https://e-journal.naureendigition.com/index.php/mj
Vol. 01. No. 02, 2023, Hal. 388–396
E-ISSN : 2964-7606

Implementasi Keamanan Data menggunakan Kriptografi Caesar Chiper

Desi Fitriani Ningrum[1], Muhlis Tahir[2], Wahyu Dwi Angelina[3], Eliza Permatasari[4], Fifi Rinazah Rofiq[5], Miftakhul Hidayati[6], Fatimatus Sahroh[7], Andi Setiawan[8]

desifitriani733@gmail.com muhlis.tahir@trunojoyo.ac.id angelinapuspita213@gmail.com elizapermatasari04@gmail.com fifirinazah@gmail.com miftakhulhidayati03@gmail.com f.zahro.14th9e@gmail.com 190631100020@student.trunojoyo.ac.id

Fakultas Ilmu Pendidikan, Universitas Trunojoyo Madura, Bangkalan

Abstrak *Keamanan data adalah salah satu isu terpenting yang harus diperhatikan oleh organisasi, bisnis, dan individu di era digital saat ini. Teknik yang sering digunakan untuk menjaga kerahasiaan data adalah kriptografi, yang mempelajari teknik keamanan data menggunakan algoritme tertentu. Salah satu algoritma enkripsi yang cukup sederhana dan umum digunakan adalah Caesar cipher yang merupakan salah satu algoritma enkripsi klasik yang sederhana namun cukup powerfull. Tujuan dari penelitian ini adalah mengimplementasikan keamanan informasi dengan Caesar Cipher dalam aplikasi sederhana. Hasil penelitian ini menunjukkan bahwa penerapan Caesar Cipher dapat meningkatkan keamanan data pada aplikasi komputer. Dengan Caesar Cipher, informasi sensitif seperti kata sandi atau informasi pribadi dapat dienkripsi sehingga hanya orang yang berwenang yang dapat mengaksesnya. Meskipun Caesar cipher cukup mudah untuk diimplementasikan, namun penggunaan algoritma ini masih memerlukan langkah-langkah keamanan tambahan untuk menghindari serangan brute force. Singkatnya, implementasi Caesar Cipher dapat menjadi pilihan untuk meningkatkan keamanan data pada aplikasi komputer. Walaupun Caesar Cipher memiliki beberapa kekurangan, namun penggunaannya tetap cukup penting untuk aplikasi sederhana yang membutuhkan tingkat keamanan yang memadai.*

Kata Kunci: *Kriptografi, Caesar chipper, keamanan, data*

Abstract *Data security is one of the most important issues that organizations, businesses, and individuals must consider in today's digital era. A technique commonly used to maintain data confidentiality is cryptography, which studies data security techniques using certain algorithms. One of the simple and commonly used encryption algorithms is the Caesar cipher, which is one of the classical encryption algorithms that is simple yet powerful. The purpose of this research is to implement information security with the Caesar Cipher in a simple application. The results of this research show that the implementation of the Caesar Cipher can improve data security in computer applications. With the Caesar Cipher, sensitive information such as passwords or personal information can be encrypted so that only authorized individuals can access it. Although the Caesar cipher is easy to implement, its use still requires additional security measures to avoid brute force attacks. In short, implementing the Caesar Cipher can be an option to improve data security in computer applications. Although the Caesar Cipher has some shortcomings, its use still important for simple applications that require adequate levels of security.*

Keywords: *Cryptography, Caesar Cipher, Security, Data*

Pendahuluan

Kerahasiaan suatu data atau keamanan sebuah informasi merupakan aspek penting dari berbagai informasi yang diterima maupun dikirim oleh pengguna. Perkembangan teknologi yang sangat cepat memberikan kemudahan bagi pengguna untuk memperoleh data atau informasi dengan sangat mudah. Apabila data tidak dilindungi maka orang lain dapat dengan mudah mengambil data atau informasi yang dimiliki seseorang. Kerahasian dan keutuhan sebuah pesan yang akan disampaikan menjadi satu aspek yang diharapkan setiap individu dalam melakukan kegiatan pertukaran informasi. Hal ini menjadi tuntutan yang sangat dibutuhkan dalam pekerjaan atau dalam berkehidupan sosial. Untuk menjaga kerahasiaan sebuah informasi, pesan teks di sandikan atau diubah bentuk aslinya dengan menggunakan kriptografi.

Kriptografi merupakan ilmu dan seni untuk menjaga pesan agar aman. Kripto berasal dari kata Crypto yang artinya rahasia dan graphy berarti tulisan sehingga kriptografi dapat diartikan tulisan yang tersembunyi. Dengan adanya tulisan yang tersembunyi ini maka orang- orang tidak mengetahui bagaimana tulisan tersebut disembunyikan dan tidak tahu bagaimana cara membaca maupun menterjemahkan tulisan tersebut. Teknik yang bisa dilakukan untuk melindungi kerahasiaan isi pesan yaitu dengan melakukan perubahan teks asli kebentuk yang lain atau sering disebut enkripsi. Pada kriptografi ada banyak metode yang bisa digunakan dalam penyandian pesan dengan tujuan pesan diubah bentuk artinya serumit mungkin. Pengelompokkan penggunaan kunci saat enkripsi dan deskripsi dibedakan menjadi dua algoritma, pertama pada saat enkripsi dan deskripsi menggunakan kode yang sama dan yang kedua, saat enkripsi dan deskripsi menggunakan kunci yang beda.

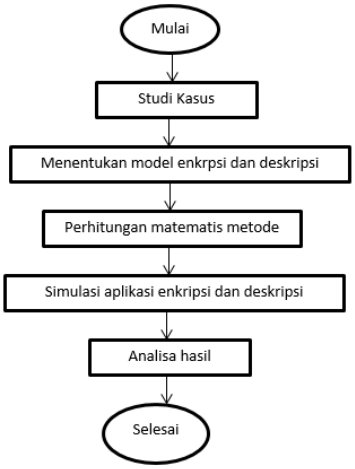
Pada pengamanan dalam kriptografi ini banyak metode atau algoritma yang dapat digunakan, seperti Caesar, Abjad Majemuk, DES, IDEA, RSA dan lain sebagainya.

Sedangkan pada penelitian ini menggunakan metode Caesar Chiper. Algoritma caesar cipher termasuk pada kriptografi klasik yang memiliki kunci simestris (hanya ada satu kunci) yang mana biasa digunakan dalam mengekripsi ataupun mendekripsi data dan informasi. Karena chiper merupakan kriptografi klasik maka proses enkripsi dan dekripsinya dilakukan dengan cara substitusi atau perpindahan. Caesar cipher juga dikenal sebagai penyandian yang paling sederahana dalam penanganan keamanan pesan. Menyandikan isi pesan dengan teknik subtitusi, dimana setiap karakter pada pesan asli akan digeser posisi masing-masing karaker sehingga menghasilkan bentuk lain yang disebut chiperteks.

Metode

Jenis Penelitian

Jenis penelitian yang digunakan adalah penelitian terapan, dimana mempunyai arti penelitian yang bertujuan untuk menyelesaikan masalah dengan menerapkan beberapa dasar teori penelitian yang dikaji tertlebih dahulu yang menyusun konsep yang berkaitan dengan kriptografi serta menggunakan DELPHI sebagai alat bantu komputasi. Pada metode ini menjelaskan tentang penentuan model enkipsi, penyelesaian algoritma enkripsi, serta analisa dari hasil simulasi enkripsi. Berikut diagram alir perancangan simulasi pada penelitian ini.



***Gambar 1.** Diagram alir perancangan simulasi*

Gambar di atas menjelaskan penelitian yang dilakukan dimulai dari studi pustaka, dilanjut dengan menemukan permasalahan, lalu menentukan model enkripsi dan deskripsi, kemudian melakukan perhitungan matematis, setelah perhitungan matematis dilakukan, maka dibuatlah aplikasi simulasi sebagai uji coba dari perhitungan matematis tersebut dan di analisa apakah sudah benar atau belum.

Metode Pengembangan Sistem

Pada metode pengembangan sistem ini menggunakan metode Extreme Programing. Merupakan sebuah metode dalam pengembangan sistem yang dilakukan untuk membuat perancangan sistem yang sedang berjalan. Berikut tahapan yang dilakukan dalam metode Extream Programing :

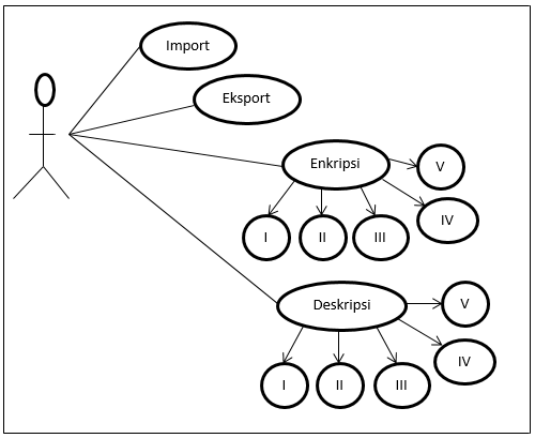
1. *Perencanaan*
   Merupakan tahapan yang dimulai dari pengumpulan segala kebutuhan serta membantu tim teknikal untuk memahami konteks dari aplikasi tersebut. Kemudian pada tahap ini juga mendefinisikan output yang akan dihasilkan.

2. *Perancangan*
   Pada metode ini ditekankan dalam desain aplikasi, bagaimana aplikasi tersebut berjalan dengan baik
3. *Pengkodean*
   merupakan konsep utama pada extrame pogramming, bagaimana cara menyusun kode sederhana sehingga mudah dipahami.
4. *Pengujian*
   Tahap ini merupakan tahapan terakhir yang difokuskan pada pengujian fitur dan fungsionalitas dari aplikasi.

Borland Delphi

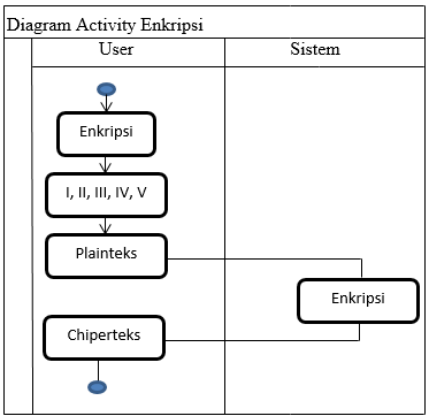
Pada awalnya borland delphi merupakan proyel rahasia yang bervolusi menjadi produk yang disebut dengan App Builder. Tujuan dari delphi tersebut adalah untuk menyediakan konektivitas database untuk programer yang akan menjadi fitur kunci pada database. Setelah tahap analisa sistem dilakukan, maka analisa sistem mendapatkan gambaran jelas tentang apa yang harus dilakukan. Kemudian analisa sistem memikirkan bagaimana membentuk sistem tersebut. Berikut alat rancang yang akan digunakan, diantaranya :

a. *Usecase*
   Merupakan bagian tertinggi dari fungsionalitas yang dimiliki sistem yang menggambarkan bagaimana seseorang atau actor yang akan menggunakan dan memanfaatkan sistem. Berikut merupakan gambar diagram use case peminjaman ruangan dan peralatan :

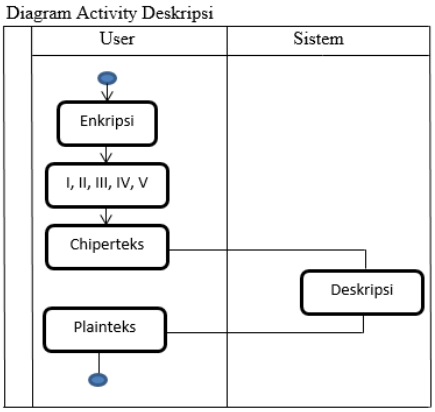


Gambar 2. *Usecase sistem enkripsi dan deskripsi*

b. *Activity Diagram*
   Activity diagram memberikan gambaran rancangan alur disetiap fungsi yang ada dalam system. Activity diagram juga menggambarkan berbagai alir aktivitas dalam sistem yang sedang dirancang bagaimana awal terjadi, dan bagaimana mereka berakhir.



Gambar 3. *Diagram Activity Enkripsi*



Gambar 4. *Diagram Activity Deskripsi*

Panel kiri pada gambar diatas merupakan pilihan antara enkripsi atau deskripsi, kemudian disampingnya terdapat pilihan untuk melakukan pergeseran antara 1 sampai 5, serta dibawah panel itu adalah input untuk plainteks yaitu teks yang akan di enkripsi, kemudian di bawah panel itu ada chiper text yaitu hasil dari proses enkripsi. Pada panel sebelah kanan merupakan fitur untuk import dan export, yaitu fitur untuk mengambil file yang ada di dalam komputer kemudian export untuk menyimpan hasil enkripsi ke dalam komputer dalam bentuk file teks yang bisa dibuka dengan notepad.

Hasil dan Pembahasan

1. *Hasil Perhitungan Matematis*

   Data yang akan digunakan sebagai pesan (plaintext) yaitu berupa karakter huruf a-z. pada pesan ini akan dilakukan proses enkripsi menggunakan kriptografi Caesar cipper, kemudian setelah terenkripsi akan menghasilkan sebrah kode (ciphertext). Kemudian ciphertext dapat dideskripsi agar kembali ke bentuk awal berupa plaintext. Tabel substitusi dari perubahan metode Caesar adalah sebagai berikut.

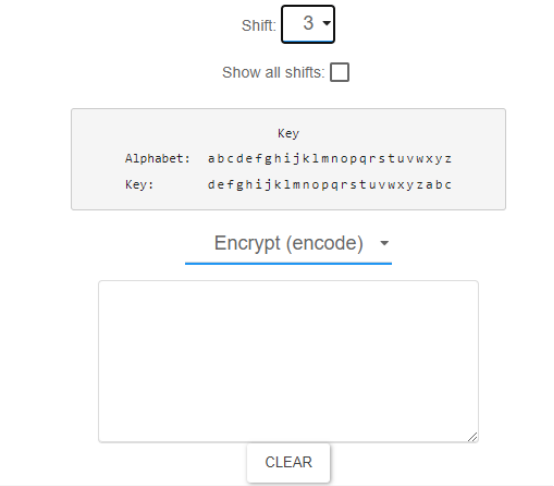
Tabel 1. *tabel Caesar cipper*

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
D	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*

Pada tabel 1 merupakan tabel sumber untuk dijadikan rujukan dalam proses enkripsi, dengan pergeseran 3 karakter, maka dilakukan proses enkripsi adalah sebagai berikut:
Plaintext : kami kelompok tiga

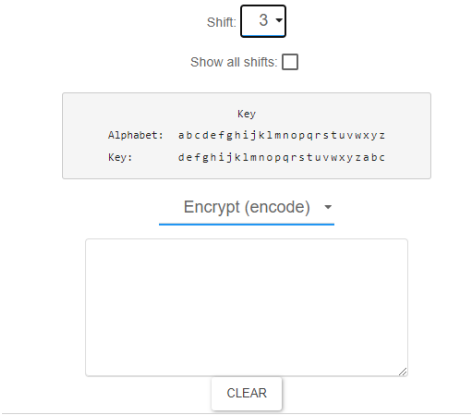
Kunci : bergeser 3 huruf
Chipertext : ndpl nhopsn wljd

2. *Simulasi Proses Enkripsi*
   Sistem enkripsi yang peniliti buat diharapkan dapat mengamankan data sehingga privasi terjaga dan aman. Berikut penjelasan program proses enkripsi:
   a. *Menu Utama*
      Menu utama merupakan halaman utama tampilan aplikasi simulasi Caesar cipper



Gambar 5. *Menu Utama*

   b. *Menu Enkripsi*
      Menu enkripsi adalah menu untuk proses enkripsi file.

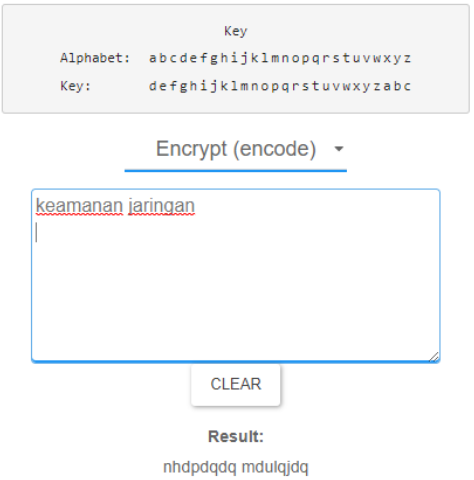


Gambar 6. *Menu Enkripsi*

   c. *Menu Deskripsi*
      Menu deskripsi adalah menu untuk proses deskripsi file.

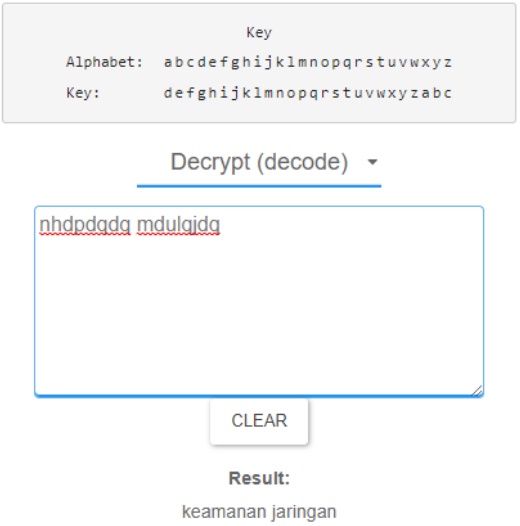
Gambar 7. *Menu Deskripsi*

d. *Enkripsi Substitusi 3*
Berikut ini adalah hasil enkripsi dengan substitusi pergeseran 3 kali huruf. Hasilnya adalah:



Gambar 8. *Enkripsi Substitusi 3*

e. *Deskripsi Caesar Chipper*
Berikut ini adalah hasil deskripsi ciphertext menjadi plaintext.



Gambar 9. *Deskripsi Caesar Chipper*

Kesimpulan

Berdasarkan pembahasan dari bab-bab sebelumnya, maka penelitian ini dapat diambil kesimpulan sebagai berikut :

a. *Algoritma caesar cipher termasuk pada kriptografi klasik yang memiliki kunci simestris (hanya ada satu kunci) yang mana biasa digunakan dalam mengekripsi ataupun mendekripsi data dan informasi.*
b. *Chiper ini berjenis chiper substitusi, dimana setiap huruf pada plaintextnya digantikan dengan huruf lain yang tetap pada posisi alphabet.*
c. *Jenis penelitian yang digunakan adalah penelitian terapan, menjelaskan tentang penentuan model enkipsi, penyelesaian algoritma enkripsi, serta analisa dari hasil simulasi enkripsi.*
d. *Metode yang digunakan pada sistem ini menggunakan metode Extreme Programming. Tahap-tahapannya sebagai berikut : perencanaan, perancangan, pengkodean, dan pengujian.*

Daftar Referensi

[1] D. Purnamasari, “Implementasi Algoritma Kriptografi Caesar Cipher dan Rail Fence Cipher untuk Keamanan Data Teks Menggunakan Python,” E-Journal.Ivet.Ac.Id, vol. 4, no. 1, pp. 1–7, 2021, [Online]. Available: http://e-journal.ivet.ac.id/index.php/jiptika/article/view/1697

[2] Febria, “Perancangan Alat Ukur Kualitas Perangkat Lunak Menggunakan Komponen ISO/IEC 9126,” E-JURNAL JUSITI J. Sist. Inf. …, no. April 2013, pp. 103–115, 2018, [Online]. Available: https://ejurnal.dipanegara.ac.id/index.php/jusiti/article/view/13

[3] F. Nuraeni and Y. H. Agustin, “The IMPLEMENTASI CAESAR CIPHER & ADVANCED ENCRYPTION STANDAR (AES) PADA PENGAMANAN DATA PAJAK BUMI BANGUNAN,” J. Ilm. Matrik, vol. 22, no. 2, pp. 187–194, 2020, doi: 10.33557/jurnalmatrik.v22i2.949.

[4] J. T. Informatika F. Sains and D. A. N. Teknologi, "Implementasi Kombinasi Algoritma Asimetri Riverst Shamir Adleman Dan Algoritma Simetris Advanced Encryption Standard Pada Aplikasi Pesan Singkat," 2017.

[5] K. Andrea, A. Wardana, B. S. Wanandi, and A. Ikhwan, “Penerapan Kriptografi Caesar Cipher Pada Fitur Aplikasi Chatting Whatsapp,” JPPIE J. Has. Penelit. dan Pengkaj. Ilm. Eksakta, vol. 2, no. 1, pp. 6–11, 2023.

[6] K. B. Ziliwu, A. Maslan, and H. Kremer, “Implementasi Caesar Cipher pada Algoritma Kriptografi dalam Penyandian Pesan Whatsapp,” J. Comasie, vol. 7, no. 2, pp. 117–125, 2022.

[7] M. N. Sutoyo and M. Murhaban, “Kombinasi Algoritma Kriptografi Caesar Chiper dan Vigenere Chiper Untuk Keamanan Data,” J. Mekanova, vol. 2, no. 2, pp. 58–66, 2016.

[8] N. Syahputri, "Rancang Bangun Aplikasi Kriptografi Pengamanan Transmisi Data Multimedia Menggunakan Algoritma Data Encryption Standard ....," Maj. Ilm. Methoda, Vol. 9, no. 2, pp, 57-63, 2019.

[9] Oktaria Riska, "Perancangan Aplikasi Pembelajaran Kriptografi Pada Algoritma Data Encryption System (DES) Menggunakan Metode Computer Assisted Instruction," Jurnal Teknik Informatika Kaputama, Vol. 3, No. 2, 2019.

[10] R. Febrianingsih and A. Hafiz, “Implementasi Kriptografi Berbasis Caesar Chiper Untuk Keamanan Data,” J. Inf. Dan Komput., vol. 7, no. 2, pp. 81–86, 2019.

[11] R. Rinaldi, “Analisis Keamanan Modifikasi Metode Caesar Chiper,” J. Digit. Ecosyst. Natual Sustain., vol. 2, no. 2, pp. 45–48, 2022

[12] Rusdiana and Irfan. Sistem Informasi Manajemen. 2014. Pustaka Setia: Bandung.

[13] S. Andayani and D. S. Agista, “KRIPTOGRAFI KLASIK TEKNIK SUBSITUSI UNTUK KEAMANAN DATA MENGGUNAKAN VB.Net 2008,” J. Matrix, vol. 4, no. 2, pp. 75–80, 2014.

[14] Sumandri, "Studi Model Algoritma Kriptografi Klasik dan Modern," Seminar Matematika Dan Pendidikan Matematika UNY, 2017.

[15] Wongso Fery, "Perancangan Sistem Pencatatan Pajak Reklame Pada Dinas Pendapatan Kota Pekanbaru dengan Metode Visual Basic," Jurnal Ilmiah Ekonomi dan Bisnis, 14(2), 160-180. 2019.