ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.2 No.1 Tahun 2023
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-2 2023
Fakultas Teknik, Universitas Pelita Bangsa, Februari 2023

Sistem Login Menggunakan Caesar Chipper Berbasis Web
Login System Using Web-Based Caesar Chipper

Febri Aditya[1], Mohammad Rizky[2], Revano Arya Saputra[3], Fikri Abei[4]
[1,2,3,4]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1]febri_aditiya@mhs.pelitabangsa.ac.id, [2]mohammadrizky@mhs.pelitabangsa.ac.id

Abstract

Security in protection when entering the web or logging in is something that must be considered, because the more developed the times, the more sophisticated the technology. So that security in the login system and accessing data on a website must be a more concern. Therefore, a method or algorithm is needed that can protect users from hacker attacks. The algorithm used in encrypting is a Caesar chipper, as a cryptographic technique for encoding usernames and passwords so that usernames and passwords look difficult to read and solve. After the username and password have been encrypted, this algorithm will insert numbers and secret letters. The conclusion of this study is that the application of the Caesar chipper Algorithm can be used as a login system security technique well even though this algorithm is relatively simple but the level of security is quite good in protecting users or users to be safer from irresponsible eavesdroppers and hackers or efforts in protecting data owned.

Keywords: *Caesar chipper, algorithm*

Abstrak

Keamanan dalam perlindungan saat masuk web atau login merupakan hal yang harus diperhatikan, dikarenakan semakin berkembangnya zaman maka semakin canggih pula teknologi. Sehingga keamanan dalam sistem login maupun mengakses data dalam sebuah website harus menjadi perhatian lebih. Oleh sebab itu dibutuhkan suatu metode atau algoritma yang dapat melindungi para pengguna dari serangan peretas. Adapun Algoritma yang digunakan dalam pengenkripsian yaitu Caesar chipper, sebagai Teknik kriptografi pengkodean username dan password agar username dan password yang terlihat sulit dibaca dan dipecahkan. Setelah username dan password yang telah dienkripsi maka algoritma ini akan menyisipkan angka dan huruf rahasia. Kesimpulan dari penelitian ini adalah bahwa penerapan Algoritma Caesar chipper bisa dijadikan Teknik pengamanan system login dengan baik walaupun Algoritma ini tergolong sederhana namun tingkat keamanan nya cukup baik dalam melindungi para user atau pengguna agar lebih aman dari para penyadap dan peretas yang tidak bertanggung jawab maupun mejadi upaya dalam perlindungan data data yang di miliki.

Kata kunci: Keamanan, Kriptografi, Caesar chipper.

Pendahuluan

Masalah keamanan dan kerahasiaan data merupakan aspek penting dari sistem informasi. Ketika datang ke masalah keamanan terkait saat menggunakan komputer, sulit membedakannya dengan enkripsi penyedia layanan keamanan termasuk keamanan untuk melindungi kata sandi. Data kata sandi anda sendiri harus dirahasiakan atau di lindungi. Jangan sampai data kata sandi yang ada, jatuh ke tangan ke orang orang yang tidak bertanggung jawab.

Dalam aplikasi web dibutuhkan mekanisme yang dapat melindungi data dari pengguna yang tidak berhak dan tidak bertanggung jawab. Mekanisme ini dapat diimplementasikan dalam bentuk sebuah proses login yang biasa nya terdiri dari tiga tahapan yakni identifikasi, otentifikasi dan autoritasi.

Seringkali banyak layanan online yang membutuhkan izin masuk (login) seperti sosial media, izin akses server web, atau akun email. Pengguna harus lebih hati hati terutama ketika akun tersebut sangat rahasia dan berharga karena kita tidak ingin orang asing mengakses akun kita tanpa izin dan mengubah isi didalam nya. Untuk menjaga agar password atau kata sandi tidak mudah dibaca oleh sniffer atau pengendus di perlukan proses pengamanan dengan melakukan enkripsi di bagian login, regist, serta nama pengguna (user) sebelum

data di simpan ke dalam database sistem agar tidak dapat dibaca oleh orang yang tidak berhak. Maka dari itu penulis akan membuat pengamanan data password yang tersimpan di database, salah satunya dnegan menggunakan algortima caesar chipper.

Pengaman data merupakan salah satu aspek untuk menyelamatkan data-data dari kemungkinan terjadinya pencurian dan pengubahan data oleh pihak yang tidak dikenal. Peningkatan kerahasian data dari waktu ke waktu mengalami banyak perubahan, di antaranya dengan menggunakan methode kriptografi. Algoritma penyandian yang dikenal dengan kriptografi telah mencakup aspek kehidupan manusia saat ini. Begitu pentingnya kriptografi, saat berbicara tentang keamanan data, orang tidak bisa memisahkannya dengan kriptografi

Basis data adalah sekumpulan informasi yang disimpan didalam komputer secara sistematik yang dapat digunakan melalui sebuah program komputer tertentu untuk menjalankannya. Untuk menjaga keamanan dan kerahasiaan data tersebut diperlukan beberapa pengamanan agar data tidak dapat dimengerti oleh sembarang orang, kecuali oleh penerima yang berhak. Beberapa cara untuk menangani masalah keamanan ini salah satunya adalah teknik penyandian data yang dikenal dengan ilmu kriptografi.

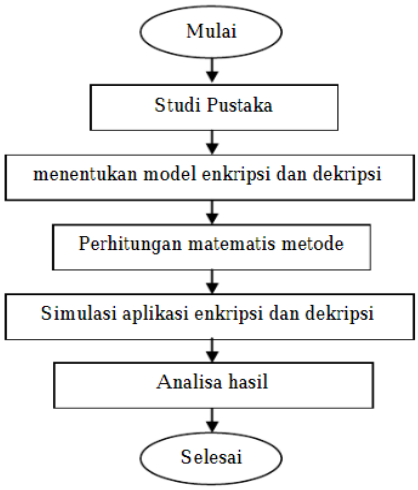
Dalam ilmu komputer terdapat beberapa algoritma yang dapat digunakan untuk mengamankan sebuah basis data misalnya MD5, Stream Cipher dan Caesar Cipher. Pada sistem ini algoritma kriptografi yang akan digunakan adalah algoritma Caesar Cipher.

Metode Penelitian

Jenis penelitian yang dilakukan adalah penelitian terapan, yaitu penelitian yang bertujuan untuk menyelesaikan masalah yang ada dengan menerapkan teori-teori yang mendasari penelitian yang dikaji dengan terlebih dahulu menyusun konsep-konsep yang berkaitan.

Pada bagian ini dijelaskan mengenai metode yang digunakan dalam penelitan ini. Metode penelitian ini meliputi penentuan model enkripsi, penyelesain algoritma enkripsi, pembuatan simulasi enkripsi dan Analisa hasil dari simulasi enkripsi.

Diagram alir perancangan simulasi pada penelitian ini secara lengkap dapat dilihat pada gambar 1 dibawah ini.

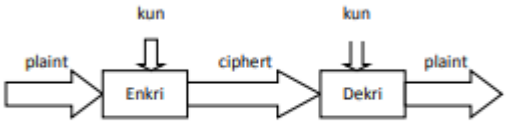


Gambar 1 diagram alir simulasi ekripsi

Pada gambar 1 di atas dapat diketahui penelitian ini dimulai dari studi pustaka, setelah menemukan permasalahan kemudian menentukan model enkripsi, langkah selanjutnya adalah menentukan perhitungan

Matematis. Setelah menentukan perhitungan matematis dibuat aplikasi simulasi sebagai uji coba dari perhitungan matematis tersebut dan Analisa apakah sudah benar atau belum.

Kriptografi modern selain memanfaatkan algoritma juga menggunakan kunci (key) untuk memecahkan masalah tersebut. Proses enkripsi dan dekripsi dilakukan dengan menggunakan kunci ini. Setiap anggota memiliki kuncinya masing-masing yang digunakan untuk proses enkripsi dan dekripsi yang akan dilakukannya. Dengan demikian ada sedikit perubahan yang harus dilakukan pada mekanisme yang digambarkan pada gambar 2.2 berikut ini. :

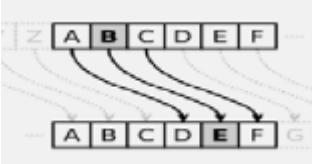


Gambar 2.2 Kriptografi berbasis kunci

Caesar Chiper adalah algoritma chiper substitution yang menggunakan pergeseran huruf dengan modul 26, modul 26 metode ini biasanya digunakan suatu informasi yang bersifat kusus. Pada Caesar cipher, tiap huruf disubtitusi dengan huruf ketiga berikutnya dari susunan alphabet yang sama. Dalam hal ini kuncinya adalah pergeseran berubah menjadi huruf tertentu yang lain.

Plaintext : KITA JUMPA BESUK PAGI

Chipertext : NLWD MXPSD EHVRN SDJL



Analisa Algoritma Caesar Cipher

Algoritma caesar cipher merupakan algoritma klasik yang memiliki langkah-langkah logis sebagai berikut :

1. Menghitung panjan karakter atau huruf yang dii nputkan dalam plaintext.
2. Tiap tiap huruf diubah menjadi kode ASCII menggunakan proses looping.
3. Untuk melakukan pergeseran atau proses enkripsi maka kode ASCII tersebut digeser dengan cara ditambah sebanyak pergeseran. Misal pergeseran 5 huruf maka kode ASCII dit ambah dengan 5.
4. Jika ditemukan spasi (ASCII=32), maka tidak usah dilakukan penambahan.
5. Hasil pergeseran bilangan ASCII dikembali kan lagi menjadi huruf atau karakter

Hasil dan Pembahasan

Hasil penelitian berupa uraian yang menunjukkan fakta/data terkait hasil penelitian. Komputer sebagai sarana penyimpanan data, informasi, dan dokumen penting dan rahasia. Peningkatan keamanan dengan menggunakan pemanfaatan teknologi dengan pemnfaatan ilmu kriftografi yakni Caesar Cipher. System enkripsi ini sudah digunakan sejak masa Romawi untuk mengenkripsi serta menyandikan pesan militer resmi dan rahasia. Enkripsi ini terbilang sederhana namun mampu membentuk cipher dengan penukaran karakter pada planteks menjadi tepat satu karakter pada chiperteks. Proses pada halaman login dengan system Caesar

cipher diguanakan untuk mengenkripsi password, sehingga melalui proses enkrip terlebih dahulu sebelum akhirnya dilakukan pencocokan data pada web. Perancangan antarmuka dimuat untuk membuat antarmuka yang mudah dimengerti dan pengguna mampu mengoperasikan web dengan interaktif. Hasil dapat disajikan dalam bentuk tabel, gambar, dan grafik. Semua tabel dan gambar harus dipanggil dalam paragraf. Untuk memperjelas uraian dapat menggunakan sub judul.

Kesimpulan

Berdasarkan hasil penelitian, maka penulis memperoleh beberapa kesimpulan, diantaranya adalah sebagai berikut :

1. Algoritma Caesar cipher dapat diimplementasikan kedalam koding.
2. Sistem yang dibangun mampu meningkatkan keamanan dan memberikan kemudahan bagi pengguna dengan menggunakan algoritma caesaar cipher.
3. Berdasarkan hasil penelitian dan pembahasan tentang Perancangan sistem Keamanan Password Login, dapat disimpulkan bahwa penelitian ini menghasilkan sebuah aplikasi keamanan enkripsi dengan metode caesar cipher. Aplikasi ini menggunakan algoritma caesar cipher sehingga keamanan informasi yang tersimpan dalam database dapat ditingkatkan dalam suatu sistem.

Saran

Diharapkan dalam penelitian lebih lanjut bisa menggunakan lebih banyak variabel-variabel lain yang mendukung sistem kemanan password login yang mendukung tingkat keamanan yang lebih maksimum agar data pengguna dapat lebih aman dari jangkauan hacker.

Daftar Rujukan

[1] C. Imama, "Penerapan Case Based Reasoning dengan Algoritma Nearest Neighbor Untuk Analisis Pemberian Kredit di Lembaga Pembiayaan," *J. Manaj. Inform.*, vol. 02, no. 01, pp. 11–21, 2013.

[2] Yoga Religia, Agung Nugroho, and Wahyu Hadikristanto, "Klasifikasi Analisis Perbandingan Algoritma Optimasi pada Random Forest untuk Klasifikasi Data Bank Marketing," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 1, pp. 187–192, Feb. 2021, doi: 10.29207/resti.v5i1.2813.

[3] A. Nugroho and Y. Religia, "Analisis Optimasi Algoritma Klasifikasi Naive Bayes menggunakan Genetic Algorithm dan Bagging," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 3, pp. 504–510, Jun. 2021, doi: 10.29207/resti.v5i3.3067.

[4] Nurani Dwi, 2018, Perancangan Aplikasi Email Menggunakan Algoritma Caesar Cipher dan Base64, JISKa (Jurnal Informatika Sunan Kalijaga), Vol.2, No.3.

[5] Syukron Akhmad, Noor Hasan, 2015, Perancangan Sistem Informasi Rawat Jalan Berbasis Web Pada Puskesmas Winong, Jurnal Bianglala Informatika, Vol.3, No.1.

[6] Zuli Faisal, Ari Irawan, 2014, Penerapan Kombinasi Sandi Caesar Dan Vigenere Untuk Pengamanan Data Pesan Pada Surat Elektronik, Studi Informatika: Jurnal Sistem Informasi , Vol.7, No.2.

[7] AnistasariFrisai Sinaga, Mesran, 2017, Implementas Algoritma ROT13 Dan Algoritma Caesar Chiper Dalam Penyandia Teks, Pelita Informatika Budi Darma, Vol.16, No.1.

[8] Desmon Harvei Hutahaean, 2012, Penerapan Computer Assisted Instruction Dalam Pembelajaran Pemahaman Algoritma Caesar Cipher, Pelita Informatika Budi Darma, Vol 1.

[9] Dhany, H. W., Izhari, F., Fahmi, H., Tulus, M., & Sutarman, M. (2017, October). Encryption and decryption using password based encryption, MD5, and DES. In International Conference on Public Policy, Social Computing and Development 2017 (ICOPOSDev 2017) (pp. 278-283). Atlantis Press.

[10] Fitria Aji, M, Hidayati, Anita. 2015. Pembangunan Aplikasi Pembanding Kriptografi Dengan Caesar Chiper dan Advance Encryption Standard (AES) Untuk File Teks. Politeknik Negeri Jakarta.

[11] Seftyanto, Donny, Apriliani, Mega, Haryanto, Tony. (2012). "Peran Algoritma Caesar Chiper dalam Membangun Karakter Akan Kesadaran Keamanan Informasi". SekolahTinggi Sandi Negara.

[12] Simamora, Fitri. 2017. Keamanan Data Base Pegawai PT. King Star Menggunakan Algoritma Caesar Chiper. Jurusan Sistem Informasi Sekolah Tinggi Teknik Harapan Medan.

[13] N. Azis, "Perancangan aplikasi enkripsi dekripsi menggunakan metode caesar chiper dan operasi xor," Ikraith-Informatika, vol. 2, no. 1, pp. 72–80, 2018.

[14] Anupama Mishra, "Enhancing Security of Caesar Cipher Using Different Method," International Journal of Research in Engineering and Technology, vol. 02, p. 332, september 2013.

[15] Apreja, A., Syarif, Z., & Ibrahim, A. (2017, November). Analisis Tingkat Keamanan Enkripsi Data Menggunakan Algoritma Base 64 Endcode. In Annual Research Seminar (ARS) (Vol. 3, No. 1, pp. 49-50).