Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 2, Issue 2, 2024 pp. 31-36 http://urj.uin-malang.ac.id/index.php/mij/index

Kombinasi algoritma *Caesar Cipher* dan algoritma *Affine Cipher*

Aam Alfain Hidayatullah
Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim Malang
e-mail: 200601110034@student.uin-malang.ac.id

Kata Kunci:
caesar cipher; affine cipher; kriptografi; keamanan pesan; kombinasi

Keywords:
caesar cipher; *affine cipher*; cryptography; message security; combination

A B S T R A K

Keamanan data dalam komunikasi digital merupakan aspek penting di era informasi saat ini. Kriptografi telah lama digunakan sebagai solusi untuk melindungi privasi data melalui penggunaan algoritma enkripsi yang kompleks. Dua algoritma kriptografi klasik yang terbukti efektif adalah Caesar Cipher dan Affine Cipher. Namun keduanya mempunyai kelemahan masing-masing. Penelitian ini mengusulkan pendekatan baru dengan menggabungkan kekuatan Caesar Cipher dan Affine Cipher agar keamanan sebuah pesan menjadi lebih kuat. Dalam pendekatan ini, Caesar cipher digunakan sebagai tahap pertama proses enkripsi, dilanjutkan dengan penerapan affine cipher sebagai tahap kedua. Tahap pertama dengan Caesar Cipher bertujuan untuk mengacak arketipe teks terbuka, sedangkan tahap kedua dengan Affine Cipher memberikan transformasi matematis tambahan pada data terenkripsi.

A B S T R A C T

Data security in digital communications is an essential aspect in today's information age. Cryptography has long been used as a solution to protect the privacy of data through the use of complex encryption algorithms. Two classical cryptographic algorithms that have proven to be effective are the *Caesar cipher* and the *Affine cipher*. However, both have their own weaknesses. This research proposes a new approach by combining the strengths of *Caesar cipher* and *Affine cipher* so that the security of a message becomes stronger. In this approach, the *Caesar cipher* is used as the first stage of the encryption process, followed by the application of the fine cipher as the second stage. The first stage with *Caesar cipher* aims to scramble open text archetypes, while the second stage with *Affine cipher* provides additional mathematical transformations on encrypted data.

Pendahuluan

Kemajuan jaringan komputer saat ini memungkinkan kita berkomunikasi dan mengirim pesan melalui infrastruktur jaringan. Salah satu cara komunikasi yang umum adalah melalui tulisan atau teks. Melalui bentuk tulisan ini, kita dapat menyampaikan berbagai informasi, termasuk yang bersifat rahasia atau pribadi.

Informasi sangat berharga dalam kehidupan sehari-hari. Semakin banyak informasi yang ingin Anda ingat, semakin sulit untuk melakukannya. Banyak orang kemudian menyimpan informasi tersebut sebagai catatan di kertas atau buku harian. Informasi yang tertulis pada catatan seringkali berkaitan dengan sesuatu yang penting

This is an open access article under the CC BY-NC-SA license.
Copyright © 2023 by Author. Published by Universitas Islam Negeri Maulana Malik Ibrahim Malang.

bagi penulisnya. Menyimpan informasi dalam bentuk catatan dinilai efektif untuk kebutuhan hafalan. Masalahnya cara ini masih mempunyai kekurangan atau kelemahan. Menyimpan informasi tulisan tangan. Kertas catatan bisa rusak, hilang atau bahkan hancur. Orang lain mempunyai kemampuan untuk mengubahnya. Penyebabnya, masyarakat belum sadar akan pentingnya menjaga kerahasiaan informasi.

Kerahasiaan dan integritas pesan dalam komunikasi penting dalam berbagai konteks, baik dalam kehidupan profesional maupun sosial. Solusi kriptografi menjadi penting dalam menjaga keamanan data dengan mengubah pesan menjadi bentuk terenkripsi. Di era digital, keamanan data menjadi hal yang penting, terutama dengan kemajuan komputasi dan potensi ancaman terhadap data digital. Oleh karena itu, penerapan algoritma enkripsi merupakan pendekatan penting untuk meningkatkan perlindungan data dan pesan yang dikirim.

Kriptografi adalah teknik yang digunakan untuk melindungi pesan atau informasi dengan menyamarkan isi aslinya, sehingga hanya orang yang memiliki akses saja yang dapat membaca dan memahaminya. Awalnya, pesan atau teks asli disebut sebagai teks biasa. Setelah melalui proses, pesan tersebut disebut ciphertext. Proses mengubah teks biasa menjadi teks tersandi disebut enkripsi, sedangkan mengubah teks tersandi kembali menjadi teks biasa disebut dekripsi.

Oleh karena itu, penulis tertarik untuk menggabungkan metode *Caesar cipher* dengan *Affine cipher* guna meningkatkan tingkat keamanan pesan. *Affine cipher* merupakan pengembangan dari teknik *Caesar cipher* yang melibatkan perkalian pesan asli (*plain text*) dengan bilangan bulat tertentu, diikuti dengan penambahan pergeseran lain (berupa bilangan bulat juga), yang dilakukan melalui operasi kongruensi.

Pembahasan

Caesar Cipher

Metode penyandian *Caesar cipher* digunakan oleh Julius Caesar untuk berkomunikasi dengan komandannya dalam bentuk pesan terenkripsi. Dalam bidang kriptografi, *Caesar cipher* juga dikenal dengan beberapa istilah lain seperti shift cipher, caesar code, atau caesar shift. Teknik ini merupakan salah satu metode enkripsi paling sederhana namun masih banyak digunakan. Sandi Caesar termasuk dalam kategori sandi substitusi, yang mana setiap huruf pada teks awal diganti dengan huruf lain yang posisinya tetap sesuai urutan abjad. Misal ada pergeseran 3 maka huruf A berubah menjadi D, B menjadi E, dan seterusnya.

Proses enkripsi pada *Caesar cipher* dapat direpresentasikan dengan menggunakan operasi aritmatika modulo 26 setelah setiap huruf diubah menjadi nilai numerik, dimana A direpresentasikan sebagai 0, B sebagai 1, dan seterusnya hingga Z sebagai 25. Dengan demikian, enkripsi *Caesar cipher* rumusnya dapat dijelaskan sebagai berikut:

$$c = \mathrm{E}(p) = (p + k) \bmod n$$

Dan rumus dekripsinya :

$$p = D(c) = (c - k) \bmod n$$

Keterangan :

1. *n* adalah jumlah alfabet
2. *k* adalah kunci rahasia (jumlah pergeseran)
3. *c* adalah ciphertext
4. *p* adalah plaintext

Kekurangan dari *Caesar cipher* adalah kemampuannya untuk dibobol melalui serangan brute force, yaitu dengan menguji berbagai kemungkinan untuk menemukan kunci yang tepat. Cara ini juga bisa menggunakan pencarian kunci, karena jumlah kemungkinan kunci terbatas (hanya 26 kunci).

Affine Cipher

Affine cipher merupakan pengembangan dari *Caesar cipher* yang bertujuan untuk mengurangi kemungkinan analisis berdasarkan frekuensi huruf. Pada *Caesar cipher* digunakan transformasi shift yang rentan terhadap pendekatan analisis frekuensi. Namun untuk mengatasinya, *affine cipher* menggunakan transformasi yang lebih kompleks menggunakan operasi matematika, tepatnya transformasi linier. Dengan demikian, enkripsi *Affine cipher* rumusnya dapat dijelaskan sebagai berikut:

$$C \equiv mP + b \pmod{n}$$

Dan rumus dekripsinya :

$$P \equiv m^{-1} (C - b) \pmod{n}$$

Keterangan :

1. *n* adalah ukuran alfabet
2. *m* bilangan bulat yang relatif prima dengan *n*
3. *b* adalah jumlah pergeseran

Kunci pada metode affine cipher terdiri dari dua variabel yaitu m dan b. Agar nilai m memiliki invers m-1, nilai tersebut harus mematuhi ketentuan bahwa gcd(m, n) harus sama dengan 1.

Kombinasi Caesar cipher dan Affine cipher

Dalam metode enkripsi yang dijelaskan di atas, tiga bilangan bulat (*k*, *m*, dan *b*) diperlukan untuk mengamankan sebuah pesan. Angka *k* digunakan untuk mengatur besarnya pergeseran pada metode *Caesar cipher*, sedangkan dua angka lainnya yaitu *m* dan *b* digunakan pada metode *Affine cipher.*

Berikut cara merahasiakan pesan (Enkripsi) adalah sebagai berikut:

1. Enkripsi *caesar cipher*

   Contoh: Terdapat pesan plainteks SEMANGAT BELAJAR dengan kunci pergeseran atau *k* = 13 huruf ke kanan.

   Misalkan A = 0, B = 1, C = 2, ... Z = 25

   Plainteks: SEMANGAT BELAJAR

   a. p_1 = 'S' = 18 -> c_1 = E(18) = (18+13) mod 26 = 5 = 'F'

   b. p_2 = 'E' = 4 -> c_2 = E(4) = (4+13) mod 26 = 17 = 'R'

   c. p_3 = 'M' = 12 -> c_3 = E(12) = (12+13) mod 26 = 25 = 'Z'

   d. p_4 = 'A' = 0 -> c_4 = E(0) = (0+13) mod 26 = 13 = 'N'

   e. p_5 = 'N' = 13 -> c_5 = E(13) = (13+13) mod 26 = 0 = 'A'

   f. dst...

   Sehingga menghasilkan Cipherteks: FRZNATNG ORYNWNE

2. Enkripsi *Affine cipher*

   Dalam metode enkripsi *affine cipher* dibutuhkan dua parameter utama yaitu *m* dan *b*. Bilangan bulat yang relatif prima *m* dipilih sesuai dengan ukuran alfabet, yang dilambangkan dengan *n*. Parameter *b* menunjukkan jumlah pergeseran karakter dalam enkripsi.

   Contoh: Terdapat pesan yang dihasilkan dari proses enkripsi *caesar cipher* yaitu FRZNATNG ORYNWNE

   Kita ambil *m* = 15 (relatif prima dengan 26) dan *b* = 11

   Enkripsi $c \equiv mP + b \pmod{26}$

   a. p_1 = 'F' = 5 -> $c_1 \equiv 15 \times 5 + 11 \bmod 26 = 86 = 8$ = 'I'

   b. p_2 = 'R' = 17 -> $c_2 \equiv 15 \times 17 + 11 \bmod 26 = 266 = 6$ = 'G'

   c. p_3 = 'Z' = 25 -> $c_3 \equiv 15 \times 25 + 11 \bmod 26 = 386 = 22$ = 'W'

   d. p_4 = 'N' = 13 -> $c_4 \equiv 15 \times 13 + 11 \bmod 26 = 206 = 24$ = 'Y'

   e. p_5 = 'A' = 0 -> $c_5 \equiv 15 \times 0 + 11 \bmod 26 = 11$ = 'L'

   f. dst...

   Sehingga menghasilkan Cipherteks: IGWYLKYX NGHYDYT

   Tahap pertama dan kedua dikenal sebagai langkah proses enkripsi dalam Kriptografi.

Adapun cara pengembalian pesan (dekripsi) adalah sebagai berikut:

1. Dekripsi *Affine cipher*

   Terdapat Cipherteks: IGWYLKYX NGHYDYT

Pertama menghitung m^{-1} yaitu 15^{-1} (mod 26) dengan menyelesaikan $15x \equiv 1$ (mod 26)

Solusinya: $x \equiv 7$ (mod 26) sebab 15 x 7 = 105 = 1 (mod 26)

Jadi, $P \equiv 7(C-10)$(mod 26)

a. c_1 = 'I' = 8 -> $p_1 \equiv 7$ (8-11) mod 26 = -21 = 5 = 'F'
b. c_2 = 'G' = 6 -> $p_2 \equiv 7$ (6-11) mod 26 = -35 = 17 = 'R'
c. c_3 = 'W' = 22 -> $p_3 \equiv 7$ (22-11) mod 26 = 77 = 25 = 'Z'
d. c_4 = 'Y' = 24 -> $p_4 \equiv 7$ (24-11) mod 26 = 91 = 13 = 'N'
e. c_5 = 'L' = 11 -> $p_5 \equiv 7$ (11-11) mod 26 = 0 = 'A'
f. dst...

Dihasilkan Plainteks untuk di proses dekripsi *caesar cipher* (Chiperteks) : FRZNATNG ORYNWNE

2. Dekripsi *caesar cipher*

Terdapat Chiperteks dari hasil Dekripsi *Affine cipher* : FRZNATNG ORYNWNE

a. c1 = 'F' = 5 -> p1 = D(5) = (5-13) mod 26 = 18 = 'S'
b. c2 = 'R' = 17 -> p2 = D(17) = (17-13) mod 26 = 4 = 'E'
c. c3 = 'Z' = 25 -> p3 = D(25) = (25-13) mod 26 = 12 = 'M'
d. c4 = 'N' = 13 -> p4 = D(13) = (13-13) mod 26 = 0 = 'A'
e. c5 = 'A' = 0 -> p5 = D(0) = (0-13) mod 26 = 13 = 'N'
f. dst...

Sehingga Hasil *Plainteks*: SEMANGAT BELAJAR

Kesimpulan dan Saran

Kombinasi penggunaan metode Caesar Cipher dan Affine Cipher mampu meningkatkan tingkat keamanan data secara efektif, lebih dari sekedar menggunakan satu metode secara terpisah. Dengan menggunakan nilai 26 sebagai kunci, hanya karakter dari A sampai Z yang dapat diproses, terlepas dari perbedaan antara huruf besar dan kecil. Menggabungkan kedua metode ini memungkinkan pesan dikembalikan ke bentuk aslinya, memastikan bahwa isi pesan tidak diubah secara tidak diinginkan. Namun perlu dipastikan bahwa nilai *a* pada metode Affine Cipher merupakan bilangan prima relatif terhadap 26, agar metode ini dapat diterapkan secara valid.

Beberapa saran bagi pembaca antara lain : 1. Mengeksplorasi metode lain yang lebih kompleks untuk meningkatkan keamanan pesan. 2. Mengembangkan karakter seperti penggunaan ASCII yang dapat meningkatkan keamanan dengan memiliki 255 karakter berbeda.

Daftar Pustaka

Dian Rachmawati, A. C. (2015). Implementasi kombinasi Caesar dan Affine Cipher untuk keamanan data teks. *Jurnal Edukasi dan Penelitian Informatika*, 60-63.

Jamilatul Maghfiroh, T. E. (2023). Pengamanan pesan menggunakan algoritma *One Time Pad* dengan *Linear Congruential Generator* sebagai pembangkit kunci. *Jurnal Riset Mahasiswa Matematika*, 122-131.

Krisma Budi Ziliwu, A. M. (2022). Implementasi Caesar Cipher pada algoritma kriptografi dalam penyandian pesan *Whatsapp*. *Jurnal Comasie*, 117-125.

Maya Sari, H. D. (2022). Review : algoritma kriptografi sistem keamanan SMS di Android. *Journal of Information Technology*, 11-15.

Nurjamiyah. (2020). Implementasi algoritma Affine Cipher untuk keamanan data teks. *Jurnal Sistem Informasi*, 50-29.