KETIK : Jurnal Informatika
ISSN: 3026 - 183X (Media Online)
Vol. 01, No. 03, Januari 2024 Hal. 95-101
Faatuatua Media Karya
https://jurnal.faatuatua.com/index.php/KETIK

Modifikasi Algoritma Caesar Cipher Menggunakan Linear Congruent Method Untuk Mengamankan Data

Surya Darma Nasution

Universitas Budi Darma, Indonesia, email: darmashadow@gmail.com

Info Artikel

Diajukan: 20-01-2024
Diterima: 21-01-2024
Diterbitkan: 30-01-2024

Kata Kunci:
Caesar Cipher; Linear Congruent Method; Kriptografi; Pengamanan Data; Modifikasi Algoritma

Keywords:
Caesar Cipher; Linear Congruent Method; Cryptography; Data Security; Algorithm Modification

Abstrak

Perkembangan teknologi digital meningkatkan kebutuhan untuk melindungi data. Algoritma kriptografi seperti Caesar Cipher menjadi solusi, namun Caesar Cipher klasik rentan terhadap serangan brute force. Penelitian ini memodifikasi Caesar Cipher dengan menggabungkannya dengan algoritma pembangkit bilangan acak Linear Congruent Method (LCM). Modifikasi ini meningkatkan keamanan dengan menambahkan proses enkripsi Caesar Cipher dua lapis. Lapis pertama menggunakan Caesar Cipher konvensional dan lapis kedua menggunakan Caesar Cipher dengan kunci yang dihasilkan oleh LCM. Hasil penelitian menunjukkan bahwa Caesar Cipher yang dimodifikasi dengan LCM lebih aman dibandingkan Caesar Cipher konvensional. Modifikasi ini meningkatkan kompleksitas proses dekripsi dan membuat serangan brute force menjadi lebih sulit.

Abstract

The development of digital technology increases the need to protect data. Cryptographic algorithms such as the Caesar Cipher are a solution, but the classic Caesar Cipher is vulnerable to brute force attacks. This research modifies the Caesar Cipher by combining it with the Linear Congruent Method (LCM) random number generator algorithm. This modification improves security by adding a two-layer Caesar Cipher encryption process. The first layer uses conventional Caesar Cipher and the second layer uses Caesar Cipher with keys generated by LCM. The research results show that the Caesar Cipher modified with LCM is safer than the conventional Caesar Cipher. This modification increases the complexity of the decryption process and makes brute force attacks more difficult.

1. PENDAHULUAN

Di era teknologi digital dimana informasi menjadi semakin mudah diakses dan rentan terhadap serangan siber, perlindungan data menjadi semakin penting. Salah satu cara umum untuk melindungi data adalah dengan menggunakan algoritma kriptografi. Banyak algoritma kriptografi yang ada saat ini, baik itu yang jenisnya kriptografi klasik ataupun kriptografi modern. Walaupun sudah banyak algoritma kriptografi yang tercipta tetapi perkembangan teknologi juga memiliki dampak pada keamanan data secara keseluruhan hal ini karena seorang kriptanalis juga terus mengembangkan metode baru untuk menembus sistem keamanan, sehingga perlu ada upaya terus-menerus untuk meningkatkan keamanan data agar tetap dapat menanggapi perkembangan tersebut. Untuk itu beberapa peneliti telah melakukan inovasi dengan memodifikasi algoritma kriptografi sehingga dapat menigkatkan kemanan pada penggunaan algoritma tersebut.

Caesar Cipher adalah salah satu algoritma enkripsi klasik yang sederhana dan mudah dimengerti, tetapi rentan terhadap serangan brute force karena kunci enkripsinya memiliki sedikit kemungkinan. Walaupun algoritma caesar cipher ini merupakan algoritma yang paling lama dan jarang digunakan, tetapi beberapa peneliti ada yang melakukan penelitian untuk memodifikasi algoritma tersebut. Modifikasi tersebut dilakukan untuk mengecoh kriptanalis karena kriptanalis tidak akan mengira bahwa algoritma caesar cipher masih digunakan dan bahkan dimodifikasi. Salah satu upaya

untuk meningkatkan keamanan dari algoritma Caesar Cipher adalah dengan menggabungkannya dengan algoritma kriptografi modern ataupun menggunakan algoritma pembangkit bilangan acak seperti Linear Congruent Method. Metode ini menambahkan lapisan keamanan tambahan dengan melakukan pengacakan dari hasil proses enkripsi yang dilakukan dengan caesar cipher.

Beberapa penelitian yang memodifikasi algoritma caesar cipher telah dilakukan, seperti yang dilakukan oleh Rizky Rinaldi, dimana pada penelitiannya mengenai analisis terhadap sistem keamanan yang menggunakan algoritma caesar cipher yang telah di modifikasi. Modifikasi yang dilakukan yaitu karakter yang dapat dienkripsi sebanyak 62 karakter terdiri dari huruf besar, huruf kecil dan juga angka. Hasil penelitian tersebut menyatakan bahwa proses modifikasi tersebut berhasil meningkatkan keamanan terhadap algoritma caesar cipher [1]. Penelitian serupa juga pernah dilakukan oleh Andy, dkk dengan mengkombinasikan dengan transposisi diagonal serta menggunakan tabel ASCII untuk karakternya, dan hal tersebut juga dapat mengamankan data menjadi lebih baik lagi dibanding hanya menggunakan caesar cipher biasa [2]. Modifikasi dengan kode ASCII juga dilakukan oleh Mira, dkk [3] dan perbedaan dengan yang dilakukan oleh Andy adalah pada penelitian andy menerapkan transposisi diagonal sebagai tambahan untuk kombinasinya sedangkan pada penelitian Mira tidak ada menggunakan algoritma lainnya

Modifikasi algoritma caesar cipher juga dilakukan oleh Rudolf dan Frangky yaitu dengan menambahkan kunci dalam melakukan proses enkripsi. Hasil dari penelitian tersebut menyatakan bahwa algoritma caesar cipher yang telah dimodifikasi dengan menambahkan kunci dapat meningkatkan keamanan[4]. Modifikasi lainnya yang menggunakan caesar cipher juga dilakukan oleh Irma, dkk yang algoritma tersebut kedalam bentuk sandi morse dan hasil dari penelitian tersebut menyatakan bahwa tingkat keamanannya menjadi lebih baik dari sebelumnya [5].

Dari penelitian-penelitian yang sudah pernah dilakukan tersebut, yang digunakan adalah algoritma caesar cipher karena langkah-langkah enkripsinya yang sangat mudah dipahami. Perbedaan penelitian ini dibanding dengan penelitian-penelitian sebelumnya adalah belum ada yang melakukan modifikasi algoritma caesar cipher menggunakan algoritma pembangkit bilangan acak seperti linear congruent method (LCM).

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi adalah seni dan ilmu yang bertujuan untuk menjaga kerahasiaan pesan dengan mengubahnya menjadi bentuk yang sulit dipahami [6]. Dalam bidang kriptografi, terdapat dua konsep utama yang dikenal sebagai enkripsi dan dekripsi. Enkripsi melibatkan proses mengubah informasi atau pesan menjadi bentuk yang sulit dikenali menggunakan algoritma khusus. Sebaliknya, dekripsi adalah proses mengembalikan pesan tersembunyi tersebut ke dalam bentuk aslinya. Pesan yang belum dienkripsi disebut sebagai plaintext, sedangkan setelah melalui proses penyandian, pesan tersebut menjadi ciphertext. Proses mengubah plaintext menjadi ciphertext disebut enkripsi, sementara proses mengembalikan ciphertext ke plaintext disebut dekripsi [7].

2.2 Algoritma Caesar Cipher

Caesar Cipher merupakan salah satu algoritma substitusi klasik tertua yang masih terkenal hingga saat ini. Algoritma ini tidak membutuhkan kunci untuk melakukan enkripsi, dan keamanannya bergantung pada kerahasiaan algoritma itu sendiri. Namun, seiring berjalannya waktu, Caesar Cipher mulai ditinggalkan karena dianggap kurang aman untuk digunakan dalam konteks zaman sekarang. Oleh karena itu, diperlukan modifikasi dengan memadukan beberapa metode dari algoritma klasik lain, seperti transposisi, untuk meningkatkan keamanan dan menguatkan hasil enkripsi agar lebih sulit ditembus menggunakan teknik brute force [8]. Secara umum, enkripsi dan dekripsi pada Caesar Cipher dilakukan dengan menggeser setiap karakter sebanyak tiga langkah, atau dapat menggunakan rumus berikut ini [9] :

Enkripsi *:*

$$C = E(k, p) = (p + k) \bmod 26 \quad (1)$$

Dekripsi :

$$p = D(k, C) = (C - k) \bmod 26 \quad (2)$$

2.3 Linear Congruent Method (LCM)

Linear Congruent Method (LCM) merupakan salah satu teknik yang digunakan untuk menghasilkan bilangan acak semu (Pseudorandom Number Generators). Dikembangkan oleh D.H.

KETIK: JURNAL INFORMATIKA
ISSN: 3026-183X (Media Online)
Vol. 01, No. 03, Januari 2024 Hal. 95-101

Lehmer pada tahun 1949, LCM menjadi populer karena kemudahannya dalam implementasi komputasional serta kecepatan eksekusinya yang relatif tinggi [10]. Rumus dari Linear Congruent Method adalah sebagai berikut:

$$Xn+1 = (a\ (\ Xn)+c) \bmod m \quad \text{..... (3)}$$

Keterangan :

Xn+1 = Bilangan acak yang akan dicari
a = Faktor Pengali
Xn = Bilangan acak sebelumnya
c = Increment
m = Modulus

3. HASIL DAN ANALISIS

Pada bagian hasil dan analisis ini akan dicoba untuk mengamankan data teks, dan yang menjadi plainteksnya adalah “AYO KITA CULIK DIA”. Untuk proses analisis kita bagi menjadi 2 (dua) bagian, yaitu menggunakan caesar cipher konvensional dan menggunakan caesar cipher yang di modifikasi.

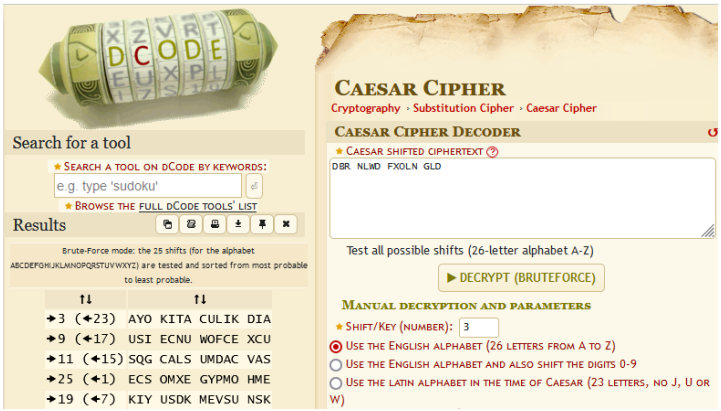
3.1 Pengamanan Menggunakan Caesar Cipher Konvensional

Penggunaan caesar cipher konvensional yaitu dengan menggeser sebanyak 3 karakter, disini kita mengabaikan penggunaan spasi. Hasil yang diperoleh dari plainteks yang ada yaitu:

A	Y	O		K	I	T	A		C	U	L	I	K		D	I	A
D	B	R		N	L	W	D		F	X	O	L	N		G	L	D

Gambar 1. Hasil Proses Enkripsi Dengan Pergeseran 3 karakter

Dapat dilihat pada gambar 1, dimana cipherteks yang dihasilkan yaitu “DBR NLWD FXOLN GLD”. Berikutnya kita akan melakukan pengujian untuk menjebol keamanan pada caesar cipher menggunakan tools yang tersedia melalui halaman web https://www.dcode.fr/caesar-cipher dan hasilnya dapat dilihat pada gambar 2 berikut ini:



Gambar 2. Hasil Uji Coba Keamanan Pada Caesar Cipher Konvensional

Pada gambar 2 tampak bahwa hasil pada urutan pertama dari cipherteks yang dimasukkan adalah “AYO KITA CULIK DIA” hal ini menunjukan bahwa algoritma caesar cipher yang konvensional sangat mudah untuk dipecahkan.

3.2 Pengamanan Menggunakan Caesar Cipher Yang Dimodifikasi

Modifikasi yang dilakukan pada penelitian ini yaitu dengan melakukan pengacakan menggunakan linear congruent method. Jadi pada proses pertama tetap melakukan proses enkripsi meggunakan caesar cipher yang konvensional yaitu “DBR NLWD FXOLN GLD”. Berikutnya hasil dari proses enkripsi tersebutlah yang akan dilakukan pengacakan sehingga memperoleh hasil yang berbeda. Proses pembangkitan bilangan acaknya menggunakan variabel sebagai berikut :

a = 1 (Ditetapkan)
c = 89 (Ditetapkan)
m = 26 (Ditetapkan dari jumlah huruf alfabet).

X0 = 18 (Berdasarkan jumlah karakter pada hasil cipherteks konvensional termasuk spasi)

Berikutnya dari variabel tersebut akan kita bangkitkan bilangan acak sebanyak 15 bilangan acak yang diambil dari jumlah huruf (tanpa spasi) pada hasil cipherteks konvensional. Untuk perhitungannya sebagai berikut :

X1 = (1 x4+89) mod 26
X1 = 107 Mod 26
X1 = 3

X2 = (1x3+89) mod 26
X2 = 92 Mod 26
X2 = 14

X3 = (1x14+89) mod 26
X3 = 103 Mod 26
X3 = 25

X4 = (1x25+89) mod 26
X4 = 114 Mod 26
X4 = 10

X5 = (1x10+89) mod 26
X5 = 99 Mod 26
X5 = 21

X6 = (1x21+89) mod 26
X6 = 110 Mod 26
X6 = 6

X7 = (1x6+89) mod 26
X7 = 95 Mod 26
X7 = 17

X8 = (1x17+89) mod 26
X8 = 106 Mod 26
X8 = 2
X9 = (1x2+89) mod 26
X9 = 91 Mod 26
X9 = 13

X10 = (1x13+89) mod 26
X10 = 102 Mod 26
X10 = 24

X11 = (1x24+89) mod 26
X11 = 113 Mod 26
X11 = 9

X12 = (1x9+89) mod 26
X12 = 98 Mod 26
X12 = 20

X13 = (1x20+89) mod 26
X13 = 109 Mod 26
X13 = 5
X14 = (1x5+89) mod 26
X14 = 94 Mod 26
X14 = 16

X15 = (1x16+89) mod 26

X15 = 105 Mod 26
X15 = 1

Langkah berikutnya melakukan enkripsi kembali menggunakan algoritma caesar cipher dengan pergeseran kunci sejumlah hasil bilangan acak yang diperoleh menggunakan rumus caesar cipher yang ada pada persamaan (1) dimana yang menjadi kunci adalah hasil bilangan acak dan yang menjadi plainteks disini adalah cipherteks pada caesar cipher konvensional dan nilai angkanya berdasarkan tabel 1 berikut ini :

Tabel 1. Karakter dan Indeks Proses Pengacakan

Karakter	Indeks
A	0
B	1
C	2
D	3
E	4
F	5
G	6

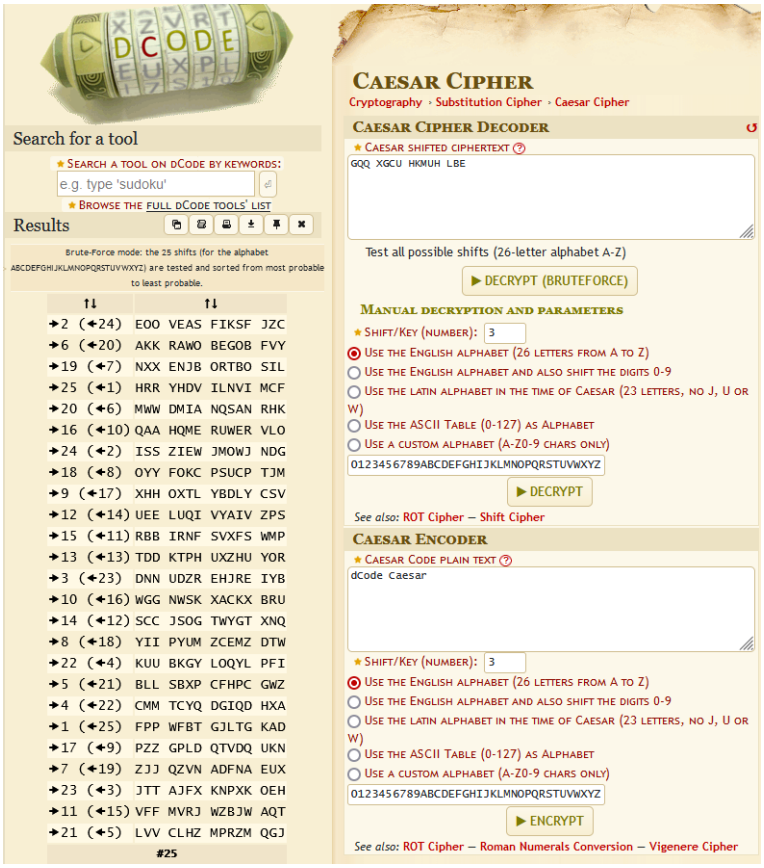
Karakter	Indeks
H	7
I	8
J	9
K	10
L	11
M	12
N	13

Karakter	Indeks
O	14
P	15
Q	16
R	17
S	18
T	19
U	20

Karakter	Indeks
V	21
W	22
X	23
Y	24
Z	25

Proses Enkripsi:
C1 = E (k=3, p="D") = (3 + 3) mod 26 = 6 (G)
C2 = E (k=14, p="B") = (2 + 14) mod 26 = 16 (Q)
C3 = E (k=25, p="R") = (17 + 25) mod 26 = 16 (Q)
C4 = E (k=10, p="N") = (13 + 10) mod 26 = 23 (X)
C5 = E (k=21, p="L") = (11 + 21) mod 26 = 6 (G)
C6 = E (k=6, p="W") = (22 + 6) mod 26 = 2 (C)
C7 = E (k=17, p="D") = (3 + 17) mod 26 = 20 (U)
C8 = E (k=2, p="F") = (5 + 2) mod 26 = 7 (H)
C9 = E (k=13, p="X") = (23 + 13) mod 26 = 10 (K)
C10 = E (k=24, p="O") = (14 + 24) mod 26 = 12 (M)
C11 = E (k=9, p="L") = (11 + 9) mod 26 = 20 (U)
C12 = E (k=20, p="N") = (13 + 20) mod 26 = 7 (H)
C13 = E (k=5, p="G") = (6 + 5) mod 26 = 11 (L)
C14 = E (k=16, p="L") = (11 + 16) mod 26 = 1 (B)
C15 = E (k=1, p="D") = (3 + 1) mod 26 = 4 (E)

Dari hasil proses pembangkitan bilangan acak dan setelah dirubah menjadi karakter berdasarkan indeksnya maka cipherteks yang dihasilkan yaitu “GQQ XGCU HKMUH LBE”. Berikutnya kita akan melakukan pengujian kembali untuk menjebol keamanan pada caesar cipher dan hasilnya dapat dilihat pada gambar 3 berikut ini:



Gambar 3. Hasil Uji Coba Keamanan Pada Caesar Cipher Yang Telah Dimodifikasi

Pada gambar 3 tampak bahwa hasil dekripsi yang dilakukan tidak dapat memecahkan atau merubah kembali menjadi plainteksnya dan dari 25 hasil teratas sama sekali menjadi kalimat yang tidak memiliki arti sehingga bisa dikatakan bahwa sistem keamanannya menjadi lebih baik.

Untuk proses mengembalikan ke plainteks, maka langkah yang harus diambil adalah :

1. Melakukan pembangkitan bilangan acak, karena jumlah karakternya sama yaitu 18 (X0) dan untuk nilai variabel a,c, dan m karena nilainya sudah ditetapkan maka tidak ada perubahan juga, sehingga hasil pembangkitan bilangan acaknya juga sama.
2. Melakukan proses dekripsi dari chiperteks hasil modifikasi dengan kunci yang didapat dari hasil pembangkitan bilangan acak.
3. Melakukan proses dekripsi menggunakan langkah dekripsi pada caesar cipher konvensional yaitu pergeseran mundur sebanyak 3.

4. KESIMPULAN

Proses modifikasi berhasil dilakukan dengan melakukan 2 lapis enkripsi dimana lapis pertama melakukan proses enkripsi menggunakan caesar cipher secara konvensional, kemudian dilakukan proses membangkitkan bilangan acak menggunakan linear congruent method dan hasil pembangkitan bilangan acak tersebut menjadi kunci pada proses enkripsi lagi menggunakan caesar cipher pada lapis ke 2. Hasil pengujian dapat membuktikan bahwa caesar cipher yang dimodifikasi lebih aman daripada caesar cipher yang konvensional.

REFERENSI

[1] R. Rinaldi, "Analisis Keamanan Modifikasi Metode Caesar Chiper Dalam Teknik Enkripsi Dan Deskripsi," 2022.

[2] A. Aprianto and E. Irawadi Alwi, "Implementasi Algoritma Caesar Cipher Dengan Kombinasi Transposisi Diagonal Untuk Enkripsi Dekripsi Menggunakan Tabel ASCII INFORMASI ARTIKEL ABSTRAK," *Buletin Sistem Informasi dan Teknologi Islam*, vol. 3, no. 3, pp. 238–247, 2022.

[3] M. Mira, H. Dwi Purnomo, and I. Sembiring, "Modifikasi Algoritma Caesar Cipher pada Kode ASCII dalam Meningkatkan Keamanan Pesan Teks," *JIFOTECH (JOURNAL OF INFORMATION TECHNOLOGY*, vol. 2, no. 1, 2022.

[4] R. Sinaga and F. Frangky, "Modification of the Caesar Cipher Algorithm by Adding a Key for Increased Security," *CSRID Journal*, vol. 15, no. 2, p. 156, 2023, doi: 10.22303/csrid.15.2.2023.156-166.

[5] I. Darmayanti *et al*., "Penerapan Keamanan Pesan Teks Menggunakan Modifikasi Algoritma Caisar Chiper Kedalam Bentuk Sandi Morse," *Jurnal IT CIDA*, vol. 4, no. 1, 2018.

[6] M. Lailatun Najah and K. Agung Santoso, "KOMBINASI CAESAR CIPHER DAN REVERSE CIPHER BERDASARKAN CIPHER BLOCK CHAINING (Combination of Caesar Cipher and Reverse Cipher Based on Cipher Block Chaining)," *Majalah Ilmiah Matematika dan Statistika*, vol. 21, pp. 101–106, 2021, [Online]. Available: http://jurnal.ac.is/index.php/MIMS/indexISSN1441-6669

[7] D. Cahyo Yudiantoro, "MODIFIKASI METODE KRIPTOGRAFI CAESAR CIPHER MENGGUNAKAN DERET SIMBOL PADA KEYBOARD SMARTPHONE," *Jurnal Teknologi Informasi*, vol. 4, no. 2, 2020.

[8] A. Syarif, "MODIFIKASI CAESAR CIPHER DENGAN PERMUTASI, TRANSPOSISI, BINARY, GERBANG LOGIKA, ASCII DAN HEXA," *Jurnal Teknologi Informasi*, vol. 4, no. 2, 2020.

[9] N. C. Safitri and A. Prihanto, "Modifikasi Cipher Kriptografi Caesar yang Dapat Dibaca dengan Menggunakan Kamus Bahasa Indonesia," 2019.

[10] F. Fauseh, R. W. Saleh Insani, and Y. Brianorman, "Implementasi Linear Congruent Method Untuk Pengacakan Soal Pada Aplikasi Bank Soal Berbasis Website," *Digital Intelligence*, vol. 2, no. 1, p. 47, Nov. 2021, doi: 10.29406/diligent.v2i1.2741.