Jurnal Kajian Ilmiah Teknologi Informasi dan Komputer
ISSN 2962-9055 (Media Online)
Vol 2, No 2, May 2024
Hal 65-73
https://journal.grahamitra.id/index.php/jutik

Implementasi Algoritma Rivest Shamir Adleman (RSA) Untuk Keamanan Data Rekam Medik Penyakit Pasien Rumah Sakit

Devi Tresia Tobing

Program Studi Teknik Informatika, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Budi Darma,
Jalan Sisingamanganraja No. 338, Medan, Sumatera Utara, Indonesia
Email: devitresiatobing@gmail.com

Abstrak

Rekam medis adalah catatan tentang siapa, apa, dimana, dan bagaimana perawatan pasien selama di rumah sakit. Salah satu aspek kegunaan rekam medis yaitu aspek dokumentasi yaitu rekam medis mengandung informasi penting yang bermanfaat untuk berbagai pihak. Rekam medis berisi data mengenai kesehatan masa lalu dan masa kini dan berisi catatan profesional kesehatan mengenai keadaan pasien saat ini dalam bentuk penemuan fisik, hasil prosedur diagnosa dan terapi serta respon pasien. Dokumen rekam medis milik dokter, dokter gigi dan sarana playanan kesehatan, sedangkan isi rekam medis merupakan milik pasien. Yang dapat diberikan, dicatat atau di gandakan pasien adalah ringkasan rekam medis. Pasien berhak mengetahui isi rekam medis akan tetapi berkas keseluruhan rekam medis hanya dapat dipegang oleh petugas kesehatan / rekam medis yang berwenang dan tidak dapat meninggalkan lokasi fasilitas kesehatan. Hal ini bertujuan untuk menjaga kerahasiaan medis (sebab informasi medis dapat disalahgunakan) serta mencegah rekam medis hilang atau rusak. Untuk mengatasi masalah tersebut dibutuhkan suatu sistem yang terkomputerisasi yang mampu mengamankan data rekam medis sehingga pihak- pihak yang tidak berkepentingan tidak dapat membacanya. Salah satu teknik yang dapat digunakan dalam mengamankan data rekam medis yaitu kriptografi. Kriptografi berasal dari bahasa yunani yang terdiri dari kata kryptos yang artinya tersembunyi dan graphia yang artinya sesuatu yang tertulis sehingga kriptografi dapat diartikan sebagai sesuatu yang tertulis secara rahasia atau tersembunyi.. Dalam menerapkan metode Rivest Shamir Adleman (RSA) dalam pengamanan data rekam medik pada Rumah Sakit Mitra Sejati Medan, yaitu dengan memasukkan coding program dari metode Rivest Shamir Adleman ke dalam bahasa pemograman yang digunakan. Selanjutnya membentuk kunci publik dan privat, kemudian melakukan proses enkripsi terhadap data rekam medik.

Kata Kunci: RSA; Kriptografi; Keamanan; Data; Rekam Medik; Rumah Sakit

Abstract

Medical records are records of the who, what, where, and how of patient care while in hospital. One aspect of the use of medical records is the documentation aspect, namely medical records contain important information that is useful for various parties. Medical records contain data regarding past and present health and contain health professional notes regarding the patient's current condition in the form of physical findings, results of diagnostic and therapeutic procedures and patient responses. Medical record documents belong to doctors, dentists and health service facilities, while the contents of medical records belong to the patient. What can be given, recorded or duplicated by the patient is a summary of the medical record. Patients have the right to know the contents of medical records, however, the entire medical record file can only be held by authorized health/medical records officers and cannot leave the location of the health facility. This aims to maintain medical confidentiality (because medical information can be misused) and prevent medical records from being lost or damaged. To overcome this problem, a computerized system is needed that is able to secure medical record data so that unauthorized parties cannot read it. One technique that can be used to secure medical record data is cryptography. Cryptography comes from Greek which consists of the words kryptos which means hidden and graphia which means something written so that cryptography can be interpreted as something written in secret or hidden.. In applying the Rivest Shamir Adleman (RSA) method in securing medical record data at home Mitra Sejati Medan Hospital, namely by inserting program coding from Shamir Adleman's Rivest method into the programming language used. Next, form a public and private key, then carry out the encryption process for medical record data.

Keywords: RSA; Cryptography; Security; Data; Medical record; Hospital

1. PENDAHULUAN

Mitra Sejati adalah salah satu rumah sakit umum swasta di kota medan Rumah sakit mitra sejati berada di daerah Kecamatan Medan Johor di Jl. AH. Nasution, rumah sakit ini banyak menangi pasien-pasien mulai dari penyakit ringan sampai penyakit berat. Pasien yang dirumah sakit mitra sejati akan dilakukan perekaman medis terhadap pasien, tentunya perekaman medis ini dilakukan oleh pihak resmi dari rumah sakit dan kepada pasien atau keluarga dekat pasien. Rekam medis berupa catatan tentang siapa, apa, bagaimana, apa dan dimana perawatan pasien selama di rumah sakit. rekam medis mengandung informasi penting yang bermanfaat untuk berbagai pihak. Rekam medis berisi data mengenai kesehatan masa lalu dan masa kini dan berisi catatan professional kesehatan mengenai keadaan pasien saat ini dalam bentuk penemuan fisik, hasil prosedur diagnosa dan terapi serta respon pasien [1].

Isi rekam medis adalah milik pasien sedangkan rekam medis yang dimasukkan kedalam bentuk dokumen adalah milik dokter dan sarana pelayanan kesehatan. Ringkasan rekam medis dapat dicatat dan diberikan kepada pada pasien. Hak pasien untuk mengetahui isi dari rekam medis , tetapi keseluruhan berkas yang ada di dalam rekam medis hanya dapat dipegang oleh petugas kesehatan/ rekam medis yang berwenang dan tidak dapat meninggalkan lokasi fasilitas kesehatan. Hal ini dilakukan untuk rahasia medis dapat terjaga (sebab penyalagunaan informasi medis dapat terjadi) serta mencegah hilang / rusaknya rekam medis. Dokter dan pasien yang dapat mengetahui informasi yang ada didalam rekam medis karena bersifat rahasia. Adapun jika informasi dari rekam medis diungkapkan, dikarenakan pasien telah melakukan persetujuan dan atas permintaan dari pasien itu sendiri, selain itu untuk pemenuhan keperluan penegak hukum atas

perintah pengadilan, institusi / lembaga berdasarkan undang-undang, untuk penelitian pendidikan dan audit medis, sepanjang tidak menyebutkan identitas pasien [2].

Selama ini Rumah Sakit Mitra Sejati dalam mengamankan data rekam medik tidak menggunakan sistem, mereka hanya menyimpan data rekam medik dalam bentuk file yang diprint dan diberi label rahasia. Tentunya hal ini kurang efektif dikarenakan dalam penyimpanan file sering terjadi kehilangan atau kerusakan file, kemudian data di dalam file tersebut juga dapat secara langsung dibaca, dicopy atau ditiru oleh orang yang tidak bertanggung jawab. Dibutuhkan suatu sitem yang terkomputerisasi untuk mengatasi masalah tersebut yang mampu mengamankan data-data rekam medis sehingga data tersebut tidak bisa dibaca oleh pihak yang tidak berkepentingan. Kriptografi merupakan teknik yang bisa digunakan untuk mengamankan data rekam medis. Kriptografi berasal dari kata kryptos yang merupakan bahasa yunani yang artinya tersembunyi dan graphia artinya suatu yang tertulis. Maka kriptografi adalah sesuatu yang tertulis secara sembunyi / rahasia.

Berdasarkan penelitian terdahulu yang dilakukan oleh Rahmat Sulaiman dengan judul Peningkatan Keamanan Pesan Berbasis Android Menggunakan Algortima kriptogafi RSA menyimpulkan bahwa dengan menggunakan fitur enkripsi dan dekripsi dalam aplikasi eclipse dan menambahkan algoritma kriptografi RSA dapat meningkatkan keamanan pesan berbasis android, proses dalam pengenkripsian pesan menggunakan key angka-angka dan ditentukan oleh pengirim dan pesan didekripsi dikirim menjadi pesan asli, sehingga pesan cukup aman dan tidak akan bisa dibaca oleh pihak lain [3].

Selain itu, penelitian yang dilakukan oleh Rizal Isnanto, Albert Ginting dan Ike Pratiwi dengan judul Implementasi Algoritma Algorima Kriptografi RSA menyimpulkan bahwa chipertext yang dihasilkan dari satu pesan asli adalah berbeda-beda, dikarenakan pembangkitan kunci RSA dalam prosesnya didasarkan pada P dan Q yang acak, akan menampilkan pesan kesalahan jika masukan bit pada saat dienkripsi bernilai kosong dan masukan password salah pada saat didekripsi [4].

Untuk mendukung kriptografi terdapat banyak algoritma yang bisa digunakan, algoritma RSA salah satunya. Ron Rivest, Adi Sahmir dan Len Adleman adalah penemu algoritma kriptografi dengan kunci publik (asimentris) yang bernama RSA (Rivest Shamir Adleman) pada tahun 1977. Kunci public dan rahasia merupakan kunci dari RSA.. konsep bilangan prima dan arimatika modul digunakan RSA dalam proses enkripsi dan dekripsi [5]. Pada penelitian ini penulis memilih menggunakan algoritma RSA karena sangat cocok digunakan untuk keamanan data rekam medik, algoritma RSA merupakan algoritma asimetris yang menggunakan 2 kunci berbeda untuk proses enkripsi dan dekripsinya, sehingga akan sulit di baca oleh orang lain atau pihak yang tidak bertanggung jawab.

Berdasarkan masalah yang ada dilatar belakang diatas, maka diangkat sebuah penelitian bertujuan untuk mengatasi masalah yang terjadi pada Rumah Sakit Mitra Sejati Medan dalam pengamanan data rekam medik dengan menerapkan metode RSA (Rivest Shamir Adleman) dalam pengamanan data rekam medik pada Rumah Sakit Mitra Sejati Medan.

2. METODOLOGI PENELITIAN

2.1 Kerangka Kerja Penelitian

Dalam penulisan penelitian ini maka perlu adanya susunan kerangka kerja (*frame work)* yang jelas tahapan-tahapannya. Kerangka kerja ini merupakan langkah-langkah yang akan dilakukan dalam penyelesaian masalah yang akan dibahas. Adapun kerangka kerja penelitian yang digunakan sebagai berikut ini.

1. Studi Literatur
   Pada tahap ini adalah tahap pembelajaran tentang sistem adalah mengumpulkan beberapa referensi yang akan digunakan dalam penelitan. Hal ini dilakukan untuk dapat diperoleh informasi dan data yang dibutuhkan untuk penulisan penelitian ini. Referensi yang digunakan dapat berupa karya tulis ilmiah, jurnal, buku-buku referensi, situs internet yang menyangkut dalam penelitian ini.
2. Analisis
   Pada tahap ini penulis menggunakan data-data yang telah didapat dan kemudian melakukan analisa terhadap hasil studi pustaka yang telah diperoleh.
3. Pengujian
   Pada tahap ini berupa prosedur dengan dasar pembuatannya, mengacu pada langkah-langkah yang ada dalam landasan teori sesuai dengan topik yang dibahas.
4. Implementasi Metode
   Pada tahap ini penulis mengimplementasikan metode Rivest Shamir Adleman (RSA) dalam kegiatan pengamanan data rekam medik pada Rumah Sakit Mitra Sejati Medan.
5. Laporan penelitian
   Sesuai hasil penelitian maka penulis merepresentasikan nilai efisiensi dan efektivitas metode Rivest Shamir Adleman (RSA) dalam pengamanan data rekam medik yang dituangkan dalam sebuah karya tulis ilmiah.

2.2 Kriptografi

Kriptografi adalah salah satu cara yang dapat digunakan untuk melindungi file atau mengamankan penyimpanan data dari akses illegal . selain itu kriptografi dapat melindungi dokumen dari orang yang melakukan kejahatan dengan merubah isi

Jurnal Kajian Ilmiah Teknologi Informasi dan Komputer
ISSN 2962-9055 (Media Online)
Vol 2, No 2, May 2024
Hal 65-73
https://journal.grahamitra.id/index.php/jutik

dokumen, mengubah password atau melakukan pemanfaatan guna untuk mencari keuntungan pribadi. Kriptogafi akan menyandikan informasi kedalam bentuk yang tidak bisa dimengerti lagi maknanya [6][7].

2.3 Algortima RSA

RSA adalah kriptografi asimetris dengan teknik kunci public yang populer. RSA memiliki keamanan yang tinggi dikarenakan penggunaan dua kunci yang berbeda pada proses enkripsi dan dekripsinya dan sulitnya memfaktorkan bilangan menjadi faktor prima dengan tujuan mendapat kunci untuk proses dekripsi. Namun salah satu ancaman yang sering dialami RSA adalah Brute Force Attack [8].

Proses dari enkripsi dan dekripsi tidak didasarkan dalam penggunaan algorima ini, proses matematikalah yang lebih dapat dilakukan dalam menghasilkan suatu kunci rahasia yang secara bebas bisa disebarkan tanpa dikhawatirkan karena pengirim dan penerima pesanlah yang dapat mendekripsikan kunci rahasia tersebut. Faktor-faktor prima akan difaktorkan oleh bilangan yang besar yang menjadi dasar dari algoritma ini [9].

Yang dibutuhkan dalam penggunakan algoritma RSA adalah dengan membuat kunci bernilai secara acak untuk digunakan pada saat pengengkripsian sebuah pesan , sehingga pesan dapat terjaga kerahasiaannya. Proses ini dilakukan pertama kali setelah pembentukan kunci yang sering disebut sebagai pembangkit kunci, setelah pembentukan kunci, selanjutnya dapat melakukan suatu proses enkripsi [10].

Adapun cara untuk menghasilkannya adalah sebagai berikut:

1. Membuat nilai p dan nilai q, dimana nilai variable tersebut bilangan prima akan tetapi nilai kedua bilangan tersebut tidak boleh sama, dimana nilai keduanya haruslah berbeda.
2. Membuat nilai untuk modulus untuk pasangan kunci public dan kunci rahasia. Nilai modulus adalah variable yang disimbolkan dengan n. Nilai n dihasilkan dari bilangan prima p dan q dimana nilai keduanya adalah hasil dari perkalian. Secara matematis, teknik yang digunakan dalam mencari nilai (RSA) modulus adalah sebagai berikut:
3. Menjumlahkan nilai Φ(n) maupun nilai totient/phi n
4. Cari nilai enciphering exponent disimbolkan dengan variabel e, akan digunakan untuk kunci public dan nilai modulus. Enciphering exponent (e) bilangan prima terhadap variabel Φ(n), e Φ(n) merupakan hasil pembagian yang bernilai harus 1.ketentuan $1< e < \Phi(n)$ dan e haruslah prima.
5. Selanjutnya adalah tentukan nilai deciphering exponent yang merupakan variabel d, nilai decipering exponent bertujuan pasangan pembangkit kunci dan modulus dalam algoritma RSA. variabel (n,d) adalah formula untuk menemukan nilai d didapatkan dengan persamaan: Variabel k adalah merupakan nilai yang bebas yang menghasilkan nilai d yang bersifat integer (bulat).
6. Nilai variabel d, p, dan q adalah nilai yang harus rahasi, nilai variabel n, e adalah nilai yang tidak perlu dirahasiakan (bebas), pasangan (n,e) merupakan kunci yang bersifat umum, pasangan (n,d) merupakan rahasia.

2.4 Rekam Medis

Secara sederhana dapat dikatakan bahwa rekam medis adalah kumpulan keterangan tentang identitas, hasil anamnesis, pemeriksaan dan catatan segala kegiatan para pelayanan kesehatan atas pasien dari waktu ke waktu [11]. Catatan ini berupa tulisan maupun gambar, dan belakangan ini pula berupa rekaman elektronik seperti computer, microfilm dan rekaman suara. Rekam medis adalah berkas yang berisikan yang berisikan catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang telah diberikan kepada pasien [12][13].

3. HASIL DAN PEMBAHASAN

3.1 Pembahasan

Sistem ini dibangun untuk pengamanan data rekam medik pada Rumah Sakit Mitra Sejati Medan. Setiap pasien yang datang ke Rumah Sakit Mitra Sejati Medan akan dilakukan perekaman medis terhadap pasien, tentunya dilakukan oleh pihak resmi di Rumah Sakit dan pasien atau keluarga terdekat pasien atas izin dari pasien. Informasi di dalam rekam medis berupa catatan tentang siapa, apa, dimana dan bagaimana perawatan pasien selama di rumah sakit adalah bersifat rahasia untuk menghindari penyalagunaan data rekam medis.

Pada proses kriptografi tersebut menggunakan metode Rivest Shamir Adleman (RSA). Algoritma RSA merupakan penerapan dari kriptografi asimetri, yakni jenis kriptografi yang menggunakan dua kunci yang berbeda yaitu kunci publik (public key) dan kunci pribadi (private key). RSA mendasarkan proses enkripsi dan deskripsinya pada konsep bilangan prima dan aritmatika modul.

Proses dari pengamanan data rekam medis menggunakan metode rivest shamir adleman dimulai dari membangkitkan kunci RSA yaitu kunci publik dan kunci privat. Kemudian melakukan enkripsi data rekam medis menggunakan kunci publik, maka data rekam medis seperti inisial pasien, alamat, tanggal masuk, tanggal keluar, hasil diagnosa, gejala dan dokter yang merawat akan terenkripsi. Selanjutnya untuk mengembalikan data yang terenkripsi yaitu dengan melakukan dekripsi data degan menggunakan kunci privat, maka data akan kembali ke bentuk semula.

Bersumber dari penelitian yang dilakukan di Rumah Sakit Mitra Sejati Medan diperoleh informasi data rekam medik pasien yaitu sebagai berikut:

Jurnal Kajian Ilmiah Teknologi Informasi dan Komputer
ISSN 2962-9055 (Media Online)
Vol 2, No 2, May 2024
Hal 65-73
https://journal.grahamitra.id/index.php/jutik

Tabel 1. Data Rekam Medik

Inisial Pasien	Alamat	Tgl. Masuk	Tgl. Pulang	Diagnosa Penyakit	Gejala Penyakit	Dokter Yang Merawat
SK	Jl. Setia Budi Gg. Tengah No. 34, Tanjung Sari – Medan Selayang	06 Januari 2020	09 Januari 2020	Demam Thyfoid	- Demam, Suhu tubuh 38^0c - Menggigil - Nafsu makan berkurang - Sakit kepala - Nyeri otot	dr.Salomo, Sp.PD
RT	Jl. Kemenyan 3 No. 14	16 Januari 2002	22 Jun 2020	Diabetes Melitus + Luka Ganggren	- Lemas - Pandangan Kabur - Luka Pada Tungkai Kaki - Sering Merasa Lapar Dan Haus - Berat Badan Menurun	dr. Salomo, Sp. PD
PL	Dusun 1V Sidodadi	23 Januari 2020	30 Januari 2020	PPOK	- Batuk berdahak - Sesak nafas - Lemas - Berat badan menurun - Nyeri dada	dr. Setia Putra, Sp. A

Pada rumah sakit Mitra Sejati Medan dalam mengamankan data rekam medik milik pasien yaitu dalam bentuk file yang diprint kemudian diberi label rahasi kemudian di simpan pada tempat tertentu, hanya orang-orang yang berkepentingan yg dapat membaca atau melihatnya.

Dalam penyimpanannya masih sering terjadi masalah seperti file yang hilang atau file yang rusak akibat faktor alam atau faktor manusia. Hal ini tentunya membuat kerugian, bagi bagi pasien ataupun bagi pihak Rumah Sakit. Untuk mengatasi masalah tersebut penulis membuat penelitian untuk mengamankan data rekam medik yang terkomputerisasi dengan menerapkan algoritma RSA. Sehingga diharapkan nantinya berkas rekam medik dapat di simpan di dalam komputer dan di enkripsi menggunakan kriptografi, hal ini agar tidak semua orang dapat membacanya apalagi menyalahgunakannya.

Pada contoh kasus dalam penelitian ini dilakukan proses pengamanan data rekam medik pada Rumah Sakit Mitra Sejati Medan. Adapun proses penyelesaian metode Rivest Shamir Adleman (RSA) untuk pengamanan data rekam medik adalah sebagai berikut:

1. Membangkitkan Kunci RSA. Algoritma Pembangkit
   Kunci RSA: $n = p \times q$
   $\phi(n) = (p-1) \times (q-1)$
   $e^R Z$ dengan gcd $(e,\phi(n)) = 1$
   $\leftarrow \phi(n)$
   $d = e^{-1}$ pada $Z_{\phi(n)}$
   $K_{Publik} = (e,n)$, $K_{Privat} = d$
2. Melakukan Enkripsi Data. Algoritma
   Enkripsi RSA
   Input : $K_{Publik} = (e,n)$, $P \in Z_n$
   Output : $C \in Z_n$
   $C : P^e \bmod n$ {gunakan algoritma *Square and Multiply*}
3. Melakukan Dekripsi Data
   Algoritma Dekripsi RSA
   Input : $KPrivat = KPublik = (e,n)$, $C \in Zn$
   Output : $P \in Zn$
   P : $Cd \bmod n$

Dalam pengujian perhitungan metodenya data yang akan di amankan sebagai contoh adalah data hasil diagnosa saja, untuk pengujian lengkapnya dapat di lihat pada aplikasi yang di bangun yang dapat dijelaskan pada bab selanjutnya. Berikut ini adalah algoritma penyelesaiannya

a. Pembangkit Kunci RSA

Jurnal Kajian Ilmiah Teknologi Informasi dan Komputer
ISSN 2962-9055 (Media Online)
Vol 2, No 2, May 2024
Hal 65-73
https://journal.grahamitra.id/index.php/jutik

Untuk menggunakan RSA terlebih dahulu pendeskripsi (*Bob*) membangkitkan sepasang kunci yaitu kunci publik dan kunci privat. Hal pertama yang dilakukan algoritma pembangkit kunci adalah membangkitkan 2 bilangan prima besar. Berikut ini algoritma penyelesaiannya:

1. Pilihlah bilangan prima dengan sembarang, dalam pemilihan ini, di pilih nilai prima (*p*) = 59 dan nilai (*q*) = 73.
2. Untuk mencari nilai dari kedua bilangan tersebut, maka dilakukan perkalian *n= p * q*
   *n= 59 * 73 = 4307*
3. Hitung (*phi*) *n*= (*p-1*) (q-1)
   *n= 58 * 72 = 4176*
4. Pilih nilai *e* dengan syarat *e* > 1 dan *greatest comman divisior* (*e,4176*) = 1
   Nilai e yang di ambil adalah 83. Bukti:
   (83, 4176)
   4176 mod 83 = 26
   83 mod 26 = 5
   26 mod 5 = 1
   5 mod 1 = 0
5. Sehingga de = 1 (mod 4176) dan d < 4176
   d * 83 = 1 mod 4176
   d * 83 mod 4176 =1
   d = 3371
   Bukti:
   3371 * 83 mod 4176 = 1
   Sehingga pasangan kunci yang di dapat adalah :
   Kunci enkripsi (public key)(e,n) = (83, 4307) dan Kunci dekripsi (private key)(d,n) = (3371, 4307)

b. Proses Enkripsi Data

Setelah di dapat nilai dari kunci enkripsi (public key), maka selanjutnya adalah melakukan enkripsi data plaintext P = Demam Thyfoid

Pertama yang harus di lakukan adalah merubah plaintext menjadi format ASCII, berikut ini adalah penyelesaiannya:

Plaintext : D e m a m (spasi) T h y f o i d
ASCII : 68 101 109 97 109 32 84 104 121 102 111 105 100

Kemudian p di pecah menjadi tiap karakter plaintext. Berikut ini adalah tabel Pi:

Tabel 2. Karakter Pi dan Kode ASCII untuk Plaintext Demam Thyfoid

Pi	Keterangan	Kode ASCII
P1	D	68
P2	e	101
P3	m	109
P4	a	97
P5	m	109
P6	(spasi)	32
P7	T	84
P8	h	104
P9	y	121
P10	f	102
P11	o	111
P12	I	105
P13	D	100

Setelah di bagi perkarakater, selanjutnya di enkripsi dengan rumus Ci = Pi^e mod n, yaitu sebagai berikut:

C1 = 68^83 mod 4307 = 772
C2 = 101^83 mod 4307 = 3971
C3 =109^83 mod 4307 = 821
C4 = 97^83 mod 4307 = 1822
C5 = 109^83 mod 4307 = 821
C6 = 32^83 mod 4307 = 2046
C7 = 84^83 mod 4307 = 2735
C8 = 104^83 mod 4307 = 3970
C9 = 121^83 mod 4307 = 2470
C10 = 102^83 mod 4307 = 1938
C11 = 111^83 mod 4307 = 2914

Jurnal Kajian Ilmiah Teknologi Informasi dan Komputer
ISSN 2962-9055 (Media Online)
Vol 2, No 2, May 2024
Hal 65-73
https://journal.grahamitra.id/index.php/jutik

C12 = 105^83 mod 4307 = 1900
C13 = 100^83 mod 4307 = 4134

Tabel 3. Karakter Ci dan Kode ASCII untuk Plaintext Demam Thyfoid

Ci	Kode
C1	772
C2	3971
C3	821
C4	1822
C5	821
C6	2046
C7	2735
C8	3970
C9	2470
C10	1938
C11	2914
C12	1900
C13	4134

Maka, setelah di enkripsi hasilnya yaitu, 772, 3971, 821, 1822, 821, 2046, 2735, 3970, 2470, 1938, 2914, 1900, 4134.

c. Proses Dekripsi Data

Proses dekripsi adalah proses untuk mengembalikan ke bentuk semula (plaintext), setelah chipertext dari kata Demam Thyfoid di dapat. Untuk merubah kembali menjadi plaintext yaitu melakukan dekripsi dengan rumus Pi= Ci^d mod n. Berikut ini adalah penyelesaiannya:

P1 = 772^3371 mod 4307 = 68
P2 = 3971^3371 mod 4307 = 101
P3 = 821^3371 mod 4307 = 109
P4 = 1822^3371 mod 4307 = 97
P5 = 821^3371 mod 4307 = 109
P6 = 2046^3371 mod 4307 = 32
P7 = 2735^3371 mod 4307 = 84
P8 = 3970^3371 mod 4307 = 104
P9 = 2470^3371 mod 4307 = 121
P10 = 1938^3371 mod 4307 = 102
P11 = 2914^3371 mod 4307 = 111
P12 = 1900^3371 mod 4307 = 105
P13 = 4134^3371 mod 4307 = 100

Maka, setelah di dekripsi hasilnya yaitu, 68, 101, 109, 97, 109, 32, 84, 104, 121, 102, 111, 105, 100 dalam karakter ASCII adalah:
ASCII : 68 101 109 97 109 32 84 104 121 102 111 105 100
Karakter : Demam Thyfoid

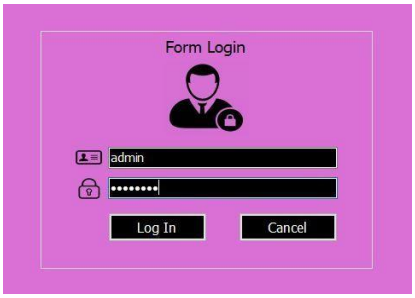
3.2 Hasil Pengujian

Implementasi sistem merupakan kegiatan akhir dari proses penerapan sistem, dimana sistem ini akan dioperasikan secara menyeluruh. Sebelum sistem benar-benar bisa digunakan dengan baik, sistem harus melalui tahap pengujian terlebih dahulu untuk menjamin tidak ada kendala yang muncul pada saat sistem digunkan. Implementasi yang dilakukan terdapat beberapa tahap prosedur untuk menyelesaikan analisa yaitu aplikasi yang disetujui, melakukan penginstalan, pengujian data, dan memulai menggunakan sistem yang diperbaiki atau sistem baru. Implementasi sebagai dukungan sistem analisa diperlukan beberapa perangkat-perangkat sebagai berikut :

a. Tampilan Form Login

Berikut ini merupakan tampilan dari form login yang berfungsi untuk melakukan proses validasi username dan password pengguna.

Jurnal Kajian Ilmiah Teknologi Informasi dan Komputer
ISSN 2962-9055 (Media Online)
Vol 2, No 2, May 2024
Hal 65-73
https://journal.grahamitra.id/index.php/jutik



Gambar 1. Form Login

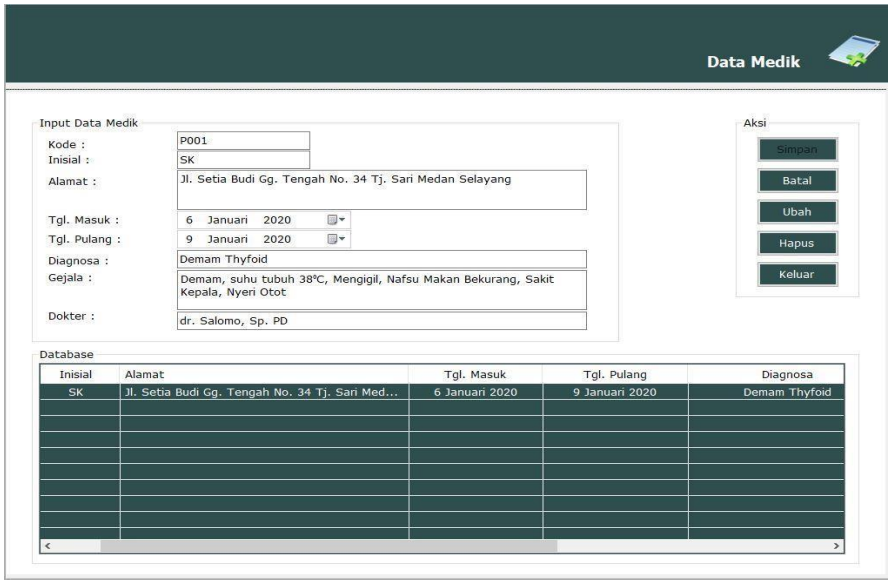
b. Tampilan Menu Utama

Berikut ini merupakan tampilan menu utama dari sistem pengamanan data rekam medik pada Rumah Sakit Mitra Sejati Medan:

Gambar 2. Form Menu Utama

c. Form Masukan Data Rekam Medik

Berikut ini merupakan tampilan dari form masukan data rekam medik yang berfungsi untuk menginput data-data rekam medik:

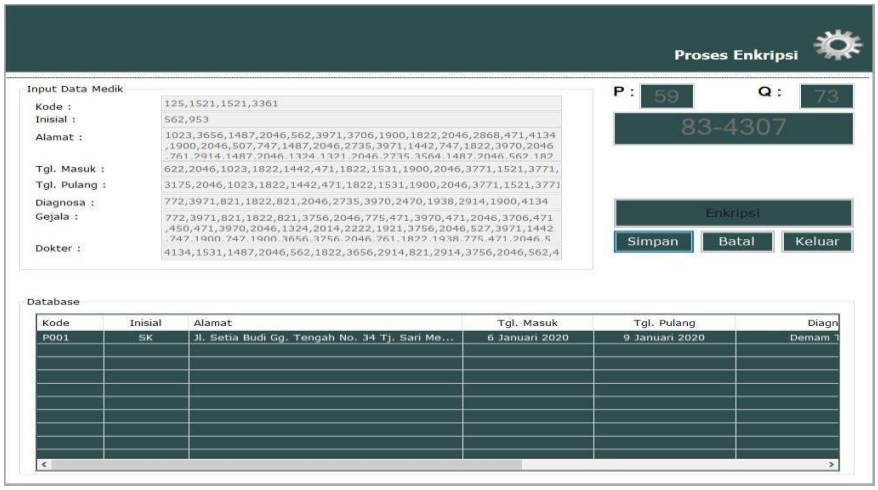


Gambar 3. Form Masukan Data Rekam Medik

d. Form Proses Enkripsi

Berikut ini merupakan tampilan dari form proses enkripsi yang berfungsi untuk proses enkripsi dari data rekam medik:

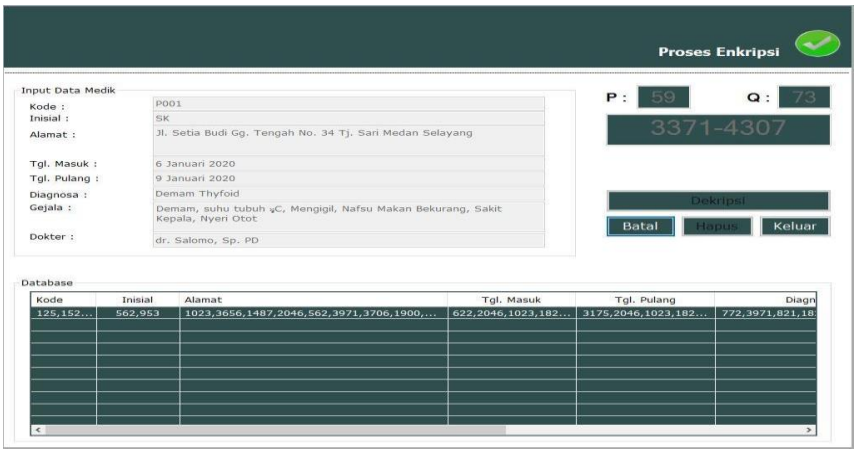
Jurnal Kajian Ilmiah Teknologi Informasi dan Komputer
ISSN 2962-9055 (Media Online)
Vol 2, No 2, May 2024
Hal 65-73
https://journal.grahamitra.id/index.php/jutik



Gambar 4. Form Proses Enkripsi

e. Form Proses Dekripsi

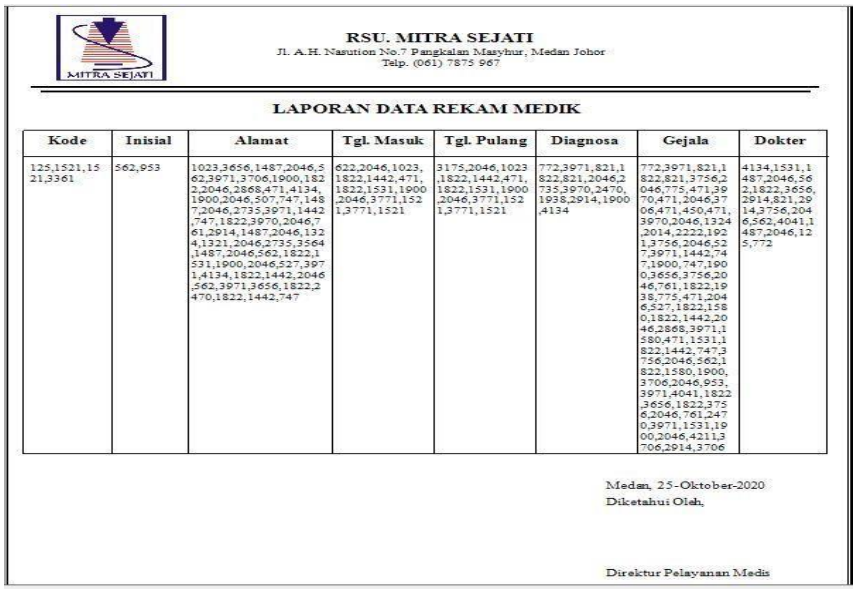
Berikut ini merupakan tampilan dari form proses dekripsi yang berfungsi untuk proses dekripsi dari data rekam medik:



Gambar 5. Form Proses Dekripsi

f. Tampilan Form Laporan

Laporan ini berfungsi untuk menampilkan hasil enkripsi data rekam medik untuk pengamanan data rekam medik pada Rumah Sakit Mitra Sejati Medan.



RSU. MITRA SEJATI
Jl. A.H. Nasution No.7 Pangkalan Masyhur, Medan Johor
Telp. (061) 7875 987

LAPORAN DATA REKAM MEDIK

Kode	Inisial	Alamat	Tgl. Masuk	Tgl. Pulang	Diagnosa	Gejala	Dokter
125,1521,1521,3361	562,953	1023,3656,1487,2046,562,3971,3706,1900,1822,2046,2868,471,4134,1900,2046,507,747,1487,2046,2735,3971,1442,747,1822,3970,2046,761,2914,1487,2046,1324,1321,2046,2735,3564,1487,2046,562,1822,1531,1900,2046,527,3971,4134,1822,1442,2046,562,3971,3656,1822,2470,1822,1442,747	622,2046,1023,1822,1442,471,1822,1531,1900,2046,3771,1521,3771,1521	3175,2046,1023,1822,1442,471,1822,1531,1900,2046,3771,1521,3771,1521	772,3971,821,1822,821,2046,2735,3970,2470,1938,2914,1900,4134	772,3971,821,1822,821,3756,2046,775,471,2970,471,2046,3706,471,450,471,3970,2046,1324,2014,2222,1921,3756,2046,527,3971,1442,747,1900,747,1900,3656,3756,2046,761,1822,1938,775,471,2046,527,1822,1580,1822,1442,2046,2868,3971,1580,471,1531,1822,1442,747,3756,2046,562,1822,1580,1900,3706,2046,953,3971,4041,1822,3656,1822,3756,2046,761,2470,3971,1531,1900,2046,4211,3706,2914,3706	4134,1531,1487,2046,562,1822,3656,2914,821,2914,3756,2046,562,4041,1487,2046,125,772

Medan, 25-Oktober-2020
Diketahui Oleh,

Direktur Pelayanan Medis

Gambar 6. Tampilan Form Laporan

4. KESIMPULAN

Adapun yang menjadi kesimpulan pada penelitian dimana dalam mengatasi masalah yang terjadi pada Rumah Sakit Mitra Sejati Medan dalam pengamanan data rekam medik yaitu dengan membuat suatu aplikasi berbasis komputer yang menerapkan algoritma kriptografi untuk keamanan data, selanjutnya algoritma kriptografi tersebut dimasukkan ke dalam source code program dan akan melakukan enkripsi data secara otomatis. Dalam menerapkan metode Rivest Shamir Adleman (RSA) dalam pengamanan data rekam medik pada Rumah Sakit Mitra Sejati Medan, yaitu dengan memasukkan coding program dari metode Rivest Shamir Adleman ke dalam bahasa pemograman yang digunakan. Selanjutnya membentuk kunci publik dan privat, kemudian melakukan proses enkripsi terhadap data rekam medik. Sistem yang telah dirancang selanjutnya diuji dan diimplementasikan dengan memasukkan data-data sesuai dengan yang ada pada bab-bab sebelumnya, kemudaian jika hasil outputnya sesuai dengan data manual maka dalam pengujian ini sistem berjalan dengan baik, menambahkan data ke database, perintah update untuk merubah data di database, perintah delete untuk menghapus data di database..

REFERENCES

[1] Tazia Intan Prasasti and Dian Budi Santoso, "Keamanan dan Kerahasiaan Berkas Rekam Medis di RSUD Dr. Soehadi Prijonegoro Sragen," 2017.
[2] Muhammad Husni Azam, Jaka Presetya, Alumni Fakultas Kesehatan UDINUS, and Staff Pengajar Fakultas Kesehatan UDINUS, "ASPEK KEAMANAN ISI DAN FISIK DOKUMEN REKAM MEDIS DITINJAU DARI HUKUM KESEHATAN DI RSU RA KARTINI JEPARA TAHUN 2015,".
[3] Silvester Tena and Sarlince O Manu, "ANALISIS PERBANDINGAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) & RIVEST CODE 6 (RC6) DALAM KEAMANAN CITRA DIGITAL,".
[4] Faizal Zuli and Ari Irawan, "IMPLEMENTASI KRIPTOGRAFI DENGAN ALGORITMA BLOWFISH DAN RIVERST SHAMIR ADLEMAN (RSA) UNTUK PROTEKSI FILE".
[5] Fresly Nandar Pabokory, Indah Fitri Astuti, and Awang Harsa Kridalaksana, "IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD," 2015.
[6] Suhardi, "APLIKASI KRIPTOGRAFI DATA SEDERHANA DENGAN METODE EXLUSIVE-OR (XOR)," 2016.
[7] "55-188-1-PB".
[8] Muhammad Iqbal Zulfikar, Gunawan Abdillah, Agus Komarudin Jurusan Informatika, and Fakultas Sains dan Informatika Universitas Jenderal Achmad Yani Cimahi, "Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA),".
[9] Awang Harsa, Andi Yusika, and Asfami Ansharie, "ENKRIPSI DATA AUDIO MENGGUNAKAN METODE KRIPTOGRAFI RSA,".
[10] Pandi Barita, Nauli Simangunsong, and Komariah Fitri, "Perancangan Aplikasi Pengamanan Citra Bewarna Dengan Algoritma RSA," 2018.
[11] Analisis RM Kuantitatif Kelengkapan Dokumen Rekam Medis Pasien Rawat Inap Dengan Diagnosa Fracture Femur Di RSUD Djoelham Binjai and Maysyarah Yolla Rizkika, "TELKOMNIKA," 2020.
[12] Nur Fadilah Dewi, dan Karmelia Agustina, Prodi Perumahsakitan, Program Pendidikan Vokasi Universitas Indonesia, and Kesehatan Kostrad, "Analisis Sistem Pelayanan Rekam Medis Rawat Inap di RSUP Dr. Kariadi Semarang Tahun 2016,".