Jurnal Hasi Penelitian Dan Pengkajian Ilmiah Eksakta
Vol. 2 No. 1 Januari 2023 Hal. 12-16
DOI : https://doi.org/10.47233/jppie.v2i1.661
ISSN : **2809-9532**

Implementasi Keamanan Database menggunakan Metode Kriptografi pada Puskesmas Karang Rejo Poli TB Paru

Fahreza Shiddiq Siregar[1)], Muhammad Hafi Isfahan Isnan[2)], Muhammad Rizky Ramadhan[3)], Ali Ikhwan[4)].

[1]Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara, Tanjung Morawa
email: fahrezashiddiqsiregar@gmail.com
[2]Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara, Medan
email: hafiisfahan21@gmail.com
[3]Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara, Medan
email: rrizkyr994@gmail.com
[4]Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara, Medan
email: ali_ikhwan@uinsu.ac.id

Abstract
The development of information technology is currently growing rapidly, especially in internet technology. A lot of data has been sent and received from internet traffic. An agency or institution must have personal data that certain parties might be able to break into. Because there have been many cases that have resulted in the loss of our personal data. Therefore many companies use security methods to protect company data and employee data. For this reason, encryption is needed as a method of securing data. At the Karang Rejo Health Center there is still a lack of security for employee data so it is vulnerable to data theft. With this encrypted data security, the Karang Rejo Health Center can minimize leaks or breaches of employee or employee data. Because with this encryption security it can protect important documents including personal data. This study uses a qualitative method in which the method aims to create an application that can help to encrypt the Karang Rejo Health Center employee database. The research results focus on the results of application design for Encryption and Decryption. The application has been tested through a prototype. So that the application can be used to assist in the security of employee data at the Karangrejo Health Center.
Keywords: *Security, Public Health Center, Encryption, Database, Data*

Abstrak
Perkembangan teknologi informasi saat ini berkembang dengan cepat terutama dalam teknologi internet. Banyak data yang telah dikirim dan diterima dari lalu lintas internet. Pada sebuah instansi atau lemabaga pasti memiliki data-data pribadi yang mungkin saja bisa dibobol oleh pihak tertentu. Karena sudah banyak kasus yang mengakibatkan hilangnya data-data pribadi kita. Maka dari itu banyak perusahaan yang menggunakan metode keamanan untuk melindungi data perusahaan dan data karyawannya. Untuk itu diperlukannya Enkripsi sebagai metode mengamankan data. Pada Puskesmas Karang Rejo masih kurangnya keamanan pada data karyawan sehingga rentan terhadap pencurian data. Dengan adanya keamanan data enkripsi ini, Puskesmas Karang Rejo dapat meminimalisir kebocoran atau kebobolan data karyawan atau pegawainya.Karena dengan adanya pengamanan enkripsi ini bisa melindungi dokumen penting yang termasuk data pribadi. Penelitian ini menggunakan metode Kualitatif yang dimana metode tersebut bertujuan untuk membuat sebuah aplikasi yang dapat membantu untuk melakukan Enkripsi pada database karyawan Puskesmas Karang Rejo. Hasil penelitian berfokus pada hasil rancangan aplikasi untuk Enkripsi dan Dekripsi. Aplikasi sudah diuji coba melalui prototype. Sehingga aplikasi dapat digunakan dalam membantu keamanan data karyawan Puskesmas Karang rejo.
Kata kunci: Keamanan, Puskesmas, Enkripsi, Database, Data

PENDAHULUAN

Puskesmas Karang Rejo merupakan tempat pelayanan kesehatan masyarakat yang terletak di Stabat, Medan. Puskesmas ini meliputi dari beberapa bagian poliklinik kesehatan, salah satunya adalah poli TB Paru. Terdapat beberapa data pribadi yang terdiri dari data perawat pada TB Paru. Pada Puskesmas Karang Rejo pengamanan data perawat atau pegawai hanya disimpan dalam file biasa tanpa adanya pengamanan, sehingga memungkinkan terjadinya data diri perawat atau pegawai yang bekerja di Puskesmas Karang Rejo terutama pada Poli TB Paru. Maka dari itu diperlukan sebuah pengamanan Enkripsi untuk

Jurnal Hasi Penelitian Dan Pengkajian Ilmiah Eksakta
Vol. 2 No. 1 Januari 2023 Hal. 12-16
DOI : https://doi.org/10.47233/jppie.v2i1.661
ISSN : **2809-9532**

mengurangi kebocoran data pribadi perawat atau pegawai tersebut.

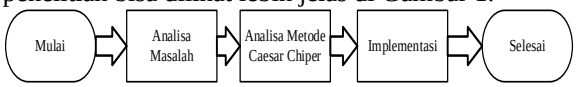
Salah satu cara untuk meningkatkan keamanan sebuah data atau file adalah dengan menggunakan metode kriptografi [1]. Kriptografi adalah alat keamanan yang digunakan untuk menyembunyikan pesan. Kriptografi sudah digunakan di semua bidang keamanan [2]-[3]. Kriptografi adalah salah satu bidang studi yang paling utama akhir-akhir ini karena sangat penting untuk menjaga kerahasiaan informasi yang didistribusikan melalui jaringan [4]. Ada dua konsep utama dalam kriptografi, yaitu enkripsi dan dekripsi. Enkripsi adalah proses di mana data/informasi yang dikirim diubah menjadi bentuk yang hampir tidak dapat dikenali sebagai informasi asli dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi, yaitu konversi bentuk tersembunyi menjadi data asli [5]-[6]. Kriptografi banyak digunakan untuk menjaga aspek keamanan informasi [7]. Berbagai organisasi, perusahaan atau pihak telah menggunakan teknologi database untuk menyimpan dan mengelola informasi organisasi atau perusahaan mereka. Memerlukan metode enkripsi yaitu ilmu pengetahuan dan seni untuk melindungi file [8]. Untuk mencegah agar informasi rahasia tidak dibagikan kepada pihak yang tidak berwenang, kriptografi digunakan sebagai kunci agar pihak-pihak tersebut tidak mengetahui informasi tersebut. Seiring banyaknya data yang dibagikan dan terhubung di dunia maya, keamanan data semakin tidak terjamin [9]. Algoritma kriptografi dibagi menjadi dua jenis, yaitu algoritma kriptografi klasik dan algoritma kriptografi modern [10]. Kriptografi menjaga kerahasiaan informasi dari orang yang tidak berwenang. Steganografi adalah seni atau ilmu menyembunyikan pesan sehingga hanya pengirim dan penerima saja yang mengetahui isi pesan tersebut, sedangkan orang lain tidak mengetahui pesan yang disembunyikan tersebut [11]. Mata kuliah Keamanan Aset Informasi merupakan salah satu mata kuliah yang diajarkan pada jurusan Sistem Informasi dimana kriptografi diajarkan pada mata kuliah keamanan aset informasi ini [12].

Algoritma Caesar adalah metode enkripsi pertama yang digunakan oleh Julius Caesar dan tentaranya selama Perang Gallic pada 50 SM. Cara kerja algoritme ini adalah semua karakter alfabet ditransfer ke jumlah kunci karakter [13]. Caesar menyandikan data ini dengan mengganti setiap huruf data dengan tiga huruf setelah data asli dalam urutan abjad. Algoritma yang digunakan dalam Caesar cipher sangat sederhana dan mudah dipecahkan, sehingga Caesar cipher dianggap kurang cocok untuk menyimpan informasi rahasia [14]. Aplikasi yang dibuat menggunakan aspek Aplikasi yang mengimplementasikan algoritma Advanced Encryption Standard (AES), yang digunakan sebagai algoritma enkripsi default untuk Caesar Chiper [15]. Untuk melindungi data teks dari ancaman pencurian, dibutuhkan sebuah sistem yang dapat mengenkripsi dan dekripsi sebuah data teks [16]. yang mana algoritma Caesar Chiper digunakan untuk enkripsi dan dekripsi kunci yang telah dimasukkan [17].Caesar mungkin bukan penemu asli dari apa yang sekarang kita sebut sandi Caesar, tapi dia membuatnya populer [18]. Sandi Caesar adalah salah satu algoritme tertua dan merupakan jenis sandi substitusi yang membentuk sandi. Kelemahan dari cipher Caesar adalah kita biasanya mendapatkan kunci dengan sangat mudah sehingga rentan terhadap brute force cracking [19]. Karena kriptografi memiliki banyak algoritma, hanya Caesar Chiper dan Vigenere Chiper yang digunakan dalam penelitian ini. [20].

Adapun tujuan penelitian ini dilakukan untuk membuat sebuah aplikasi keamanan atau enkripsi data perawat atau pegawai Puskesmas Karang Rejo terutama pada poli TB Paru. Aplikasi ini nantinya akan menggunakan metode Caesar Cipher. Dengan adanya aplikasi enkripsi maka akan mengurangi resiko kebocoran data perawat atau pegawai.

METODE PENELITIAN

Pada penelitian kali ini kami menggunakan metode Caesar Chiper sebagai metode penilitan. Urutan penelitian bisa dilihat lebih jelas di Gambar 1.

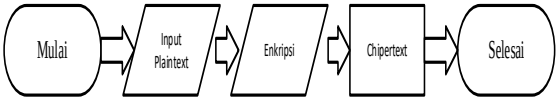


Gambar. 1

2.1 Analisa Masalah

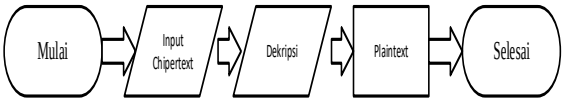
Pada puskesmas karang sari rejo masih menggunakan sistem yang tertinggal hingga beresiko terjadinya pembobolan data dan tindakan kejahatan siber. Data karyawan yang tersimpan didalam database tidak menggunakan metode enkripsi apapun sehingga rawan dicuri.

2.2 Analisa Metode Caesar Chiper



Gambar. 2

Gambar diatas merupakan proses enkripsi dimulai dari memasukkan plaintext kemudian diproses enkripsi. Setelah proses enkripsi maka hasil akan keluar sebagai chipertext



Gambar. 3

Jurnal Hasi Penelitian Dan Pengkajian Ilmiah Eksakta
Vol. 2 No. 1 Januari 2023 Hal. 12-16
DOI : https://doi.org/10.47233/jppie.v2i1.661
ISSN : **2809-9532**

Gambar diatas merupakan proses dekripsi. Proses hampir sama dengan enkripsi yang membedakan adalah memasukkan chipertext terlebih dahulu lalu diproses menjadi plaintext

Rumus untuk mengenkripsi menggunakan metode caesar chiper adalah sebagai berikut :

$$C = P + K \; Mod \; N$$

Keterangan :
C = cipher text
P = plain text
K = kunci
Mod = modular
N = jumlah karakter

Dan rumus untuk dekripsi adalah sebagai berikut :

$$P = C - K \; Mod \; N$$

Keterangan :
C = cipher text
P = plain text
K = kunci
Mod = modular
N = jumlah karakter

2.3 Implementasi

Setelah menentukan metode dilanjutkan dengan merancang sebuah program. Disini penulis menggunakan bahasa pemprograman PHP sebagai media untuk membuat enkripsi dan dekripsi.

HASIL DAN PEMBAHASAN

3.1 Analisa masalah

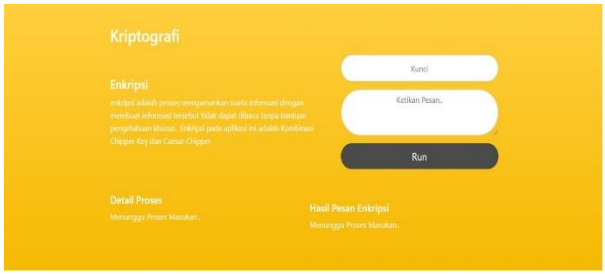
Ditemukan bahwa semua data karyawan pada Puskesmas Karang Sari Rejo Belum menggunakan teknik enkripsi apapun sehingga rentang terhadap pencurian data. Oleh karena itu penulis membuat sebuah aplikasi berbasis web untuk membantu mengenkripsi data-data karyawan tersebut Pembahasan adalah penjelasan dasar, hubungan dan generalisasi yang ditunjukkan oleh hasil. Uraiannya menjawab pertanyaan penelitian. Jika ada hasil yang meragukan maka tampilkan secara objektif.

3.2 Analisa Metode Caesar Chiper

Metode Caesar Chiper merupakan salah satu teknik enkripsi yang sudah tua. Walaupun terbilang tua tapi metode ini masih bisa digunakan untuk sekarang. Pada penggunaan kali ini metode Caesar Chiper akan diimplementasikan kepada bahasa pemprograman PHP yang dimana aplikasi yang akan dibuat akan berbasis website

3.3 Implementasi

Berdasarkan hasil analisis yang dilakukan, maka dihasilkan sebuah aplikasi enkripsi data perawat atau pegawai dengan keamanan data menggunakan metode kriptografi Caesar Cipher berbasis web sehingga dapat dijadikan media untuk mengamankan kerahasiaan data dari pihak-pihak yang tidak bertanggung jawab. 3.3.1 Tampilan Utama Aplikasi



Gambar 4. Tampilan utama

Pada tampilan ini dijelaskan terlebih dahulu tentang apa itu enkripsi. Lalu terdapat sebuah text box untuk memasukkan kata kunci yang ingin di enkripsi. Pertama isi terdahulu kolom kunci, setelah itu isi kolom pesan lalu klik run untuk menuju ke halaman selanjutnya.

3.3.2 Tampilan Hasil Enkripsi

Gambar 5. Tampilan hasil enkripsi

Tampilan diatas merupakan tampilan dari hasil enkripsi data. Dimana pada kolom teks awal diisi anggapinipassword maka dienkripsi dan hasilnya menjadi “DQJJDSLQLSDDVZRUG”.

3.3.3 Tampilan Halaman Dekripsi

Gambar 6. Tampilan halaman dekripsi

Sama dengan halaman awal Enkripsi, dihalaman ini juga dijelaskan pengertian tentang apa itu Dekripsi. Jika ingin menDekripsi pesan yang telah diEnkripsi maka isi kolom kunci sama dengan kolom

Jurnal Hasi Penelitian Dan Pengkajian Ilmiah Eksakta
Vol. 2 No. 1 Januari 2023 Hal. 12-16
DOI : https://doi.org/10.47233/jppie.v2i1.661
ISSN : **2809-9532**

diEnkripsi tadi, dan kolom pesan diisi dengan hasil dari Enkripsi tadi.

3.3.4 Tampilan Database Sebelum di enkripsi

nama	password
Faridah F. Hutasoit	idahutasoit
Normala Dewi, AMK	malanurrrdewi
Ade Ardian, S.Kep, Ners	adeardianade
Nurhidayani Yus, AMK	yushidayani

Gambar 7. Tampilan database sebelum Enkripsi

Disini terlihat password untuk data perawat atau pegawai masih terlihat dan belum diEnkripsi sehingga memungkinkan mudah untuk dibobol.

3.3.5 Tampilan Database Setelah di enkripsi

nama	password
Faridah F. Hutasoit	LGDKXWDVRLW
Normala Dewi, AMK	PDODQXUUUGHZL
Ade Ardian, S.Kep, Ners	DGHDUGLDQDGH
Nurhidayani Yus, AMK	BXVKLGDBDQL

Gambar 9. Tampilan database setelah dienkripsi

Pada tampilan ini password data diri perawat dan pegawai terlihat sudah terenkripsi menjadi huruf yang sudah ditentukan dengan rumus Caesar Cipher tadi, sehingga password lebih susah untuk dibobol.

SIMPULAN

Cipher Caesar adalah jenis cipher substitusi di mana setiap huruf dalam teks biasa diganti dengan huruf pada beberapa posisi tetap di bawah alfabet. Teknik ini juga dikenal sebagai kode tunggal. Berdasarkan penelitian, implementasi dan pengujian, maka dapat diambil kesimpulan sebagai berikut :

1. Caesar chiper merupakan enkripsi yang mudah sehingga dapat dideskripsi sendiri oleh orang lain.

2. Keefektifan Caesar Cipher sangat kurang disarankan karena Caesar sendiri sering kehilangan datanya.

3. Caesar chiper mungkin bisa menjadi teknik enkripsi untuk keamanan sebuah data jika metode tersebut digabungkan dengan metode terbaru

4. Keamanan data karyawan pada Puskesmas Karang Rejo disarankan untuk menggunakan enkrpsi yang lebih modren untuk menghindari pembobolan data pada database tersebut**.**

UCAPAN TERIMAKASIH

Terimakasih kami ucapkan kepada pihak ataupun instansi yang membantu kami dalam melakukan penelitian ataupun memberikan izin.

DAFTAR PUSTAKA

[1] R. Siringoringo, "Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File," KAKIFIKOM Kumpul. Artik. Karya Ilm. Fak. core.ac.uk, 2020. [Online]. Available: https://core.ac.uk/download/pdf/327176749.pdf

[2] M. Zulham, H. Kurniawan, and ..., "Perancangan Aplikasi Keamanan Data Email Menggunakan Algoritma Enkripsi RC6 Berbasis Android," Semin. Nas. …, 2017, [Online]. Available: http://e-journal.potensi-utama.ac.id/ojs/index.php/SNIf/article/view/221

[3] D. Rachmawati, S. M. Hardi, and ..., "Combination of columnar transposition cipher caesar cipher and lempel ziv welch algorithm in image security and compression," J. Phys. …, 2019, doi: 10.1088/1742-6596/1339/1/012007.

[4] D. Gautam, C. Agrawal, P. Sharma, and ..., "An enhanced Cipher technique using Vigenere and modified Caesar cipher," … Trends …, 2018, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8553910/

[5] N. Azis, "Perancangan aplikasi enkripsi dekripsi menggunakan metode caesar chiper dan operasi xor," ikraith-informatika. journals.upi-yai.ac.id, 2018. [Online]. Available: http://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/download/214/113

[6] F. Muharram, H. Aziz, and A. R. Manga, "Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)," Pros. SAKTI (Seminar …, 2018, [Online]. Available: http://e-journals.unmul.ac.id/index.php/SAKTI/article/view/1844

[7] R. Amalia, "Implementasi Algoritma AES dan Algoritma XOR pada Aplikasi Enkripsi dan Dekripsi Teks Berbasis Android," Fakt. Exacta, 2018, [Online]. Available: https://journal.lppmunindra.ac.id/index.php/Faktor_Exacta/article/view/2878

[8] S. Retno and N. Hasdyna, "Analisis Kinerja Algoritma Honey Encryption dan Algoritma Blowfish Pada Proses Enkripsi Dan Dekripsi," TECHSI-Jurnal Tek. Inform.,

Jurnal Hasi Penelitian Dan Pengkajian Ilmiah Eksakta
Vol. 2 No. 1 Januari 2023 Hal. 12-16
DOI : https://doi.org/10.47233/jppie.v2i1.661
ISSN : **2809-9532**

2018, [Online]. Available: https://ojs.unimal.ac.id/techsi/article/view/858

[9] N. S. B. Sembiring, "Perancangan Aplikasi Kriptografi Dengan Metode Modifikasi Caesar Cipher Yang Diperkuat Dengan Vernam Cipher Untuk Keamanan Teks," J. Sist. Inf. dan Teknol. Inf., 2018, [Online]. Available: https://www.neliti.com/publications/288652/perancangan-aplikasi-kriptografi-dengan-metode-modifikasi-caesar-cipher-yang-dip

[10] Y. Yusfrizal, "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android," JTIK (Jurnal Tek. Inform. Kaputama), 2019, [Online]. Available: http://jurnal.kaputama.ac.id/index.php/JTIK/article/view/173

[11] S. Agustini and M. Kurniawan, "Peningkatan Keamanan Teks Menggunakan Kriptografi Dan Steganografi," SCAN-Jurnal Teknol. Inf. …, 2019, [Online]. Available: http://www.ejournal.upnjatim.ac.id/index.php/scan/article/view/1685

[12] J. Rahmadoni, "Perancangan Simulasi Pembelajaran Kriptografi Klasik Menggunakan Metode Web Based Learning," INTECOMS J. Inf. Technol. …, 2018, [Online]. Available: https://journal.ipm2kpe.or.id/index.php/INTECOM/article/view/160

[13] M. F. A. Sinaga, "… ALGORITMA ROT13 DAN ALGORITMA CAESAR CHIPER DALAM PENYANDIAN TEKSIMPLEMENTASI ALGORITMA ROT13 DAN ALGORITMA CAESAR CHIPER …," Pelita Inform. Inf. …, 2020, [Online]. Available: http://stmik-budidarma.ac.id/ejurnal/index.php/pelita/article/view/255

[14] I. Darmayanti, D. N. Astrida, and D. Ariyus, "Penerapan Keamanan Pesan Teks Menggunakan Modifikasi Algoritma Caisar Chiper Kedalam Bentuk Sandi Morse," J. Ilm. IT CIDA, 2019, [Online]. Available: http://journal.amikomsolo.ac.id/index.php/itcida/article/view/78

[15] M. A. J. Plaza and M. Ishak, "METODE KRIPTOGRAFI CAESAR CHIPER PADA APLIKASI CHATTING BERBASIS LOCAL AREA NETWORK (STUDI KASUS STMIK SURYA INTAN KOTABUMI)," J. …, 2021, [Online]. Available: http://jurnal.stmiksuryaintankotabumi.ac.id/index.php/STMIK/article/view/17

[16] J. HUTABARAT, IMPLEMENTASI ALGORITMA ROT13 DAN CAESAR CHIPER DALAM PENYANDIAN TEKS BERBASIS WEB. repository.potensi-utama.ac.id, 2018. [Online]. Available: http://repository.potensi-utama.ac.id/jspui/handle/123456789/3242

[17] I. T. Y. Hasan, "IMPLEMENTASI ALGORITMA CAESAR CHIPER UNTUK ENKRIPSI EXTERNAL KEY ALGORITMA DES DALAM PENGAMANAN FILE WINZIP," academia.edu. [Online]. Available: https://www.academia.edu/download/68315594/Prosiding_SNITI_Tahun_2016_Iskandar_dan_yasir.pdf

[18] J. Holden, The mathematics of secrets: cryptography from caesar ciphers to digital encryption. books.google.com, 2018. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=N3SYDwAAQBAJ&oi=fnd&pg=PA7&dq=caesar+cipher&ots=TMDdBZQ8Fl&sig=hoTJfnuDHuQDnFEeYDjmEfkAV8k

[19] I. Gunawan, H. S. Tambunan, E. Irawan, and ..., "Combination of Caesar Cipher Algorithm and Rivest Shamir Adleman Algorithm for Securing Document Files and Text Messages," J. Phys. …, 2019, doi: 10.1088/1742-6596/1255/1/012077.

[1] [20] M. Syaifuddin, J. Hutagalung, and ..., "E-Learning Dalam Pengembangan Pembelajaran Kriptografi," … (Jurnal Teknol. dan …, 2021, [Online]. Available: https://jurnal.stmikroyal.ac.id/index.php/jurteksi/article/view/914