BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Kemudahan dalam memperoleh informasi tidak terlepas dari pengaruh teknologi dan ilmu pengetahuan yang terus berkembang yang salah satunya adalah dampak dari teknologi (Putra et al., 2022). Penggunaan teknologi pun sudah diterapkan di berbagai bidang karena perkembangannya yang sangat pesat. Mulai dari pekerjaan sederhana hingga pekerjaan yang sulit sekalipun. Penggunaan teknologi memang sangat diperlukan, namun masih ada juga hal yang tidak bisa dilupakan yaitu privasi data, karena pada dasarnya setiap informasi memiliki privasinya masing-masing (Khoirunnisa & Djuniadi, 2021).

Pada bidang kesehatan, data pasien baik berupa rekam medis adalah informasi yang bersifat rahasia atau hak milik karena informasi tersebut mencakup informasi pribadi tentang riwayat kesehatan pasien yang dimiliki baik oleh pasien maupun dokter. Informasi rekam medis adalah berkas yang berisi catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, prosedur dan pelayanan lain yang diberikan kepada pasien. Informasi tentang rekam medis dapat berupa teks, gambar, suara atau video (Kartika H, 2018). Pada peraturan yang ada di Menteri Kesehatan No. 269/MENKES/III/2008 tentang rekam medis, pasal 10 ayat menyatakan bahwa informasi atau data pada rekam medis memiliki nilai kerahasiaan yang harus dijaga karena rekam medis berisi riwayat kesehatan pasien. Oleh karena itu rumah sakit memiliki kewajiban untuk menjaga keamanan dan kerahasiaan rekam medis (Tarigan & Herfiyanti, 2021).

Selain disimpan oleh puskesmas atau rumah sakit terkait, data rekam medis terkadang juga akan dikirimkan ke rumah sakit lain sebagai data rujukan pasien. Adanya transfer data tersebut tentunya meningkatkan kemungkinan penyebaran atau penyalahgunaan informasi. Efek negatif ini hanyalah salah satu dari banyak efek yang disadari pengguna komputer saat ini. Melihat adanya kemungkinan tersebut, maka perlu dilakukan pencegahan berupa perlindungan dokumen guna mengurangi hal yang tidak semestinya (Khoirunnisa & Djuniadi, 2021).

Di puskesmas Pematang Raya kegiatan rekam medis belum terkomputerisasi sepenuhnya. Rekam medis di puskesmas ini masih dibuat menggunakan sistem manual dan untuk data rujukan petugas menyimpan data rekam medis di media komputer. Perlindungan data pada media komputer dan pada saat mengirim data perlu diperhatikan guna mengurangi hal yang tidak semestinya. Terkadang petugas juga kesusahan untuk mencari data pasien secara manual. Sehingga diperlukan sistem rekam medis guna kemudahan mengelola data, mengirim data dengan sistem keamanan yang mencegah baik terjadinya kebocoran data rekam medis. sehingga mencegah terjadinya kebocoran data rekam medis.

Proses dalam mengamankan data, dibutuhkan teknik yang baik dalam mengubah data menjadi untaian kata yang tidak dapat dipahami oleh orang lain. Dalam dunia komputer, alat bantu untuk melakukan ini disebut dengan kriptografi (Pandi, 2019).

Kriptografi merupakan ilmu matematika yang juga bersangkutan dengan bidang keamanan informasi seperti integritas entitas, dan integritas data. Kriptografi menggunakan berbagai metode untuk melindungi data. Mengirim dan menyimpan data dengan sarana elektronik atau komputer membutuhkan proses yang menjamin keamanan dan integritas data. Untuk memastikan keamanan informasi, informasi harus diperlakukan secara rahasia baik saat diterima maupun saat dikirimkan (Maryanti & Rakhman, 2018).

Kriptografi terdiri dari enkripsi dan deskripsi. Enkripsi mengubah informasi (data) menjadi bentuk yang tidak dapat dimengerti dengan menggunakan algoritma tertentu saat pengiriman. Deskripsi adalah proses sebaliknya, mengembalikan bentuk yang tidak dapat dimengerti menjadi informasi asli yang dapat dimengerti (Muharram, 2018). Algoritma enkripsi memberikan output yang berbeda dengan ketentuan pada kunci yang dipergunakan. Mengubah kunci pada saat enkripsi akan mengubah hasil dari algoritma enkripsi. Kemudian ciperteks dikirimkan oleh pengirim. Selanjutnya adalah proses deskripsi, adalah proses mengembalikan teks acak ke bentuk aslinya dengan menggunakan kunci yang sama seperti awal proses enkripsi. Dalam proses ini dilakukan oleh penerima, sehingga teks dikembalikan menjadi informasi yang dipahami oleh penerima (Manaor et al., 2017).

Saat ini banyak algoritma kriptografi yang digunakan untuk menjaga keamanan data, seperti *MD2, MD4, LOKI, RSA, GOST, Blowfish, Vigenere*, dll. Masing-masing metode kriptografi ini memiliki kekuatan dan kelemahan. Selain algoritma kriptografi diatas, masih ada algoritma kriptografi lainnya, disini penulis mencoba menggunakan algoritma *Hill Cipher*. *Hill Cipher* adalah salah satu cipher *clasic* yang sangat susah untuk dipecahkan oleh *cryptanalyst* jika mereka hanya mengetahui file cipherteks. Karena *Hill Cipher* tidak mengganti huruf *plaintext* dengan huruf yang sama dengan huruf *ciphertext* lainnya karena menggunakan perkalian matriks berdasarkan enkripsi dan deskripsi (Gunawan et al., 2018).

Hill Cipher adalah algoritma kriptografi yang menggunakan matriks sebagai kunci untuk melakukan enkripsi dan dekripsi, serta menggunakan aritmetika modulo. Dalam *Hill Cipher,* setiap karakter pada plainteks dan ciperteks dikonversi menjadi angka (Hidayat & Alawiyah, 2013).

Penelitian sebelumnya dilakukan oleh (Gusti Awang Aritonang et al., 2019) dalam penelitiannya berjudul "Implementasi Kriptografi Dengan Metode *Hill Cipher* Untuk Keamanan Data Gaji Karyawan Kasir Di PT. Matahari Department Store Plaza Medan Fair". Dari hasil penelitian tersebut diketahui bahwa Metode *Hill Cipher* dapat di implementasikan untuk data gaji kariawan yang bertujuan untuk menjaga privasi data menjadi lebih aman sehingga data tidak jatuh ke pihak yang tidak bertanggung berwenang.

Penelitian lain yang berjudul "*Optimization of Hill Cipher Method for Encryption and Decryption of Prescription Drugs at Puskesmas Twano Jayapura City*" yang dilakukan oleh (Elvis Pawan et al., 2021). Dari penelitian tersebut diketahui bahwa algoritma *Hill Cipher* dapat digunakan dengan baik pada keamanan data keamanan data peresepan obat di puskesmas Twano kota Jawapura.

Penelitian lain yang berjudul "Implementasi dan Perancangan Aplikasi Kriptografi Algoritma *Hill Cipher* dalam Deskripsi Enkripsi Data Keuangan Nasabah Bank Sampoerna Menggunakan Kode ASCII" yang di lakukan oleh (Warni Hasibuan & Budhiati Veronica, 2022). Penelitian ini menunjukkan bahwa Algoritma *Hill Cipher* merupakan salah satu algoritma kriptografi klasik yang sangat kuat dalam hal keamanan dan efektif dalam melawan serangan *ciphertext-*

only. Hal ini terjadi karena Hill Cipher menggunakan operasi perkalian matriks dalam proses enkripsi dan deskripsi.

Dengan Kesimpulan penelitian sebelumnya, algoritma *Hill Cipher* digunakan untuk meningkatkan tingkat keamanan dan privasi data. Dengan latar belakang yang telah dipaparkan maka penulis tertarik untuk mengimplementasikan proses enkripsi dan deskripsi algoritma *Hill Cipher* dalam rekam medis, dengan judul "Impementasi Algoritma *Hill Cipher* Untuk Kemanan Data Rekam Medis di Puskesmas Pematang Raya". Dimana di harapkan data - data rekam medis dapat dikelola dengan lebih mudah dan ditransmisikan dengan lebih aman, sehingga dapat mengurangi risiko kehilangan atau pencurian data.

1.2 Identifikasi Masalah

Dengan latar belakang yang sudah di jelaskan di atas, diangkatlah identifikasi masalah pada penelitian ini supaya menjadi lebih jelas maka perlu di identifikasi. Adapun identifikasi dalam penelitian ini adalah :

1. Kurangnya sistem keamanan yang diterapkan pada data rekam medis, sehingga adanya kemungkinan data tersebar atau dipergunakan tidak semestinya oleh orang yang tidak berwenang.
2. Diperlukan sistem untuk memudahkan dalam mencari data rekam medis dan mentransmisikan data dengan lebih efisien dan aman.

1.3 Rumusan Masalah

Dari penjelasan latar belakang yang telah dijelaskan di atas, dapat dirumuskan suatu pokok permasalahan yang di dapat dari penelitian ini yaitu ;

1. Bagaimana cara mengimplementasikan algoritma *Hill Cipher* untuk keamanan rekam medis?
2. Bagaimana melakukan proses enkripsi dan deskripsi dengan algoritma *Hill Cipher*?
3. Bagaimana meningkatkan sistem keamanan pada data rekam medis?

1.4 Batasan Masalah

Dalam penelitian ini, peneliti mempertimbangkan keterbatasan kemampuan dan luasnya permasalahan dengan batasan sebagai berikut :

1. Kunci matriks yang digunakan pada algoritma *Hill Cipher* menggunakan matriks 2x2.
2. Sistem dengan algoritma *Hill Cipher* ini hanya untuk petugas puskesmas dalam mengelola data rekam medis dan petugas instansi lain yang ditujukan.
3. Perancangan sistem menggunakan bahasa pemrograman PHP dan MySQL digunakan sebagai Database Server.
4. Inputan data pada sistem berupa teks.

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah disebutkan, adapun tujuan penelitian ini adalah;

1. Mengimplementasikan algoritma *Hill Cipher* untuk kemanan rekam medis.
2. Mengetahui proses enkripsi dan deskirpsi pada algoritma *Hill Cipher.*
3. Meningkatkan sistem keamanan pada data rekam medis dengan menggunakan algortima *Hill Cipher.*

1.6 Manfaat Penelitian

1. Bagi Peneliti

   Menambah pengetahuan tentang enkripsi dan deskripsi kriptografi algoritma *Hill Cipher*.
2. Bagi Instansi

   Dapat mengamankan data penting pada rekam medis pasien dan mencegah terjadinya kebocoran informasi pada rekam medis pasien sehingga tidak terjadi penyalahgunaan data. Manfaat lainnya mempermudah petugas instansi untuk mencari data rekam medis dan transmisi data dengan lebih efisien dan aman.