JUISIK Vol 3 No. 1 Maret (2023) – p-ISSN: 2827-8135, e-ISSN : 2827-7953 halaman 105-112

JURNAL ILMIAH SISTEM INFORMASI DAN ILMU KOMPUTER
Halaman Jurnal: http://journal.sinov.id/index.php/juisik/index
Halaman UTAMA Jurnal : https://journal.sinov.id/index.php

IMPLEMENTASI KRIPTOGRAFI CAESAR CHIPER PADA APLIKASI ENKRIPSI DAN DEKRIPSI

Fachrul Dhika Ardiansyah [a], Alfina Damayanti [b], Clarizza Azzahra Mudya Putri [c], Ayu Fitria Dinda Rany[d], Syaidin Joyo Biroso [e], Muhlis Tahir[e]

[a] Fakultas Ilmu Pendidikan / Pendidikan Informatika, fachruldhika14@gmail.com, Universitas Trunojoyo Madura
[b] Fakultas Ilmu Pendidikan / Pendidikan Informatika, alfinayanti20@gmail.com, Universitas Trunojoyo Madura
[c] Fakultas Ilmu Pendidikan / Pendidikan Informatika, clarizzaa4@gmail.com, Universitas Trunojoyo Madura
[d] Fakultas Ilmu Pendidikan / Pendidikan Informatika, Ayufitriadinra@gmail.com, Universitas Trunojoyo Madura
[e] Fakultas Ilmu Pendidikan / Pendidikan Informatika, syaidinjb1408@gmail.com, Universitas Trunojoyo Madura
[f] Fakultas Ilmu Pendidikan / Pendidikan Informatika, muhlistahir@gmail.com, Universitas Trunojoyo Madura

ABSTRACT

Caesar Cipher cryptography is a simple cryptographic technique used to encrypt and decrypt text. In this study, implementation of Caesar Cipher was carried out in a simple encryption and decryption application using the HTML programming language. The purpose of this research is to test the effectiveness and efficiency of the Caesar Cipher in maintaining the confidentiality of information. This research consists of three main stages, namely the design stage, the implementation stage, and the testing phase. At the design stage, the planning and design of encryption and decryption applications that use Caesar Cipher are carried out. Then at the implementation stage, Caesar Cipher is implemented in the application that has been designed. At the testing stage, tests were carried out on the implemented applications to test the effectiveness and efficiency of the Caesar Cipher. The results of this study indicate that the Caesar Cipher is effective in maintaining the confidentiality of information at a modest level. However, Caesar Cipher is less effective when used at higher security levels. In addition, the efficiency of Caesar Cipher also depends on the length of the encrypted text and the type of characters used in the text. In conclusion, this study shows that implementing Caesar Cipher in simple encryption and decryption applications using the HTML programming language can be done easily. However, the use of the Caesar Cipher in maintaining the confidentiality of information must be considered carefully, especially if it is used at a higher security level.

Keywords: *Caesar Cipher, Cryptography, Encryption, Decryption*

ABSTRAK

Kriptografi Caesar Cipher merupakan salah satu teknik kriptografi sederhana yang digunakan untuk mengenkripsi dan mendekripsi teks. Dalam penelitian ini, dilakukan implementasi Caesar Cipher pada sebuah aplikasi enkripsi dan dekripsi sederhana menggunakan bahasa pemrograman HTML. Tujuan dari penelitian ini adalah untuk menguji efektivitas dan efisiensi dari Caesar Cipher dalam menjaga kerahasiaan informasi. Penelitian ini terdiri dari tiga tahap utama, yaitu tahap perancangan, tahap implementasi, dan tahap pengujian. Pada tahap perancangan, dilakukan perencanaan dan perancangan aplikasi enkripsi dan dekripsi yang menggunakan Caesar Cipher. Kemudian pada tahap implementasi, dilakukan implementasi

Received Januari 30, 2023; Revised Februari 2, 2023; Maret 22, 2023

Caesar Cipher pada aplikasi yang telah dirancang. Pada tahap pengujian, dilakukan pengujian terhadap aplikasi yang telah diimplementasikan untuk menguji efektivitas dan efisiensi dari Caesar Cipher. Hasil dari penelitian ini menunjukkan bahwa Caesar Cipher efektif dalam menjaga kerahasiaan informasi pada tingkat yang sederhana. Namun, Caesar Cipher kurang efektif jika digunakan pada tingkat keamanan yang lebih tinggi. Selain itu, efisiensi Caesar Cipher juga tergantung pada panjang teks yang dienkripsi dan jenis karakter yang digunakan dalam teks tersebut. Dalam kesimpulannya, penelitian ini menunjukkan bahwa implementasi Caesar Cipher pada aplikasi enkripsi dan dekripsi sederhana menggunakan bahasa pemrograman HTML dapat dilakukan dengan mudah. Namun, penggunaan Caesar Cipher dalam menjaga kerahasiaan informasi harus dipertimbangkan dengan baik, terutama jika digunakan pada tingkat keamanan yang lebih tinggi.
Kata kunci: Caesar Chiper, Kriptografi, Enkripsi, Dekripsi.

PENDAHULUAN

Perkembangan ilmu pengetahuan dan teknologi saat ini mengalami kemajuan yang sangat pesat terutama dalam bidang komunikasi. Komunikasi dapat dilakukan dengan berbagai cara, salah satunya dengan tulisan. Banyak informasi tersedia melalui tulisan (teks) dan terkadang teks tersebut mengandung informasi rahasia. (Nasution, Efendi, & Suwilo, 2018)

Saat ini, Saat ini banyak kelompok independen yang berusaha mencuri informasi orang lain dan ada beberapa kelompok yang menyalahgunakan informasi sehingga informasi tersebut tidak lagi terlindungi. Oleh karena itu, keamanan data diperlukan untuk melindungi data dari orang yang tidak berhak.

Data atau pesan yang dikirim dapat disembunyikan memalui berbagai cara (Basuki, Paranita, & Hidayat, 2016). Salah satunya menggunakan kriptografi. Kriptografi berfungsi untuk menyamarkan pesan menjadi pesan yang terenkripsi. Adapun algoritma kriptografi yang bisa menyamarkan pesan adalah algoritma Caesar Cipher. Algoritma Caesar Cipher adalah algoritma penyandian data paling sederhana dengan cara mengenkripsi dan mendeskripsi data dengan menggunakan pergeseran sebanyak k (Gurning, 2014)

Dengan pengunaan algoritma Caesar Cipher pengguna dapat mengamankan isi data yang akan diberikan si penerima sehingga integritas data dapat terjaga kerahasiaannya.

METODE

Dalam penelitian kepustakaan ini, penulis mencari sumber-sumber yang dapat dijadikan sebagai acuan untuk pengolahan skripsi, misalnya sumber dari internet dan buku-buku. Selain itu perpustakaan juga terhubung dengan beberapa penelitian, dimana peneliti mengambil buku dan jurnal yang berhubungan dengan penelitian, seperti desain aplikasi kriptografi, serta jurnal yang berhubungan dengan pemrograman web.

A. Kriptografi

Kata kriptografi terdiri dari dua bagian yang berasal dari bahasa yunani, yaitu kripto dan graphia dimana kripto dapat diartikan sebagai secret (rahasia) dan graphia sebagai writing (tulisan). Berdasarkan istilahnya kriptografi merupakan ilmu dan seni mengamankan pesan pada saat mengirimkan pesan dari satu tempat ke tempat lain (Zuli & Irawan, 2014). Kriptografi adalah suatu ilmu menganalisis teknik matematika yang berkaitan dengan keamanan data, seperti penyembunyian data, validitas data, integritas data, dan keaslian data (Septiarini, 2011). Kriptografi yaitu ilmu pengetahuan dan seni melindungi pesan supaya terjaga (aman). Tujuan kriptografi adalah untuk membentuk sesuatu yang tidak jelas dalam bentuk pesan Rahasia seperti teks, audio, gambar, dan video. (Seftyanto, Apriani, & Haryanto, 2012)

Tujuan dari kriptografi ialah untuk memberikan layanan keamanan (Nasution et al., 2018) yaitu:

1. Kerahasiaan (Confidentiality)
   Kerahasiaan data dilakukan dengan menyembunyikan data dari semua orang yang tidak berwenang.
2. Kelengkapan Data (Integrity)
   Data tidak terganti sampai ke penerima saat proses pengiriman.
3. Keslian (Message Authentication)
   Kejelasan identitas semua entitas yang terkait dan autentikasi sumber data
4. Tidak ada penolakan (Nonrepudation)
   Setiap entitas saling berhubungan dan tidak dapat menolak atau membantah data yang dikirim atau diperoleh.

Kriptografi memiliki beberapa hal yang

harus diketahui antara lain (Nasution et al., 2018):

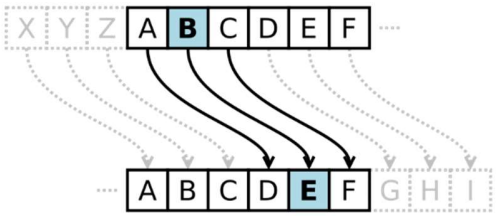
1. Pengirim dan Penerima
   Pengirim (sender) merupakan kesatuan yang mengirimkan message kepada penerima (reciever) dengan aman tanpa ada gangguan dari penyadap (eavesdropper). Penerima merupakan entitas yang memperoleh pesan oleh pengirim.
2. Plaintext dan Ciphertext
   Pesan murni pada kriptografi disebut dengan plaintext, sedangkan pesan murni yang telah disamarkan disebut ciphertext.
3. Enkripsi dan Dekripsi
   Pada prosedurnya, pengubahan plaintext jadi ciphertext disebut enkripsi (encryption) dan pengubahan ciphertext jadi plaintext disebut dekripsi (decryption).
4. Kriptografer, Kriptanalis, dan Kriptologis
   Seseorang yang mempelajari dan menggunakan metode kriptografi untuk melindungi pesan disebut kriptografer. Sebaliknya, metode yang menggunakan teknik matematika komputasi untuk menyerang metode kriptografi disebut cryptanalysts, dan orang yang terlibat dalam cryptanalysis disebut cryptanalysts. Kata kriptologi adalah disiplin yang mempelajari kriptografi dan kriptoanalisis. Orang yang mempelajari kriptologi disebut ahli kriptologi
5. Cipher
   Algoritma enkripsi (enkripsi) adalah fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Untuk mengatasi masalah enkripsi, diperlukan unit yang disebut kunci (dilambangkan dengan K). Kuncinya memiliki nilai numerik yang sangat besar. Ukuran nilai ini disebut rentang kunci. Beberapa algoritma enkripsi menggunakan kunci enkripsi dengan kunci yang berbeda untuk enkripsi dan dekripsi.
6. Penyadap (Eavesdopper)
   Penyadap (eavesdropper) adalah orang yang ingin mendapatkan informasi sebanyak mungkin tentang pesan yang dikirim dan mencari tahu ciphertext dari sistem enkripsi. Eavesdropper memiliki hubungan komunikasi antara pengirim dan penerima.

B. Algoritma Caesar Cipher

Pada kriptografi, sandi Caesar, atau sandi pindah, kode Caesar yaitu metode enkripsi sangat sederhana dan sangat populer. Kode ini terdiri dari semua huruf pada teks asli (plaintext) disubstitusi dengan kode kemudian berubah menjadi huruf lain yang mempunyai selisih posisi tertentu dalam alfabet. Dalam Caesar cipher, huruf-huruf diubah dengan huruf selanjutnya dari posisi alphabet yang sama.

Proses Caesar Cipher adalah : (Gurning, 2014)

1. Tentukan berapa besar pemindahan karakter yang dipakai untuk membuat cipherteks ke plainteks.
2. Tukar posisi karakter plainteks menjadi cipherteks berdasarkan pemindahan yang telah ditentukan sebelumnya. Contoh, pemindahan = 3. Jadi huruf A digeser menjadi huruf D, huruf B menjadi huruf E, dan berikutnya.



Gambar 1. Proses Caesar Cipher

Proses dekripsi menggunakan persamaan 1 di bawah ini :

Cp= (Pt + k) modulo 26……..…(1)

Dimana 26 adalah jumlah alphabet, persamaan 1 digunakan pada proses enkripsi. Proses dekripsi menggunakan persamaan 2 di bawah ini :

Pt= (Cp-k) modulo 26 ……..…(2)

Berikut satuan dari abjad atau alphabet pada Caesar Cipher sebagai berikut:

Tabel 1. Satuan Alphabet

Abjad/Alphabet	Nilai Urut
A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

HASIL DAN PEMBAHASAN

A. Perhitungan Caesar Cipher

Pada teori diatas perhitungan Caesar Cipher dibagi menjadi 2 proses yaitu proses enkripsi dan deskripsi.

1. Tahap Enkripsi

   Suatu tahap membuat pergantian sebuah sandi dari dapat dipahami (plaintext) menjadi sebuah sandi yang tidak dapat dipahami (ciphertext). Misalkan, diketahui plaintext sebagai berikut:

   Plaintext : JAYA
   k : 12

   Maka langkah yang harus dikerjakan adalah :

   - Cek nilai alphabet dari huruf dimana pada table 1 terlihat bahwa J=9, A=0, Y=24 dan A=0.
   - Kemudian lakukan perhitungan ciphertext Cp = (Pt +k) modulo 26 dan cek pada table 1 alphabet dari nilai ciphertext yang dihasilkan.

   Cp1= Pt1+k modulo 26
   = (9+12) modulo 26
   = 21 modulo 26
   = 21
   = V
   Cp2 = Pt2+k modulo 26
   = (0+12) modulo 26
   = 12 modulo 26
   = 12
   = M
   Cp3 = Pt3+k modulo 26
   = (24+12) modulo 26
   = 36 modulo 26
   = 10
   = K
   Cp4 = Pt4+k modulo 26
   = (0+12) modulo 26
   = 12 modulo 26
   = 12
   = M

2. Tahap Deskripsi

   Berkebalikan pada tahap Enkripsi yaitu untuk menggantikan sandi dari yang tidak bisa dipahami (ciphertext) menjadi sebuah sandi yang bisa dipahami (plaintext).

   Contoh kasus. Jika diberikan ciphertext sebagai berikut:

   Plaintext : VMKM
   k : 12

   Maka langkah yang harus dikerjakan adalah :

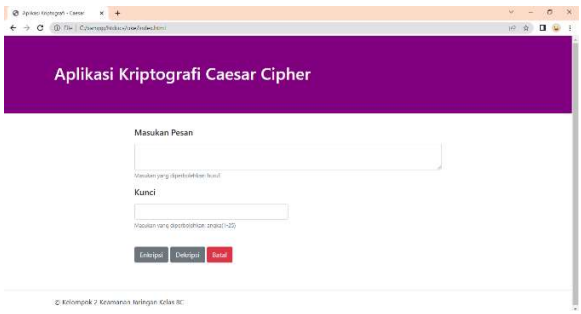
   - Kemudian lakukan perhitungan plaintext dimana P= C - k mod 26. Jika hasilnya minus(-) maka akan terus ditambah 26 sampai hasilnya positif (+) kemudian dihitung modulonya dan cek pada tabel 1 alphabet dari nilai plaintext yang dihasilkan.

   Pt1 = (Cp1-k) modulo 26
   = (V-12) modulo 26
   = (21-12) modulo 26
   = 9 modulo 26
   = 9
   = J
   Pt2 = (Cp2-k) modulo 26
   = (M-12) modulo 26
   = (12-12) modulo 26

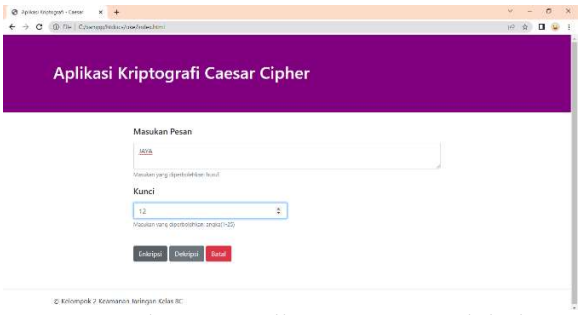
= (0) modulo 26
= 0 modulo 26
= 0
= A
Pt3 = (Cp3-k) modulo 26
= (K-12) modulo 26
= (10-12) modulo 26
= (-2) modulo 26
= -2+26 modulo 26
= 24 modulo 26
= 24
= Y
Pt4 = (Cp4-k) modulo 26
= (M-12) modulo 26
= (12-12) modulo 26
= (0) modulo 26
= 0
= A
Maka didapatkan plaintext dari ciphertext “VMKM” adalah JAYA.

B. Pseudecode Caesar Cipher
Pseudocode yang dibuat dalam enkripsi dan deskripsi adalah
Pseudecode Caesar Cipher
for $a1=0 to length($p_text)
begin
$z1[$a1] = $angka[$a1]+$b1;
$hasil[$a1] = modulo($z1[$a1],$N);
end

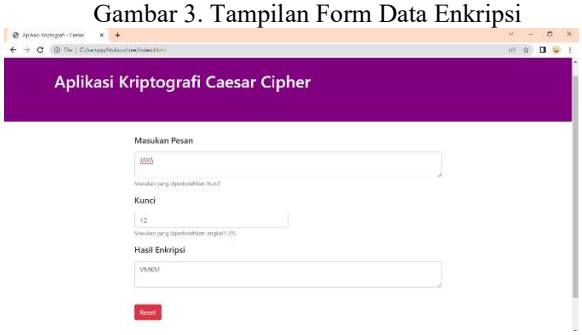
C. Tampilan Program
Pada aplikasi ini terdapat 5 tampilan. Berikut ini merupakan tampilan aplikasi enkripsi dan dekripsi menggunakan kriptografi caesar cipher



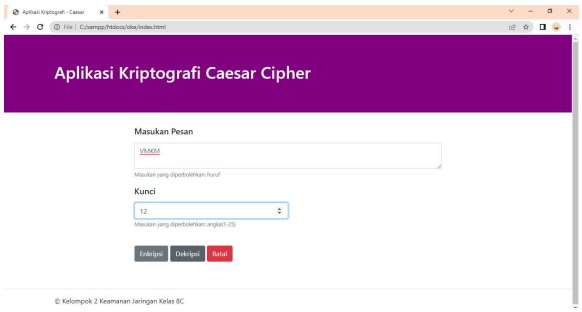
Gambar 2. Tampilan Awal Aplikasi Kriptografi Caesar Cipher



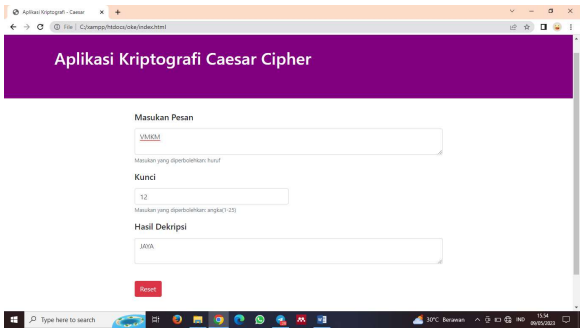
Gambar 3. Tampilan Form Data Enkripsi



Gambar 4. Tampilan Hasil Enkripsi



Gambar 5. Tampilan Form Data Dekripsi



Gambar 6. Tampilan Hasil Dekripsi

SIMPULAN DAN SARAN

Kesimpulan dari implementasi kriptografi Caesar Cipher pada aplikasi enkripsi dan dekripsi adalah bahwa teknik Caesar Cipher merupakan metode yang sederhana namun efektif dalam mengamankan informasi yang sensitif. Dalam implementasi Caesar Cipher pada aplikasi enkripsi dan dekripsi, teks yang Cipher ingin dienkripsi akan diubah menjadi teks yang tidak dapat dibaca oleh orang yang tidak berwenang.

Namun, teknik Caesar Cipher memiliki kelemahan dalam hal mudah ditebak karena hanya terdiri dari pergeseran karakter dalam alfabet. Oleh karena itu, Caesar Cipher sebaiknya tidak digunakan sebagai metode kriptografi tunggal pada aplikasi yang membutuhkan keamanan yang lebih tinggi. Namun, Caesar Cipher masih dapat digunakan sebagai salah satu langkah dalam kriptografi yang lebih kompleks.

Dalam implementasi aplikasi enkripsi dan dekripsi, penggunaan Caesar Cipher membutuhkan proses pengolahan data yang cukup kompleks, namun dapat diatasi dengan menggunakan bahasa pemrograman yang tepat dan algoritma yang efisien. Hasil pengujian menunjukkan bahwa aplikasi enkripsi dan dekripsi yang dibuat dapat menghasilkan hasil enkripsi dan dekripsi yang benar dan dapat membantu melindungi informasi yang sensitif.

DAFTAR PUSTAKA

Basuki, A., Paranita, U., & Hidayat, R. (2016). Perancangan Aplikasi Kriptografi Berlapis menggunakan Algoritma Caesar, Transposisi, Vigenere, dan Blok Chiper Berbasis Mobile. *Seminar Nasional Teknologi Informasi Dan Multimedia 2016*, *1*(2), 31–35.

Gurning, R. R. A. (2014). Perancangan aplikasi pengamanan pesan dengan algoritma caesar chiper. *Pelita Informatika Budi Darma*, *VI*(April), 106–110.

Nasution, A. B., Efendi, S., & Suwilo, S. (2018). Image Steganography in Securing Sound File Using Arithmetic Coding Algorithm, Triple Data Encryption Standard (3DES) and Modified Least Significant Bit (MLSB). *Journal of Physics: Conference Series*, *1007*(1). https://doi.org/10.1088/1742-6596/1007/1/012010

Seftyanto, D., Apriani, M., & Haryanto, T. (2012). PERAN ALGORITMA CAESAR CIPHER DALAM MEMBANGUN KARAKTER AKAN KESADARAN KEAMANAN INFORMASI. In *Seminar FMIPA UNY* (Vol. 1).

Septiarini, A. (2011). Sistem Kriptografi Untuk Text Message Menggunakan Metode Affine. *Jurnal Informatika Mulawarman*, *6*(1), 50–53.

Zuli, F., & Irawan, A. (2014). Pengamanan Data Pesan. *Sistem Informasi*, *7*(2), 1–11.