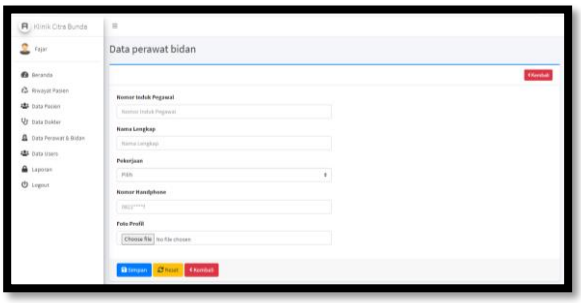
Gambar 14. Tampilan Hasil Enkripsi Database Halaman Dokter

Tampilan Halaman Data Perawat dan Bidan



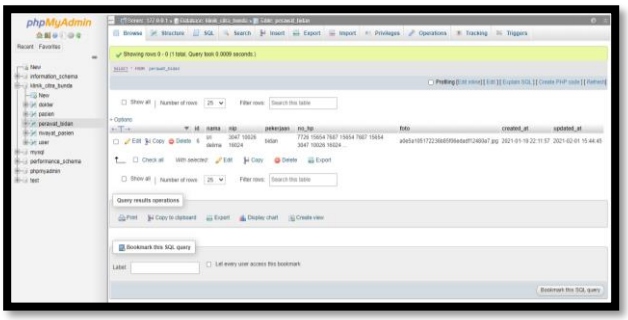
Gambar 15. Tampilan Halaman Data Perawat dan Bidan

Tampilan Halaman Tambah Data Perawat dan Bidan



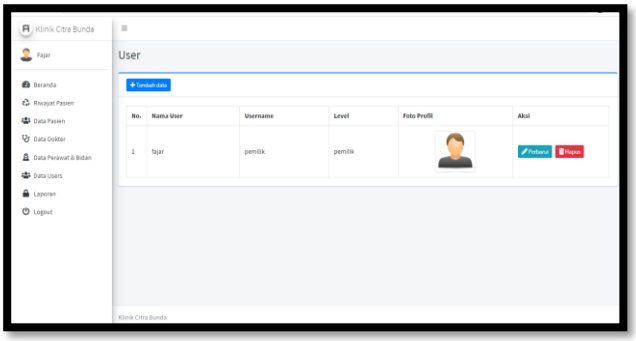
Gambar 16. Tampilan Tambah Data Perawat dan Bidan

Tampilan Halaman Hasil Enkripsi Data Perawat dan Bidan



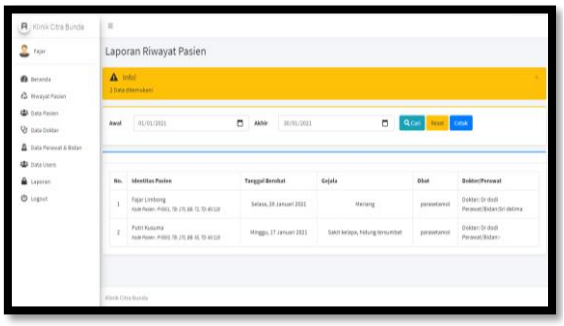
Gambar 17. Tampilan Hasil Enkripsi Data Perawat dan Bidan

Tampilan Halaman User



Gambar 18. Tampilan Halaman User

Tampilan Halaman Laporan Data Riwayat Pasien



Gambar 20. Tampilan Halaman Laporan Data Riwayat Pasien

SIMPULAN

Dari hasil kegiatan dan uraian dalam pembahasan laporan ini, penulis dapat menyimpulkan sebagai berikut:

1. Algoritma Kriptografi RSA (*Rivest Shamir Adleman*) dapat di Implementasikan pada Aplikasi Rekam Medis Pasien sebagai keamanan data Pasien yang terdapat di database.
2. Menyediakan data dan informasi berbasis web agar data dapat diakses dengan mudah oleh pihak klinik.
3. Mengurangi adanya pemalsuan atau kebocoron data dokumen di Klinik Citra Bunda.

DAFTAR PUSTAKA

Andriani, D. (2017). Perancangan Aplikasi Penyandian Teks Dengan Menggunakan Algoritma Chiper Block Chaining. *Jurnal Teknik Informatika UNIKA Santo Thomas, 2*(2), 14-23.

Anggraini, D., & Juanita, S. (2018). Aplikasi E-Arsip Pengamanan Pesan Elektronik Berbasis Web dengan Mengimplementasikan Algoritma Kriptografi RSA dan Elgamal pada Klinik Dr. H. Hartono. *Jurnal Ilmiah, 6*(3), 122.

Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. *Jurnal Teknologi dan Sistem Komputer, 3*(2), 253-258.

Haryanto, E. V. (2021). Desain Steganografi untuk Keamanan Gambar dengan Algoritma RSA dan LSB Berbasis Android. *CSRID (Computer Science Research and Its Development Journal), 11*(3), 179-190.

Rakhman, A. A., & Kurniawan, A. W. (2015). Implementasi Algoritma Kriptografi Rivest Shamir Adleman (Rsa) Dan Vigenere Cipher Pada Gambar Bitmap 8 Bit. *Techno. Com, 14*(2), 122-134.

Setyawati, E., Widjayanti, C. E., Siraiz, R. R., & Wijoyo, H. (2021). Pengujian keamanan komputer kriptografi pada surat elektronik berbasis website dengan enkripsi metode MD5. *Jurnal Manajamen Informatika Jayakarta, 1*(1), 56-67.

Siringoringo, R. (2020). Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File. *KAKIFIKOM: Kumpulan Artikel Karya Ilmiah Fakultas Ilmu Komputer, 2*(1), 31-42.

Tohirin, T. (2020). Penerapan Keamanan Remote Server Melalui Ssh Dengan Kombinasi Kriptografi Asimetris Dan Autentikasi Dua Langkah. *JurTI (Jurnal Teknologi Informasi), 4*(1), 133-138.

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer, 10*(1), 20-31.

Yusfrizal, Y. (2019). Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android. *JTIK (Jurnal Teknik Informatika Kaputama)*, *3*(2), 29-37.