BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Rekam medis merupakan berkas yang berisi catatan dan dokumentasi mengenai identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang telah diberikan kepada pasien [1]. Rekam medis dibuat dengan tujuan untuk menciptakan tertib administrasi dalam upaya peningkatan pelayanan kesehatan di rumah sakit yang didukung oleh suatu pengelolaan rekam medis dengan baik dan benar [2]. Dalam pengelolaan rekam medis adanya perkembangan dalam teknologi informasi yaitu transisi dari rekam medis berbasis kertas menjadi rekam medis elektronik [3].

Pada kenyataannya rekam medis elektronik memiliki beberapa ancaman terhadap keamanan data yang menyebabkan bocornya data rekam medis atau diaksesnya data rekam medis elektronik oleh orang lain [4]. Kondisi tersebut sangat mengkhawatirkan karena data yang terdapat dalam rekam medis bersifat rahasia sehingga perlu untuk dilakukan pengamanan data. Data tersebut harus terjamin agar tidak bisa diakses oleh pihak lain karena dapat merugikan pasien maupun dokter. Masalah terkait keamanan data tersebut terjadi pada Rumah Sakit Mitra Husada. Berdasarkan hasil wawancara dengan Staff IT Rumah Sakit Mitra Husada, pernah terjadi kasus pengubahan dan penghapusan data rekam medis yang kemungkinan dilakukan oleh pihak internal Rumah Sakit yang tidak memiliki hak akses. Hal tersebut diakibatkan oleh 2 faktor yaitu Data Rekam Medis dan Data User belum

memiliki sistem pengamanan dan akses server yang masih rentan dikarenakan port terbuka melalui IP Publik. Hal tersebut dapat mengakibatkan sistem rawan terhadap tindakan pencurian dan penyalahgunaan data oleh pihak lain yang tidak memiliki hak akses. Berdasarkan Peraturan Pemerintah Nomor 32 tahun 1996 pasal 22 ayat (1) tentang Standar Profesi dan Perlindungan Hukum yang membahas tentang kerahasiaan identitas dan data kesehatan pribadi pasien dan pemeliharaan rekam medis. Maka dari itu perlu dilakukan upaya untuk melakukan pengamanan data salah satunya dengan menggunakan algoritma kriptografi.

Kriptografi merupakan teknik untuk menyimpan dan mengirimkan data dalam format tertentu dan dapat menyembunyikan informasi secara sistematis sehingga hanya pihak berwenang yang memiliki akses [5]. Algoritma kriptografi berisi fungsi matematika yang digunakan untuk melakukan proses enkripsi dan dekripsi. Algoritma kriptografi dapat diklasifikasikan berdasarkan kuncinya, salah satunya yaitu kunci asimetris. Kunci asimetris menggunakan dua kunci yang berbeda yaitu kunci publik dalam melakukan proses enkripsi dan kunci privat dalam melakukan proses dekripsi [6]. Contoh dari algoritma yang menggunakan kunci asimetris adalah algoritma *Rivest Shamir Adleman* (RSA) [7]. Algoritma RSA merupakan algoritma yang menggunakan bilangan faktorisasi terbesar dan metode distribusi yang sulit dipecahkan [8]. Kekuatan utama dari algoritma RSA yaitu didasarkan pada kesulitan pemfaktoran dalam bilangan bulat besar [9]. Keunggulan dari algoritma ini terletak pada proses eksponensialnya, yaitu menguraikan suatu bilangan menjadi 2 bilangan prima, dan kedua bilangan prima ini membutuhkan waktu yang lama untuk melakukan pemfaktorannya.

Berdasarkan uraian permasalahan di atas, maka peneliti akan melakukan penelitian dengan judul "RANCANG BANGUN APLIKASI KEAMANAN DATA REKAM MEDIS PASIEN MENGGUNAKAN ALGORITMA *RIVEST SHAMIR ADLEMAN* (RSA) BERBASIS WEB (STUDI KASUS: RUMAH SAKIT MITRA HUSADA)". Dengan adanya penelitian ini diharapkan mampu melindungi data rekam medis pasien yang ada di Rumah Sakit Mitra Husada.

1.2 Identifikasi Masalah

Berdasarkan uraian dalam latar belakang masalah, maka masalah yang dapat diidentifikasi dalam penelitian ini yaitu:

1. Belum adanya sistem pengamanan data rekam medis di Rumah Sakit Mitra Husada terutama data pasien yang bersifat rahasia sesuai dengan Peraturan Pemerintah Nomor 32 tahun 1996 pasal 22 ayat (1) tentang Standar Profesi dan Perlindungan Hukum yang membahas tentang kerahasiaan identitas dan data kesehatan pribadi pasien dan pemeliharaan rekam medis.
2. Pernah terjadinya serangan pada sistem sehingga dikhawatirkan data rekam medis dicuri atau bocor dan disalahgunakan oleh orang yang tidak memiliki hak akses dan terdapat kasus pengubahan dan penghapusan data rekam medis yang kemungkinan dilakukan oleh pihak internal Rumah Sakit yang tidak memiliki hak akses. Hal tersebut disebabkan Data Rekam Medis dan Data User belum memiliki sistem pengamanan dan akses server yang masih rentan dikarenakan port terbuka melalui IP Publik.

1.3 Rumusan Masalah

Berdasarkan masalah yang telah diidentifikasi dan telah dijelaskan sebelumnya, maka peneliti dapat merumuskan masalah dalam penelitian ini yaitu sebagai berikut:

1. Bagaimana membangun aplikasi yang dapat melakukan pengamanan dan mengantisipasi serangan atau kebocoran data rekam medis pasien?
2. Bagaimana mengimplementasikan algoritma *Rivest Shamir Adleman* (RSA) dalam rancang bangun aplikasi keamanan data rekam medis pasien?

1.4 Batasan Masalah

Agar penelitian dapat fokus untuk mengatasi permasalahan, maka dari itu diperlukan batasan masalah dalam penelitian ini antara lain yaitu:

1. Sistem yang dibangun ditujukkan untuk melakukan pengamanan data rekam medis pasien secara enkripsi dan dekripsi.
2. *Output* yang dihasilkan dari penelitian ini adalah sebuah aplikasi berbasis *website* yang dapat melakukan pengamanan data rekam medis pasien.
3. Data rekam medis yang diamankan yaitu DIAGNOSA AWAL dan DIAGNOSA AKHIR.
4. Data rekam medis pasien yang diinput adalah pasien BPJS.
5. Aktor atau *user* yang terlibat dalam aplikasi ini yaitu Admin Poli dan PPA (Professional Pemberi Asuhan) meliputi Dokter, Bidan, Perawat.

6. Hak akses untuk aktor atau *user*, yaitu :

   a. Admin Poli

      - Login diharuskan ketika admin poli akan mengakses sistem.
      - Admin poli dapat mengelola data rekam medis pasien.
      - Admin poli dapat menginput data rekam medis pasien.

   b. PPA (Professional Pemberi Asuhan)

      - Login diharuskan ketika PPA akan mengakses sistem.
      - Dokter dapat mengakses data rekam medis yang sudah didekripsi dengan cara memasukkan kunci *private* lalu klik tombol dekripsi yang terdapat dalam sistem dan memberi tindakan pada sistem untuk pasien seperti *Hecting* (Menjahit luka), *Up Hecting* (Membuka Jahitan), Cuci Luka Sedang, Cuci Luka Berat, Pemeriksaan Kadar Gula Darah, Kolesterol, Asam Urat dan *Nebulizer*.
      - Bidan dapat mengakses data rekam medis yang sudah didekripsi dengan cara memasukkan kunci *private* lalu klik tombol dekripsi yang terdapat dalam sistem dan memberi tindakan pada sistem untuk pasien seperti Partus (lahiran) di ruang Ponek (ruang bersalin IGD) atau di ruang VK (ruang bersalin rawat inap) dan dengan lahiran normal atau *Sectio Caesarea* (sc).
      - Perawat dapat mengakses rekam medis yang sudah didekripsi didekripsi dengan cara memasukkan kunci *private* lalu klik tombol dekripsi yang terdapat dalam sistem dan melihat tindakan yang berikan oleh Dokter dan Bidan pada sistem.

7. *Tools* yang digunakan dalam membangun sistem adalah sebagai berikut:
    - Sistem dibangun dengan menggunakan bahasa pemrograman *Python* serta MySQL sebagai *database.*
    - Sistem dirancang dengan menggunakan aplikasi draw.io

1.5 Tujuan Penelitian

Adapun tujuan dari dilakukannya penelitian ini yaitu sebagai berikut:

1. Untuk membangun aplikasi yang dapat melakukan pengamanan dan mengantisipasi serangan atau kebocoran data rekam medis pasien.
2. Untuk mengimplementasikan algoritma *Rivest Shamir Adleman* (RSA) dalam rancang bangun aplikasi keamanan data rekam medis pasien.

1.6 Manfaat Penelitian

Manfaat dari penelitian ini terbagi menjadi manfaat teoritis dan manfaat praktis sebagai berikut:

1. Manfaat Teoritis

   Penelitian ini diharapkan dapat dijadikan sebagai sumber bacaan atau referensi bagi pengembangan penelitian selanjutnya.

2. Manfaat Praktis

   Penelitian ini diharapkan dapat membantu pengamanan data rekam medis pasien pada Rumah Sakit Mitra Husada.

1.7 Pertanyaan Penelitian

Pertanyaan penelitian yaitu selaras dengan pertanyaan yang disusun dalam rumusan masalah sebagai berikut:

1. Bagaimana membangun aplikasi yang dapat melakukan pengamanan dan mengantisipasi serangan atau kebocoran data rekam medis pasien?
2. Bagaimana mengimplementasikan algoritma *Rivest Shamir Adleman* (RSA) dalam rancang bangun aplikasi keamanan data rekam medis pasien?

1.8 Hipotesis Penelitian

Hipotesis yang akan diuji dalam penelitian ini yaitu:

1. Aplikasi dapat menyimpan dan mengamankan data rekam medis pasien di Rumah Sakit Mitra Husada.
2. Penggunaan Algoritma RSA pada aplikasi dapat mencegah terjadinya kebocoran data rekam medis pasien.

1.9 Metodologi Penelitian

Metodologi yang digunakan dalam penelitian ini terbagi menjadi tiga yaitu metode pengumpulan data, metode pengembangan sistem, dan metode penyelesaian masalah.

1.9.1. Metode Pengumpulan Data

Metode pengumpulan data dalam penelitian ini terbagi menjadi tiga metode yaitu observasi, wawancara, dan studi pustaka. Alasan pemilihan tiga metode pengumpulan tersebut dikarenakan dengan melakukan observasi dan wawancara didapatkan data primer yang berasal dari sumbernya langsung. Selain itu dengan

melakukan studi literatur didapatkan data sekunder yang berasal dari sumber ilmiah seperti jurnal-jurnal penelitian sebelumnya yang berkaitan dengan penelitian ini.

1. Observasi

   Observasi dilakukan secara langsung dengan mendatangi Rumah Sakit Mitra Husada yang berada di Jl. Raya Siliwangi No. 151, Ciawigebang, Kecamatan Ciawigebang, Kabupaten Kuningan, Jawa Barat 45591. Observasi dilakukan untuk mengetahui lokasi Rumah Sakit, meminta izin melakukan penelitian, serta melakukan pengamatan sistem yang berjalan dan mencatat kebutuhan dalam melakukan penelitian.

2. Wawancara

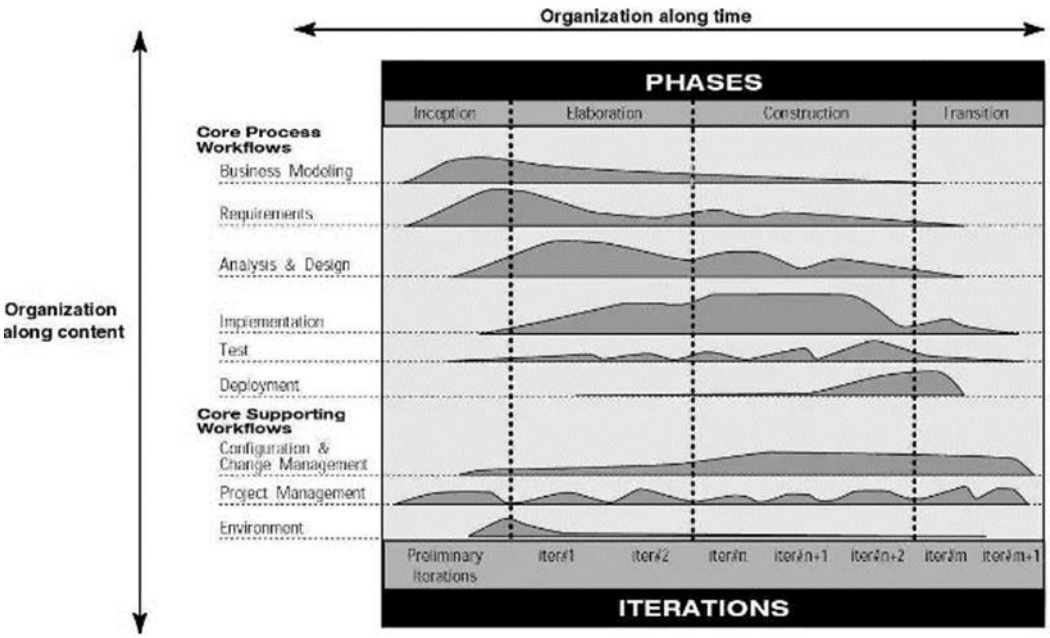
   Wawancara dilakukan dengan Wakil Direksi Bagian Umum yaitu Bapak dr. Fajar Rafsanjani Heryadi untuk membahas perizinan dan membahas terkait kebutuhan sistem serta dengan Kepala Staff IT yaitu bapak Andrik Hermawan, S.Kom beserta anggota Staff IT yaitu bapak Muhamad Iyad Muayyad, S.Kom untuk membahas sistem yang berjalan serta kebutuhan sistem di Rumah Sakit Mitra Husada.

3. Studi Pustaka

   Studi pustaka dilakukan dengan mencari sumber informasi yang bersifat ilmiah mengenai data rekam medis pasien, keamanan data rekam medis pasien, algoritma RSA serta hal-hal lain yang berhubungan dengan penelitian melalui sumber seperti jurnal.

1.9.2. Metode Pengembangan Sistem

Dalam mengembangkan sistem keamanan dalam penelitian ini digunakan metode pengembangan *Rational Unified Process* (RUP). RUP merupakan metode pengembangan perangkat lunak dengan iterasi untuk mendapatkan umpan balik pengguna yang berguna untuk menyelaraskan solusi perangkat lunak dengan kebutuhan pengguna. Setiap iterasi akan melewati empat tahapan yaitu *inception, elaboration, construction,* dan *transition* [11]. Tahapan dalam metode RUP yaitu sebagai berikut:



Gambar 1.1 Metode RUP [12]

1. *Inception* (Pemahaman Awal Proyek)

   Pada tahap ini dilakukan analisis kebutuhan pengguna dan melakukan perancangan awal perangkat lunak berupa *use case diagram.* Pada akhir tahap ini *prototype* perangkat lunak versi *alpha* harus sudah dirilis.

2. *Elaboration* (Analisis dan Perencanaan *Detail*)

   Tahap *elaboration* merupakan tahap untuk melakukan desain secara lengkap berdasarkan hasil pada tahap *inception.* Pada tahap ini dilakukan perancangan perangkat lunak dengan menggunakan *Unified Modeling Language* (UML) serta melakukan spesifikasi fitur yang dimiliki oleh perangkat lunak. Pada tahap ini terdapat perilisan *prototype* versi *betha* dari perangkat lunak.

3. *Construction* (Pengembangan Perangkat Lunak)

   Tahap *construction* merupakan tahapan dalam melakukan implementasi hasil desain dan melakukan pengujian hasil implementasi. Implementasi rancangan perangkat lunak dilakukan dengan menggunakan bahasa pemrograman *Phyton* dan dilakukan pengujian menggunakan metode *blackbox testing.*

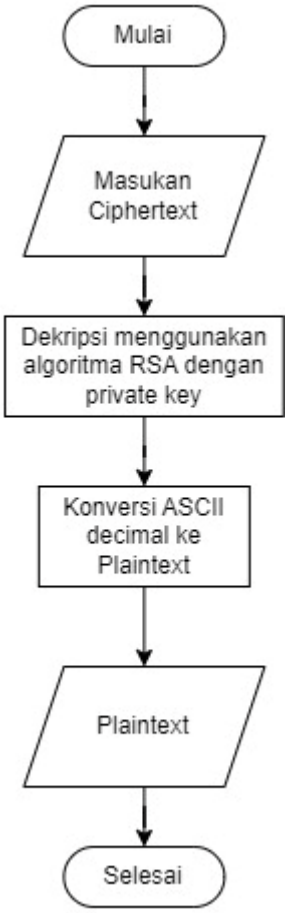
4. *Transition* (Pengiriman dan Pengujian)

   Pada tahap *transition* dilakukan untuk menyerahkan sistem aplikasi kepada *user* yang umumnya mencakup pelatihan dan *beta testing.*

1.9.3. Metode Penyelesaian Masalah

Dalam menyelesaikan masalah terkait keamanan data rekam medis pasien, dilakukan proses enkripsi dan dekripsi dengan menggunakan algoritma RSA. Pada proses enkripsi yaitu dilakukan dengan *generate* kunci publik yang digunakan untuk enkripsi dan kunci privat yang digunakan untuk dekripsi. Selanjutnya dilakukan enkripsi data rekam medis dengan kunci publik dan menghasilkan data yang telah dienkripsi berupa *ciphertext.* Lalu pada proses dekripsi dilakukan pada data rekam medis dengan kunci privat yang hanya dapat diakses oleh penerima sehingga menghasilkan data seperti semula. Metode penyelesaian masalah dengan menggunakan algoritma RSA melalui proses enkripsi dan dekripsi dapat dilihat pada Gambar 1.2 dan 1.3 dibawah:

Gambar 1.2 *Flowchart Enkripsi* RSA [13]



Gambar 1.3 *Flowchart Dekripsi* RSA [13]

RSA menggunakan 2 angka (e dan d) [14]. Keamanan pada algoritma ini ditunjukkan dengan sulitnya mencari hasil faktor-faktor prima dari bilangan yang besar, yang dalam hal ini adalah memfaktorkan n menjadi a dan b. Kemudian sekali n berhasil difaktorkan menjadi a dan b, maka $m = (a - 1)\ (b - 1)$ dapat dihitung. Selanjutnya karena kunci enkripsi diutamakan e bebas (tidak rahasia), maka kunci dekripsi d dapat dihitung dari persamaan $e.\ d = 1\ (mod\ m)$. Hal tersebut merupakan

proses dekripsi yang dilakukan oleh orang yang tidak berhak. Terdapat beberapa parameter penting pada algoritma RSA antara lain dapat dilihat pada Tabel 1.1 [14].

Tabel 1.1 Parameter Pada RSA [14]

Parameter	**Sifat**
P dan q (bilangan prima)	Rahasia
N = p.q	Tidak Rahasia
$\phi(n)$ = (p-1)(q-1)	Rahasia
e (kunci enkripsi)	Tidak Rahasia
d (kunci dekripsi)	Rahasia
m (plainteks)	Rahasia
C (Chipertext)	Tidak Rahasia

Terdapat tiga pondasi penting dalam algoritma kriptografi khususnya algoritma RSA yaitu Pembangkit Kunci, Enkripsi dan Dekripsi [14].

1.10 Jadwal Kegiatan Penelitian

Adapun jadwal kegiatan dalam penelitian ini dapat dilihat pada Tabel 1.2.

Tabel 1.2 Jadwal Kegiatan Penelitian

Kegiatan	Kegiatan penelitian tahun 2023-2024															
	November 2023				Desember 2023				Januari 2024				Februari 2024			
	I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV
Analisis Kebutuhan																
SUP																
Pemodelan / Design																
Implementasi / Coding																
Pengujian																
SHP																
Sidang Skripsi																

Kegiatan	Kegiatan penelitian tahun 2023-2024															
	Maret 2024				April 2024				Mei 2024				Juni 2024			
	I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV
Analisis Kebutuhan																
SUP																
Pemodelan / Design																
Implementasi / Coding																
Pengujian																
SHP																
Sidang Skripsi																

1.11 Sistematika Penulisan

BAB I PENDAHULUAN

Pada bab ini menjelaskan mengenai latar belakang masalah, identifikasi masalah, batasan masalah, tujuan penelitian, manfaat penelitian, pertanyaan penelitian, hipotesis penelitian, metodologi penelitian, jadwal kegiatan penelitian serta sistematika penelitian yang dilakukan.

BAB II LANDASAN TEORITIS

Pada bab ini menjelaskan mengenai teori-teori yang berkaitan dengan penelitian ini, tinjauan penelitian terdahulu, serta kerangka teroritis penelitian.

BAB III ANALISIS DAN PERANCANGAN

Pada bab ini berisi mengenai analisis sistem, perancangan sistem, dan perancangan antar muka pada sistem yang akan dibangun.

BAB IV PENGUJIAN DAN IMPLEMENTASI

Pada bab ini berisi mengenai pengujian terhadap sistem yang akan dibangun dengan menggunakan *blackbox testing* dan *whitebox testing.* Serta terdapat implementasi dari sistem yang dibangun.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi mengenai kesimpulan dari penelitian yang telah dilakukan serta dilakukan pemberian saran untuk pengembangan penelitian selanjutnya.