Nusantara Hasana Journal
Volume 2 No. 9 (Februari 2023), Page: 254-259
E-ISSN : 2798-1428

PENERAPAN KRIPTOGRAFI CAESAR CIPHER PADA FITUR PESAN TEKS

Application Of Caesar Cipher Cryptography To The Text Message Feature

Samsuriah[1], Ida[2]

[1,2]STMIK Profesional Makassar

Email: samsuriahagus@gmail.com
Email : idamulyadi@stmikprofesional.ac.id

Abstract
The progress of communication in the era of technological development where applications and communication support in various ways are increasingly sophisticated indicates that more and more people need access and relationships in every existing communication. Therefore, data or information security is needed to maintain confidentiality. One way to secure data or information is with Cryptology. Cryptography is the study of posting security (confidentiality), cryptographic algorithm techniques consisting of substitution and transposition techniques. Cryptographic methods or techniques can be trusted to deal with data or information security problems, because apart from using computer programming languages, cryptography also uses mathematical formulas, ranging from simple formulas to complex formulas. From the results of the study it can be concluded that with the formula used in the Caesar Cipher cryptographic method, it can be said that even though the Caesar Cipher is difficult to solve, it can be easily solved using mathematical formulas and using a programming language to obtain encryption and decryption results.
Keywords: *Cryptography, Caesar , Cipher*

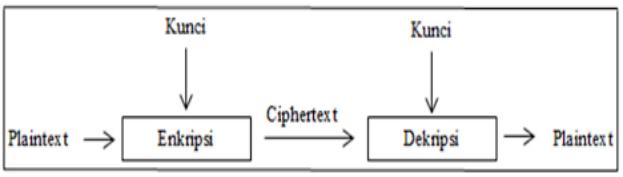
Abstrak
Kemajuan komunikasi di era perkembangan teknologi di mana aplikasi dan penunjang komunikasi dalam berbagai hal semakin canggih menunjukkan bahwa semakin banyaknya masyarakat yang membutuhkan akses dan hubungan dalam setiap komunikasi yang ada. Oleh karena itu di butuhkannya keamanan data ataupun informasi dalam menjaga kerahasiaan. Salah satu cara untuk mengamankan data atau informasi dengan Kriptologi. Kriptografi adalah studi keamanan (kerahasiaan) posting, teknik algoritma kriptografi terdiri dari teknik substitusi dan transposisi . Metode atau teknik kriptografi dapat dipercaya untuk menangani masalah keamanan data atau informasi, karena selain menggunakan bahasa pemrograman komputer, kriptografi juga menggunakan rumus matematika, mulai dari rumus sederhana untuk formula kompleks. Dari hasil penelitian dapat disimpulkan bahwa dengan adanya formula yang dipakai dalam metode kriptografi Caesar Cipher, dapat dikatakan bahwa Caesar Cipher meskipun sulit untuk dipecahkan, namun dalam hal dapat dengan mudah di pecahkan dengan menggunakan rumus matematika dan dengan menggunakan bahasa pemrograman untuk mendapatkan hasil enkripsi dan dekripsi.
Kata Kunci: Kriptografi, Caesar, Cipher

PENDAHULUAN

Kemajuan komunikasi di era perkembangan teknologi di mana aplikasi

Nusantara Hasana Journal
Volume 2 No. 9 (Februari 2023), Page: 254-259
E-ISSN : 2798-1428

dan penunjang komunikasi dalam berbagai hal semakin canggih menunjukkan bahwa semakin banyaknya masyarakat membuthkan akses dan hubungan dalam setiap komunikasi yang ada. Oleh karena itu di butuhkan keamanan data dan informasi dalam menjaga kerahasiaan. Salah satunya adalah penerapan kriptografi. Penerapan kriptografi tidak hanya dilakukan dengan satu metode saja, akan tetapi dapat dilakukan dengan berbagai cara dan metode, diantaranya dengan menggabungkan beberapa metode dalam pengamanan data informasi yang bersifat penting ataupun pribadi dengan cara melakukan enkripsi terlebih dahulu sebelum informasi tersebut di kirim ke pihak kedua yaitu penerima sehingga kerahasiaan data dan keamanan data informasi dapat terjaga dengan baik[2].



Gambar 1. Skema Enkripsi dan Dekripsi menggunakan Kunci

Pada penelitian oleh Pamungkas dan Muhammad, (2022) menyatakan bahwa Perkembangan dalam dunia teknologi informasi memanfaatkan teknologi komputer menjadikan salah satu pilihan dalam melakukan berbagai hal yang terdapat di dalamnya dapat berupa aplikasi, sms ataupun sistem pengamanan data yang menjaga keamanan dan kerahasiaan data informasi dalam ilmu penegembangan seperti kriptografi. Pada penerapan yang di lakukan tidak dari satu teknik keamanan saja melainkan dapat dilakukan dengan berbagai kombinasi, ataupun modifikasi dalam keamanan data dan informasi. Konsep utama pada kriptograsi yakni enkripsi dan dekripsi. Sebuah pesan, informasi ataupun data yang di enkripsi agar orang yang tidak berhak untuk membaca pesan tersebut tidak akan dapat membacanya. Dari perkembangan berbagai metode penggunaan kriptografi dapat sering kali di pecahkan dan di selesaikan oleh pihak lain yang tidak berhak di karenakan kunci dari informasi pesan data tersebut tidak sulit memecahkannya. Dalam tulisan yang di buat ini penulis memodifikasi metode Caesar cipher menggunakan beberapa symbol dan angka sehingga menghasilkan pola dengan beberapa tahap metode[1].

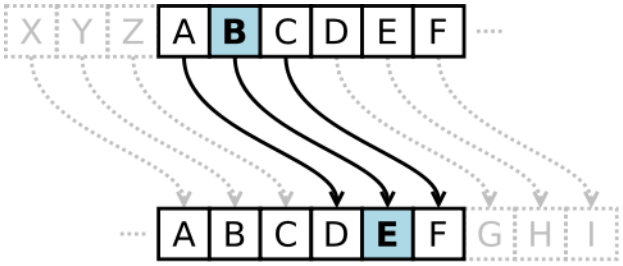
Berdasarkan uraian dan permasalahan yang ditemukan maka penulis akan melakukan uraian topik yang membahas tentang Penerapan Kriptografi Caesar cipher pada fitur pesan teks.

METODE

Caesar cipher adalah metode penyandian yang digunakan oleh Julius Caesar untuk berkomunikasi dengan para panglimanya. Dalam kriptografi Caesar cipher di kenal dengan beberapa nama seperti : shift cipher, Caesar's code atau Caesar shift. Caesar cipher merupakan teknik enkripsi yang paling sederhana dan banyak digunakan[5]. Cipher ini berjenis cipher substitusi, dimana setiap huruf pada plaintexnya di gantikan dengan huruf lain yang tetap pada posisi alphabet. Misalnya di ketahui bahwa pergeseran = 3, maka huruf A akan di gantikan oleh

Nusantara Hasana Journal
Volume 2 No. 9 (Februari 2023), Page: 254-259
E-ISSN : 2798-1428

huruf D, huruf B menjadi huruf F, dan seterusnya, untuk proses pergeseran dapat dilihat pada gambar 2



Gambar 2. Proses pergeseran 3 huruf

Gambar 2 dapat direpresentasikan dengan menyelaraskan plaintext dengan chipertext ke kiri atau kanan sebanyak jumlah pergeseran yang di inginkan sebagai contoh dengan jumlah pergeseran sebanyak 3.

Plaintext : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher : DEFGHIJKLMNOPQRSTUVWXYZABC

Untuk membaca pesan yang di enkripsi penerima dapat menyelaraskan huruf chipertext yang diterima dengan plaintext yang tepat berada di atasnya. Sebagai contoh dekripsinya sebagai berikut

Cipher : VHPLQDU QDVLRQDOP DWHPDWLND
Plaintext : SEMINAR NASIONAL MATEMATIKA

Proses enkripsi pada Caesar Cipher dapat di representasikan menggunakan operator aritmatika modulo 26 setelah sebelumnya setiap huruf di transformasikan ke dalam angka, yaitu: A = 0, B = 1, …. Z = 25. Maka Caesar Cipher dirumuskan sebagai berikut : Proses Enkripsi suatu huruf P dengan pergeseran K dapat di nyatakan secara matematis sebagai berikut :

Enkripsi : C = E(P) = (P + K) mod 26
Dekripsi : P = D(C) = (C - K) mod 26

Dengan C adalah ciphertext, P adalah plaintext, K adalah kunci rahasia, E(P) adalah enkripsi, dan D(C) adalah dekripsi. Kelemahan dari Caesar Cipher adalah dapat di pecahkan dengan cara brute force attack, suatu bentuk serangan yang dilakukan dengan mencoba coba berbagai kemungkinan untuk menemukan kunci. Bisa juga menggunakan exhaustive key search, karena jumlah kunci sangat sedikit (hanya ada 26 kunci)

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

Nusantara Hasana Journal
Volume 2 No. 9 (Februari 2023), Page: 254-259
E-ISSN : 2798-1428

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

Abjad/Alphabet	Nilai Urut
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 di bagi menjadi 2 proses yaitu proses enkripsi dan dekripsi.

1. Tahap Enkripsi

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

Plaintext : LOVE

K :12

Kemudian lakukan perhitungsn ciphertext Cp = (Pt + k) modulo 26 dan cek pada tabel 1 alphabet dari nilai ciphertext yang dihasilkan.

Cp1 = Pt1+k modulo 26
=(11+12) modulo 26
= 23 modulo 26
= 23 = X

Cp2 = Pt2+k modulo 26
= (14+12) modulo 26
=26 modulo 26
= 0 = A

Cp3 = Pt3+k modulo 26
= (21+12) modulo 26
= 33 modulo 26
= 7 = H

Cp4 = Pt4+k modulo 26
= (4+12) modulo 26
= 16 modulo 26
= 16 = Q

~ Hasil Enkripsi adalah " XAHQ" ~

2. Tahap Dekripsi

Berkebalikan pada tahap Enkripsi yaitu untuk menggantikan sandi dari yang tidak bisa di pahami(ciphertext) menjadi sebuah sandi yang bisa dipahami (plaintext). Contoh kasus. Jika diberikan ciphertext sebagai berikut :

Plaintext : XAHQ

K : 12

Pt1 = (Cp1-k) modulo 26
= (X-12) modulo 26
= (23-12) modulo 26
= (11) modulo 26
= 11 = L

Pt2 = (Cp2-k) modulo 26
=(A-12) modulo 26
=(0-12) modulo 26
= (-12) modulo 26
= -12+26 modulo 26

Nusantara Hasana Journal
Volume 2 No. 9 (Februari 2023), Page: 254-259
E-ISSN : 2798-1428

= 14 modulo 26
= 14= O

Pt3 = (Cp3k) modulo 26
= (H-12) modulo 26
= (7-12) modulo 26
= (-5) modulo 26
= -5+26 modulo 26
= 21 modulo
= 21 = V

Pt4 = (Cp4-k) modulo 26
= (Q-12) modulo 26
= (16-12) modulo 26
= (4) modulo 26
= 4 = E

~ Hasil Dekripsi adalah “LOVE” ~

B. Tampilan Output

1. Output Enkripsi

Hasil Output menampilkan Pesan, Key, Enkripsi dan Deksripsi

```
---------------------< com.mycompany:CaesarCipher >---------------------
Building CaesarCipher 1.0-SNAPSHOT
--------------------------------[ jar ]---------------------------------

--- exec-maven-plugin:3.0.0:exec (default-cli) @ CaesarCipher ---
 Plaintext :
LOVE
Key :
12
 ciphertext : XAHQ
------------------------------------------------------------------------
BUILD SUCCESS
------------------------------------------------------------------------
Total time:  14.280 s
Finished at: 2023-02-03T03:50:45+08:00
------------------------------------------------------------------------
```

Gambar 3. Output Enkripsi

2. Output Dekripsi

Hasil Output menampilkan : Hasil tampilan Pesan, Nilai Pergeseran, Pesan Dekripsi

```
---------------------< com.mycompany:CaesarCipher >---------------------
Building CaesarCipher 1.0-SNAPSHOT
--------------------------------[ jar ]---------------------------------

--- exec-maven-plugin:3.0.0:exec (default-cli) @ CaesarCipher ---
 Input the ciphertext message :
XAHQ
 Enter the shift value :
12
 decrypt message : LOVE
------------------------------------------------------------------------
BUILD SUCCESS
------------------------------------------------------------------------
Total time:  12.903 s
Finished at: 2023-02-02T22:40:03+08:00
------------------------------------------------------------------------
```

Gambar 4. Output Dekripsi

Nusantara Hasana Journal
Volume 2 No. 9 (Februari 2023), Page: 254-259
E-ISSN : 2798-1428

KESIMPULAN

Proses penyandian dengan algoritma Caesar Cipher berhasil digunakan untuk menyembunyikan pesan dan dapat mengembalikan pesan tersebut seperti semula. Program hanya memproses karakter A hingga Z di karenakan penggunaan angka 26. Karakter akan di hapus jika karekter bukan A hingga Z.

UCAPAN TERIMA KASIH

Ucapan terima kasih penulis persembahkan kepada STMIK Profesional Makassar dan teman serta keluarga yang telah memberi dukungan dalam hal penyediaan data dan dukungan fasilitas selama penelitian dilakukan.

DAFTAR PUSTAKA

[1] P. G. Pamungkas and A. H. Muhammad, "Modifikasi Algoritma Kriptografi Caesar Cipher pada Deretan Simbol dan Huruf di Smartphone dan Laptop," *Journal of Information Technology*, 2(1), 1-5, 2022.

[2] A. Pradipta, "Implementasi Metode Caesar Cipher Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan Informasi," *Indones. J. Netw. Secur*, 5(3), 3-6. 2016.

[3] A.B. Nasution, "Implementasi Pengamanan Data Dengan Menggunakan Algoritma Caesar Cipher dan Transposisi Cipher," (Jur IT) Jurnal Teknologi Informasi, 3(1), 1-6. 2019.

[4] C. Nas, "Pengamanan User Account Data Belajar Pada E-Task UCIC Menggunakan Algoritma Caesar Cipher Berbasis QRCode," *Jurnal Teknologi dan Informasi.*, 12(2), 2022, 118-130.

[5] Y. D. Putri., R. Rosihan and S. Lutfi, "Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance," *JIKO (Jurnal Informatika dan Komputer).*, 2(2), 87-94. 2019.