Journal of Digital Ecosystem for Natural Sustainability (JoDENS)
Vol.2, No.2, Desember 2022, pp. 45~48
e-ISSN: 2798-6179
DOI https://doi.org/10.63643/jodens.v2i2.99

Analisis Keamanan Modifikasi Metode Caesar Chiper Dalam Teknik Enkripsi Dan Deskripsi

Rizky Rinaldi [1*]
[1]*Teknologi Informasi, Universitas Pembangunan Pancabudi*
**Corresponding author E-mail: rizkyrinaldi055@gmail.com*

Article Info

Article history:

Received 24-11-2022
Revised 02-12-2022
Accepted 02-12-2022

Keyword:

Kriptografi, Caesar Chiper, Enkripsi, Dekripsi, Keamanan Komputer

ABSTRACT

The confidentiality and integrity of a message that will be conveyed is one aspect that every individual expects in carrying out information exchange activities. Many techniques that can be used to secure data include cryptography. Cryptography aims to provide security services (which are also referred to as security aspects). To be able to use cryptographic techniques, a method is needed, one of which is the Caesar Cipher method. Changes made to the character set in the caesar chiper algorithm have succeeded in making this algorithm have a better level of security. The result of the analysis of this study is that the chipertext pattern that is incited is more varied so that the level of security of this method is better than before.

I. PENDAHULUAN

Kerahasiaan 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 [1]. Pencurian data pribadi adalah tindakan yang melanggar hukum pada bidang teknologi informasi. Oleh sebab itu, pengamanan data serta informasi yang berharga yang bersifat pribadi harus memiliki tingkat pengamanan yang baik. Tingkat pengamanan data dilakukan sebagai upaya dalam melindungi data atau informasi yang bersifat rahasia agar tidak diketahui orang lain. Salah satu contoh upaya pengaman data atau informasi pribadi yang biasa dilakukan adalah dengan memberikan password terhadap file data yang bersifat rahasia [2]. Banyak teknik yang dapat digunakan untuk mengamankan data diantaranya adalah kriptografi. Teknik tersebut memiliki fungsi masing masing, kriptografi yang bertujuan untuk menyamarkan suatu pesan menjadi suatu pesan yang sulit dibaca atau dimengerti [3].

Kriptografi adalah seni dan ilmu mengenai teknik enkripsi atau penyembunyian pesan, dimana "naskah asli" (*plaintext*) diacak menggunakan suatu kunci enkripsi menjadi "naskah acak yang sulit dibaca" (*ciphertext*) oleh seseorang yang tidak memiliki kunci dekripsi. Ilmu kriptografi juga dapat dikatakan sebagai suatu teknik untuk mengamankan data atau pesan, pengamanan data atau pesan dapat dilakukan dengan menggunakan berbagai algoritma [4]. pada ilmu kriptografi ada dua konsep utama. yaitu enkripsi dan dekripsi. Enkripsi artinya proses membarui data atau informasi atau plaintext sebagai ciphertext sehingga tidak bisa dimengerti sang pihak ketiga. Sedangkan dekripsi ialah proses mengubah data atau info *ciphertext* yg sudah dienkrips ke dalam bentuk semula atau bisa disebut *plaintext*.

Kriptografi bertujuan untuk memberi layanan keamanan (yang juga dinamakan sebagai aspek-aspek keamanan). Untuk dapat menggunakan teknik kriptografi, dibutuhkan sebuah metode salah satunya adalah metode Caesar Cipher [5]. Caesar Cipher merupakan salah satu algoritma tertua, dan merupakan salah satu jenis cipher substitusi yang menyusun huruf dalam plaintext yang digeser dan diganti dengan huruf beberapa posisi tetap di bawah alfabet. Namun beberapa algoritma kriptografi klasik yang telah banyak diketahui secara luas memiliki kelemahan yang dapat diketahui dan dipecahkan oleh *criptanalysis*. Kriptanalisis melakukan pengecekan serangan teks biasa dengan mempelajari pengaruh hasil putaran pasangan teks cipher iteratif.

Caesar Cipher merupakan teknik enkripsi substitusi yang pertama kali dikenal dan paling sederhana, yang ditemukan oleh Julius Caesar. Metode yang digunakan dalam Caesar cipher ini adalah dengan mempertukarkan setiap huruf asli

(*plain text*) dengan huruf lain menggunakan interval 3 sehingga membentuk suatu *cipher text* [6]. *Plaintext* atau bisa diartikan sebagai teks biasa merupakan sebutan untuk pesan yang bisa dimengerti oleh siapapun yang membaca isi pesan tersebut. menurut ahli *plaintext* Merupakan pesan asli sebelum diubah menjadi pesan rahasia. Ciphertext atau bisa diartikan sebagai teks sandi merupakan sebutan untuk pesan yang hanya bisa dimengerti oleh segelintir orang yang mengetahui *Key* dari pesan tersebut. menurut ahli *Ciphertext* Merupakan pesan sandi atau pesan rahasia yang sulit diterjemahkan. Algoritma kriptografi caesar chiper merupakan salah satu metode tertua dalam dunia kriptografi. Oleh karna itu tak jarang apabila metode caesar chiper ini disebut sebagai penentu cikal bakal metode kriptografi lainya sampai era modern saat ini.

Dalam penggunaannya algoritma kriptografi caesar cipher mudah untuk pahami. Dalam pengerjaannya algoritma kriptografi ini hanya melakukan pergeseran urutan karakter sebanyak nilai yang ada [7]. Kriptogram dengan metode Caesar Chiper bekerja dengan cara huruf-huruf dalam plainteks digantikan oleh huruf lainnya dalam posisi tertentu dalam susunan alphabet yang menggeser sebanyak n huruf, jadi huruf chiper pada algoritma Caesar adalah hasil pergeseran sekian huruf dari huruf asli [8].

Proses pengkodean (*ciphering*) dari metode Ceasar Cipher dibentuk oleh dua persamaan [9]. Berikut merupakan persamaan yang digunakan dalam metode Caesar Chiper.

a. Persamaan Untuk Enkripsi

$$(Cx) = (Px) + (k)\ mod\ 26 \quad (1)$$

b. Persamaan Untuk Deskripsi

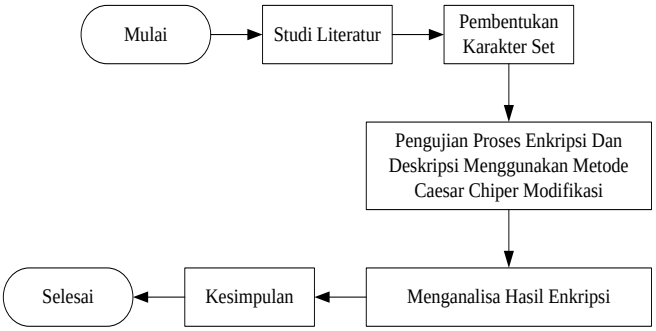
$$(Px) = (Cx) - (k)\ mod\ 26 \quad (2)$$

Dengan (Cx) adalah nilai desimal karakter *ciphertext* (data terenkripsi) ke-*i*, (Px) adalah nilai desimal karakter *plaintext* (data asli) ke-*i*, (k) adalah nilai desimal karakter *key* (kunci) ke-*i* dan $mod\ 26$ adalah modulus dari jumlah karakter alfabet yaitu 26 [10].

Namun seiring berkembangnya jaman, banyak orang yang mulai meninggalkan metode Caesar Chiper karna alasan keamanan. Oleh sebab itu perlu adanya modifikasi terhadap metode Caesar Chiper agar tingkat keamanannya semakin baik. Berdasarkan latar belakang masalah yang ada, yang membedakan penelitian ini dengan penelitian lainnya adalah penelitian ini mengubah karakter set pada algoritma Caesar Chiper menjadi 62 karakter. Hasil penelitian ini untuk melihat apakah perubahan karakter set pada caesar chiper dapat dilakukan dan apa dampaknya secara signifikan terhadap tingkat keamanan data.

II. METODE

Metode penelitian adalah langkah yang dimiliki dan dilakukan oleh peneliti dalam rangka untuk mengumpulkan informasi atau data serta melakukan investigasi pada data yang telah didapatkan tersebut. Metode penelitian memberikan gambaran rancangan penelitian yang meliputi prosedur dan langkah-langkah yang harus ditempuh, sumber data dan langkah apa data-data tersebut diolah dan dianalisis.



Gambar 1 Alur Penelitian

A. Studi Literatur

Pada tahap ini dilakukan peninjauan terhadap jurnal-jurnal maupun hasil penelitian terdahulu sebagai referensi yang diperlukan dalam melakukan penelitian. Ini dilakukan untuk memperoleh informasi terkait dengan operasi Caesar Cipher. Pada studi literatur ini, penulis melakukan pencarian sumber yang dapat menjadi acuan dalam pengerjaan peneltian ini seperti sumber dari internet dan buku-buku. Selain itu juga ada beberapa penelitian terkait pada pustaka dimana peneliti mengambil jurnal yang terkait dengan penelitian, seperti halnya seputar tentang aplikasi kriptografi, dan jurnal-jurnal lain yang terkait.

B. Pembentukan Karakter Set

Pada tahap ini, dibentuk karakter set sesuai dengan apa yang direncanakan dalam modifikasi metode caesar chiper ini. Karakter set ini dibentuk dengan disertakan pula kode dari setiap karakter setnya. Karakter set yang dibentuk berjumlah 62 karakter dengan kode dimulai dari 0 hingga 61. Karakter set selengkapnya dapat dilihat pada tabel di bawah ini.

Tabel 1. Karakter Set

Char	Code	Char	Code
A	0	f	31
B	1	g	32
C	2	h	33
D	3	i	34
E	4	j	35
F	5	k	36
G	6	l	37
H	7	m	38
I	8	n	39
J	9	o	40
K	10	p	41
L	11	q	42
M	12	r	43
N	13	s	44
O	14	t	45
P	15	u	46

Char	Code	Char	Code
Q	16	v	47
R	17	w	48
S	18	x	49
T	19	y	50
U	20	z	51
V	21	0	52
W	22	1	53
X	23	2	54
Y	24	3	55
Z	25	4	56
a	26	5	57
b	27	6	58
c	28	7	59
d	29	8	60
e	30	9	61

C. Pengujian Proses Enkripsi Dan Deskripsi

Pada tahap ini dilakukan proses enksipsi dan deskripsi dengan metode caesar chiper berdasarkan karakter set yang telah dibentuk seperti pada tabel di atas. Dikarenakan karakter set yang digunakan berjumlah 62 karakter, maka rumus caesar chiper dilakukan modifikasi, sehingga menjadi persamaan berikut ini.

a. Persamaan Untuk Enkripsi

$$(Cx) = (Px) + (k)\ mod\ 62 \quad (3)$$

b. Persamaan Untuk Deskripsi

$$(Px) = (Cx) - (k)\ mod\ 62 \quad (4)$$

D. Menganalisa Hasil Enkripsi

Pada tahap ini dilakukan pengamatan dan analisi dari hasil enkripsi yang telah diuji pada langkah sebelumnya. Hal ini bertujuan untuk melihat bagaimana perbedaan hasil chipertext yang dihasilkan. Selain itu pada tahap ini juga dilakukan untuk mengetahui seberapa lebih baiknya tingkat keamanan algoritma Caesar Chiper setelah dilakukan modifikasi terhadap karakter set yang digunakan.

III. HASIL DAN PEMBAHASAN

Pada tahap ini, akan dilakukan proses enkripsi dan deskripsi berdasarkan metode caesar chiper dengan karakter set yang telah dibentuk seperti pada tabel 1. Pada tahap percobaan ini akan dilakukan proses enkripsi pesan dengan pesan atau *plaintext* **Hancurkan** dan kunci yang digunakan adalah **11** geseran.

A. Proses Enkripsi

Untuk melakukan proses enkripsi dengan caesar chiper, terlebih dahulu dilakukan pengkodean terhadap setiap karakter plaintext. Pengkodean harus merujuk pada kode karakter pada Tabel 1. Berikut ini hasil pengkodean selengkapnya.

H	**a**	**n**	**c**	**u**	**r**	**k**	**a**	**n**
7	26	39	28	46	43	36	26	39

Setelah berhasil dilakukan pengkodean dari tiap karakter *plaintext*, selanjutnya dapat dilakukan proses enkripsi berdasrkan kunci 11 geseran dan persamaan (3) yang telah ditetapkan. Berikut ini hasil enkripsi selengkapnya.

H = 7
$$(Cx) = (Px) + (k) mod\ 62 = (7 + 11) mod\ 62 = (18) mod\ 62 = 18$$

a = 26
$$(Cx) = (Px) + (k) mod\ 62 = (26 + 11) mod\ 62 = (37) mod\ 62 = 37$$

n = 39
$$(Cx) = (Px) + (k) mod\ 62 = (39 + 11) mod\ 62 = (50) mod\ 62 = 50$$

c = 28
$$(Cx) = (Px) + (k) mod\ 62 = (28 + 11) mod\ 62 = (39) mod\ 62 = 39$$

u = 46
$$(Cx) = (Px) + (k) mod\ 62 = (46 + 11) mod\ 62 = (57) mod\ 62 = 57$$

r = 43
$$(Cx) = (Px) + (k) mod\ 62 = (43 + 11) mod\ 62 = (54) mod\ 62 = 54$$

k = 36
$$(Cx) = (Px) + (k) mod\ 62 = (36 + 11) mod\ 62 = (47) mod\ 62 = 47$$

a = 26
$$(Cx) = (Px) + (k) mod\ 62 = (26 + 11) mod\ 62 = (37) mod\ 62 = 37$$

n = 39
$$(Cx) = (Px) + (k) mod\ 62 = (39 + 11) mod\ 62 = (50) mod\ 62 = 50$$

Berdasarkan hasil perhitungan menggunakan persamaan 3 sebagai enkripsi, didapatkan chiper text sebagai berikut.

18	37	50	39	57	54	47	37	50
S	**l**	**y**	**n**	**5**	**2**	**v**	**l**	**y**

Hasil enkripsi metode caesar chiper dengan modifikasi 62 karakter set dari plaintext **Hancurkan** adalah **Slyn52vly**.

B. Proses Deskripsi

Setelah pesan berhasil di enskripsi, tentunya penerima pesan tersebut harus mendeskripsikan kembali pesan agar dapat dibaca. Untuk melakukan deskripsi pesan dapat dilakukan dengan mengacu pada persamaan (4). Berikut adalah hasil dari proses deskripsi selengkapnya.

S = 18

$$(Px) = (Cx) - (k) mod\ 62$$
$$= (18 - 11) mod\ 62$$
$$= (7) mod\ 62 = 7$$

l = 37

$$(Px) = (Cx) - (k) mod\ 62$$
$$= (37 - 11) mod\ 62$$
$$= (26) mod\ 62 = 26$$

y = 50

$$(Px) = (Cx) - (k) mod\ 62$$
$$= (50 - 11) mod\ 62$$
$$= (39) mod\ 62 = 39$$

n = 39

$$(Px) = (Cx) - (k) mod\ 62$$
$$= (39 - 11) mod\ 62$$
$$= (28) mod\ 62 = 28$$

5 = 57

$$(Px) = (Cx) - (k) mod\ 62$$
$$= (57 - 11) mod\ 62$$
$$= (46) mod\ 62 = 46$$

2 = 54

$$(Px) = (Cx) - (k) mod\ 62$$
$$= (54 - 11) mod\ 62$$
$$= (43) mod\ 62 = 43$$

v = 47

$$(Px) = (Cx) - (k) mod\ 62$$
$$= (47 - 11) mod\ 62$$
$$= (36) mod\ 62 = 36$$

l = 37

$$(Px) = (Cx) - (k) mod\ 62$$
$$= (37 - 11) mod\ 62$$
$$= (26) mod\ 62 = 26$$

y = 50

$$(Px) = (Cx) - (k) mod\ 62$$
$$= (50 - 11) mod\ 62$$
$$= (39) mod\ 62 = 39$$

Berdasarkan hasil deskripsi yang dilakukan di atas, *chipertext* berhasil di *decrypt* kembali ke *plaintext* sebagai berikut.

7	26	39	28	46	43	36	26	39
H	**a**	**n**	**c**	**u**	**r**	**k**	**a**	**n**

IV. KESIMPULAN

Berdasarkan hasil uji yang telah dilakukan dengan modifikasi 62 karakter set pada metode caesar chiper dapat disimpulkan bahwa modifikasi berhasil dilakukan. Modifikasi ini juga dapat meningkatkan keamanan metode enkripsi caesar chiper. Selain itu, dengan dilakukanya modifikasi ini menjadikan hasil enkripsi atau chipertext lebih bervariasi. Diharapkan ke depannya dapat dilakukan modifikasi-modifikasi tambahan agar metode caesar chiper dapat lebih baik tingkat ke amanannya.

UCAPAN TERIMA KASIH

Diucapkan terima kasih kepada semua pihak yang terlibat dalam membantu penulisan jurnal ini hingga dapat dipublikasi.

DAFTAR PUSTAKA

[1] D. Purnamasari and H. Prasetyani, "Analisis Performansi Kriptografi Berbasis Algoritma Caesar Cipher dan Rail Fence Cipher pada Tembang Macapat," pp. 1–8.

[2] D. Nataliana, F. Hadiatna, and A. Fauzi, "Rancang Bangun Sistem Keamanan RFID Tag menggunakan Metode Caesar Cipher pada Sistem Pembayaran Elektronik," vol. 7, no. 3, pp. 427–441, 2019.

[3] B. Web, S. Kasus, S. Tangerang, N. Chafid, and H. Soffiana, "IMPELEMENTASI ALGORITMA KRIPTOGRAFI KLASIK CAESAR UNTUK RANCANG BANGUN APLIKASI E-VOTING," vol. 6, 2022.

[4] M. R. Zulfikar and S. Mulyati, "PENERAPAN KRIPTOGRAFI CAESAR CIPHER DAN VIGENERE CIPHER UNTUK MENGAMANKAN DATABASE BARANG BELTING PADA PT . MULTI MITRA USAHA BERSAMA APPLICATION OF CAESAR CIPHER AND VIGENERE CIPHER METHODS TO SECURE DATABASE OF BELTINGS AT PT MULTI," no. September, pp. 402–410, 2022.

[5] I. W. Utomo, R. Latifah, and D. Risanty, "APLIKASI KRIPTOGRAFI BERBASIS ANDROID MENGGUNAKAN ALGORITMA CAESAR CIPHER DAN VIGENERE CIPHER."

[6] D. P. Manurung *et al.*, "Perbandingan Metode Stream Dengan Metode Caesar Cipher Terhadap Pengiriman Pesan Pada Jaringan Wireless," vol. 1, no. 1, pp. 332–342.

[7] Y. D. Putri *et al.*, "PENERAPAN KRIPTOGRAFI CAESAR CIPHER PADA FITUR CHATTING SISTEM INFORMASI FREELANCE APPLICATION OF CAESAR CIPHER CRIPTOGRAPHY IN FREELANCE," vol. 2, no. 2, pp. 87–94, 2019.

[8] H. D. Purnomo, I. Sembiring, J. D. No, K. Sidorejo, K. Salatiga, and J. Tengah, "Modifikasi Algoritma Caesar Cipher pada Kode ASCII dalam Meningkatkan Keamanan Pesan Teks," vol. 2, no. 1, 2022.

[9] N. Oper, S. Balafi, and T. F. Al-Khaliq.Z, "MODIFIKASI ALGORITMA KRIPTOGRAFI CAESAR CIPHER MENJADI ALGORITMA KRIPTOGRAFI ASIMETRIS DENGAN METODE AGILE," *JINTEKS (Jurnal Inform. Teknol. dan Sains)*, vol. 4, no. 3, pp. 179–184, 2022.

[10] K. B. Ziliwu and A. Maslan, "IMPLEMENTASI CAESAR CIPHER PADA ALGORITMA KRIPTOGRAFI KLASIK DALAM PENYANDIAN PESAN," *J. Comasie*, vol. 02, no. 07, pp. 117–126, 2022.