JSS JOURNAL OF SMART SYSTEM

Vol. 1 No. 1 Juli 2021

# Modifikasi Kriptografi Klasik Kombinasi Metode Vigenere Cipher dan Caesar Cipher
## *(Modification of Classical Cryptography Combination of the Vigenere Cipher and Caesar Cipher Methods)*

Nisrina Yulia Setyawati[1)], Adi Nur Khofid[2)], Alessandro U.B Rundi[3)], Vera Wati[4)]
[1)2)3)4)]Program Studi Sistem Informasi Kota Cerdas, Fakultas Teknik, Universitas Tunas Pembangunan
E-mail: [1)]nisyuliaa@gmail.com, [2)]adinur12345678@gmail.com, [3)]ballarundi2@gmail.com, [4)]vera.w@lecture.utp.ac.id

**Abstrak**

Keamanan dan kerahasiaan data masih menjadi aspek yang perlu diperhatikkan dalam berkomunikasi. Tidak adanya prosedur keamanan yang tepat menyebabkan maraknya kasus pencurian data. Tindakan pencurian data sering terjadi pada aplikasi maupun jaringan komunikasi khususnya data berupa teks. Penyebab utama tindakan pencurian data berupa teks adalah belum adanya prosedur keamanan yang tepat. Maka diperlukan suatu metode penyandian data atau kriptografi. Penyandian atau enkripsi data merupakan salah satu teknik keamanan data yang sering digunakan. Adanya metode kriptografi diharapkan dapat meminimalisir kasus pencurian atau penyadapan data. Penelitian ini bertujuan untuk memberikan prosedur keamanan pada data teks dengan menggabungkan dua metode kriptografi yaitu Vigenere Cipher dan Caesar Cipher, dalam proses kombinasi metode Vigenere Cipher dan Caesar Cipher menggunakan kata kunci yang berbeda. Vigenere menggunakan kunci berupa teks sedangkan Caesar menggunakan pergeseran angka sebagai kuncinya. Pada penelitian ini akan dilakukan penyandian dengan perhitungan manual dan program. Dari hasil pengujian didapatkan bahwa hasil penyandian dengan cara perhitungan manual bernilai sama dengan perhitungan program, jika input plainteks menggunakan huruf kapital. Berdasarkan kapasitas informasi didapatkan bahwa tingkat keberhasilan pengujian 100% dengan 15 kali percobaan proses hingga 5000 karakter plainteks dan cipherteks.

**Kata Kunci—** Kriptografi Klasik, Vigenere Cipher, Caesar Cipher

***Abstract***

*Data security and confidentiality are still aspects that need to be considered in communicating. The absence of proper security procedures has led to many cases of data theft. Data theft often occurs in applications and communication networks, especially data in the form of text. The main cause of data theft in the form of text is the absence of proper security procedures. So we need a data encoding method or cryptography. Encryption or data encryption is one of the data security techniques that is often used. The cryptographic method is expected to minimize cases of theft or data eavesdropping. This study aims to provide security procedures for text data by combining two cryptographic methods, namely Vigenere Cipher and Caesar Cipher, in the process of combining the Vigenere Cipher and Caesar Cipher methods using different keywords. Vigenere uses a text key while Caesar uses a numeric shift as the key. In this study, the encoding with manual calculations and programs will be carried out. From the test results, it is found that the results of encoding by manual calculation have the same value as program calculations if the plaintext input uses capital letters. Based on the information capacity, it was found that the success rate of the test was 100% with 15 processing trials of up to 5000 plaintext and ciphertext characters.*

***Keywords—*** *Classical Cryptography, Vigenere Cipher, Caesar Cipher*

## 1. Pendahuluan

Perkembangan teknologi dan informasi yang semakin maju, ditandai dengan munculnya fasilitas-fasilitas komunikasi seperti email, SMS, dan fitur *chatting* pada media sosial sehingga komunikasi tidak lagi dilakukan secara tatap muka [1]. Komunikasi secara digital ini tidak sepenuhnya aman, kejahatan seperti kasus penyadapan pesan dan pencurian data sering terjadi. Data atau pesan yang dikirimkan memerlukan sebuah prosedur keamanan berupa teknik penyandian agar keamanan dan kerahasiaan pesan tetap terjaga [2].

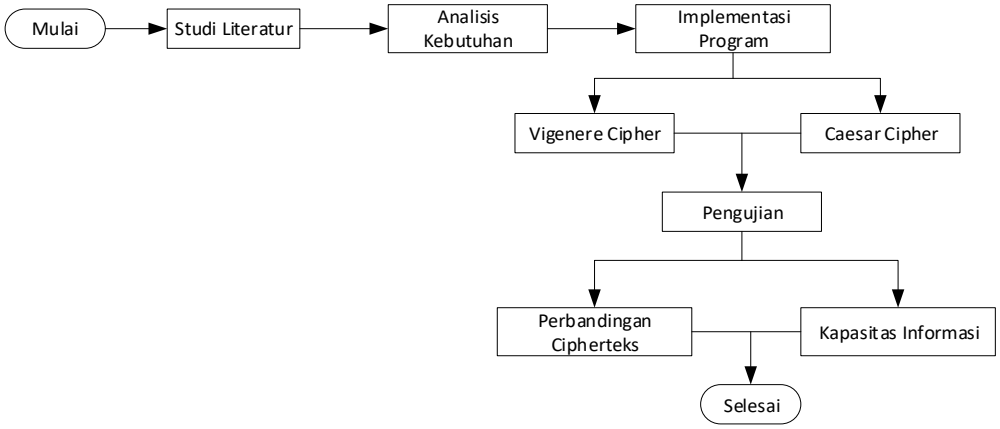
Teknik penyandian yang digunakan untuk menjaga keamanan dan kerahasiaan data adalah kriptografi. Kriptografi merupakan ilmu untuk menjaga kerahasiaan pesan dengan cara mentransformasikan pesan ke dalam sandi tak bermakna, proses yang ada di dalam kriptografi adalah proses enkripsi dan proses dekripsi [3]. Proses enkripsi adalah mengubah pesan dari pesan bermakna (plainteks) menjadi pesan tak bermakna (cipherteks) sedangkan proses dekripsi adalah mengubah pesan tak bermakna (cipherteks) menjadi pesan bermakna (plainteks).

Penyandian metode kriptografi klasik seringkali dipelajari sebagai konsep dasar dari kriptografi dan memiliki kelemahan pada sistem cipher. Algoritma kriptografi klasik biasanya menggunakan teknik subtitusi atau transposisi. Teknik subtitusi dilakukan dengan cara mengganti karakter demi karakter sedangkan transposisi dilakukan dengan cara permutasi [4]. Meski demikian, peneliti melakukan modifikasi pada kriptografi klasik yaitu Caesar Cipher kombinasi Vigenere Cipher sebagai upaya meningkatkan keamanan. Vigenere Cipher dan Caesar Cipher termasuk dalam metode kriptografi klasik. Penerapan kedua metode itu juga dapat dijadikan solusi untuk meningkatkan keamanan pesan teks. Selain itu, menerapkan kedua metode secara terpisah dimana akan dilakukan juga pengkombinasian antara Vigenere Cipher dan Caesar Cipher, agar dapat dibandingkan keefektifannya dalam menyandikan pesan.

Penelitian oleh Maricar dan Sastra, 2018 [1] dilakukan pengujian pada beberapa metode, mulai dari Cipher Substitusi, Vigenere Cipher dan Cipher Transposisi, penelitian tersebut dilakukan untuk mencari keefektifan dari masing masing metode. Termasuk hasil penelitian tersebut menghasilkan pengujian data dan waktu, serta cara perhitungan manual enkripsi dan dekripsi. Penelitian lain oleh Romindo, 2018 [3] bertujuan untuk membandingkan antara Algoritma Monoalphabetic Cipher dengan Algoritma One Time Pad (OTP), baik itu perbandingan sifat, proses enkripsi Monoalphabetic dengan proses enkripsi OTP serta kekurangannya. Penelitian tersebut ditampilkan cara perhitungan manual dari algoritma Monoalphabetic maupun algoritma OTP. Penelitian lain seperti yang dilakukan Hardhita dan Sholeha, 2021 [6] merupakan penelitian yang menggabungkan antara Caesar Cipher dan Vigenere Cipher dimana isi yang terkandung di dalamnya merupakan hasil pengujian proses enkripsi maupun dekripsi menggunakan cara perhitungan tabel dan juga hasil dari implementasi pemrograman PHP *(Hypertext Preprocessor)*. Penelitian oleh Gautam, 2018 [7] merupakan penelitian yang mengkombinasi Vigenere Cipher dengan modifikasi Caesar Cipher dengan pembahasan pada penelitian dijelaskan secara teori dan juga dibuktikan dengan perubahan rumus asli. Penelitian oleh Rahim, 2019 [8] melakukan metode penelitian penggabungan Caesar dengan Vigenere, tetapi hanya menjelaskan tahapan enkripsi (alur dari plainteks ke cipherteks) dan bukan prosesnya meliputi penerapan cara pendekatan matematis dari kriptografi. Disamping itu, penelitian tersebut belum menyertakan proses dekripsi.

Maka dari itu pada penelitian yang akan dilakukan peneliti menggunakan gabungan metode klasik dari dua metode kriptografi yaitu Vigenere Cipher dan Caesar Cipher. Adapun keunggulan dari jurnal ini melakukan pengoptimalan kriptografi klasik dengan penggabungan 2 metode sehingga memperkuat enkripsi dan juga menggunakan perhitungan manual dan pembuktian dengan *source code*. Pengujian yang dilakukan akan melakukan perbandingan perhitungan manual kriptografi dan kapasitas informasi.

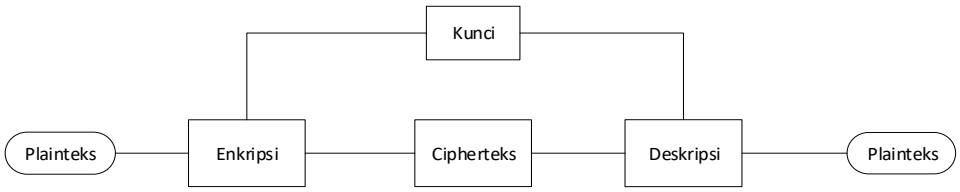
## 2. Metode Penelitian




**Gambar 1.** Langkah Penelitian

Penelitian ini menggunakan dua metode dalam proses enkripsi dan dekripsi. Metode yang diterapkan pada Vigenere Cipher adalah setiap huruf pada plainteks akan dipasangkan dengan satu huruf yang ada pada kata kunci [2]. Metode Caesar Cipher adalah dengan subtitusi huruf pada pesan asli dengan huruf lain berdasarkan kunci yang telah diberikan dalam posisi alfabet [9].

Kriptografi klasik adalah kriptografi yang dilakukan dengan cara mengacak huruf yang digunakan pada masa sebelum komputer ditemukan ataupun sudah ditemukan tapi belum belum canggih. Terdapat 2 metode dalam kriptografi klasik yaitu subtitusi dan transposisi. Metode substitusi adalah metode yang dilakukan dengan cara mengganti huruf plainteks dengan huruf cipherteks, sedangkan untuk metode transposisi adalah metode yang dilakukan dengan cara mengubah susunan/posisi huruf plainteks ke posisi lainnya [5].




**Gambar 2.** Proses Kriptografi

Vigenere Cipher merupakan metode sandi polialfabetik yang mengenkripsi sekaligus sebuah teks yang terdiri dari beberapa huruf [6]. Sedangkan Caesar Cipher adalah metode persandian klasik yang berbasis substitusi sederhana, yang dilakukan dengan menggeser yang mensubtitusi suatu huruf menjadi huruf pada daftar alfabet berada di sebelah kanan atau sebelah kiri huruf tersebut, baik pada proses enkripsi maupun dekripsi [6]. Vigenere Cipher dan Caesar Cipher memiliki rumus matematis yang sama, yaitu:

Enkripsi:

$$Ci = E(Pi) = (Pi + k) \, mod \, 26 \quad (1)$$

Dekripsi:

$$Pi = D(Ci) = (Ci - k) \, mod \, 26 \quad (2)$$

Keterangan :

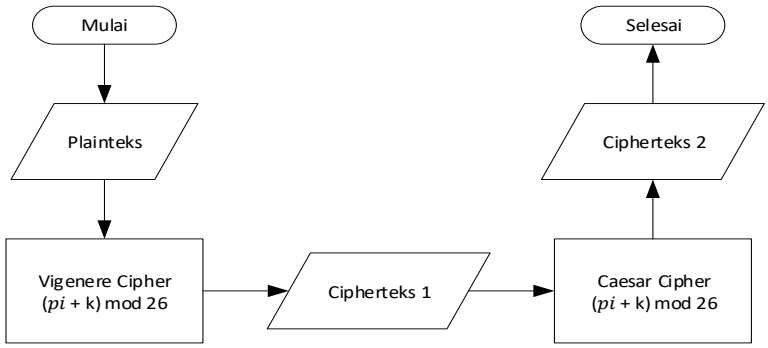
$Pi$ = karakter plainteks ke$-i$

$Ci$ = karakter cipherteks ke$-i$

$k$ = kunci

Pada tahap analisis kebutuhan membutuhkan pesan teks yang memiliki jumlah karakter sebanyak kelipatan 50 (lima puluh) yang digunakan untuk pengujian. Selain itu juga terdapat kebutuhan hardware berupa laptop atau komputer sedangkan kebutuhan software berupa Jupyter Notebook. Pada tahap implementasi program dilakukan metode kriptografi dengan kombinasi Vigenere Cipher dan Caesar Cipher, kemudian selanjutnya akan dilakukan tahap pengujian. Pengujian hasil cipherteks dilakukan untuk membandingkan hasil dari perhitungan manual dan perhitungan program. Sedangkan pengujian kapasitas informasi dilakukan untuk mengetahui ketahanan algoritma.

## 3. Hasil dan Pembahasan




**Gambar 3.** Flowchart Program

Perhitungan cipherteks dalam kombinasi Vigenere Cipher dan Caesar Cipher dilakukan secara manual dan program. Flowchart program kombinasi Vigenere dan Caesar disajikan pada Gambar 3. Proses perhitungan manual menggunakan rumus yang telah disajikan pada rumus matematis (1)(2).

**a. Proses Penyandian**

Pada proses penyandian pertama, peneliti menggunakan algoritma Vigenere Cipher dalam proses pengubahan pesan atau data menjadi cipherteks. Cipherteks tersebut akan menjadi plainteks dari proses penyandian kedua atau Caesar Cipher. Teks data awal yang akan disandikan yaitu "UTPJUARA" dengan kunci Vigenere adalah SIKC sedangkan kunci Caesar adalah kunci geser 7. Berikut merupakan proses enkripsi dari kombinasi Vigenere Cipher dan Caesar Cipher yang akan dilakukan secara manual dan menggunakan program.

1) Perhitungan Manual
   a) Vigenere Cipher
   Plainteks : UTPJUARA
   Kunci : SIKC

**Tabel 1.** Proses Vigenere Cipher

| U | T | P | J | U | A | R | A |
|---|---|---|---|---|---|---|---|
| 20 | 19 | 15 | 9 | 20 | 0 | 17 | 0 |
| **S** | **I** | **K** | **C** | **S** | **I** | **K** | **C** |
| 18 | 8 | 10 | 2 | 18 | 8 | 10 | 2 |

$$Ci = E(U) = 20 + 18 \, mod \, 26 = 38 \, mod \, 26 = 38 - 26 = 12 \rightarrow (M) \quad (3)$$
$$Ci = E(T) = 19 + 8 \, mod \, 26 = 27 \, mod \, 26 = 27 - 26 = 1 \rightarrow (B) \quad (4)$$
$$Ci = E(P) = 15 + 10 \, mod \, 26 = 25 \rightarrow (Z) \quad (5)$$
$$Ci = E(J) = 9 + 2 \, mod \, 26 = 11 \rightarrow (L) \quad (6)$$
$$Ci = E(U) = 20 + 18 \, mod \, 26 = 38 \, mod \, 26 = 38 - 26 = 12 \rightarrow (M) \quad (7)$$
$$Ci = E(A) = 0 + 8 \, mod \, 26 = 8 \rightarrow (I) \quad (8)$$
$$Ci = E(R) = 17 + 10 \, mod \, 26 = 27 - 26 \rightarrow (B) \quad (9)$$
$$Ci = E(A) = 0 + 2 \, mod \, 26 = 2 \rightarrow (C) \quad (10)$$

Plainteks adalah $MBZLMIBC$

   b) Caesar Cipher
   Plainteks : $MBZLMIBC$
   Kunci : 7

**Tabel 2.** Proses Caesar Cipher

| M | B | Z | L | M | I | B | C |
|---|---|---|---|---|---|---|---|
| 12 | 1 | 25 | 11 | 12 | 8 | 1 | 2 |

$$Ci = E(M) = 12 + 7 \, mod \, 26 = 19 \rightarrow (T) \quad (11)$$
$$Ci = E(B) = 1 + 7 \, mod \, 26 = 8 \rightarrow (I) \quad (12)$$
$$Ci = E(Z) = 25 + 7 \, mod \, 26 = 32 \, mod \, 26 = 32 - 2 = 6 \rightarrow (G) \quad (13)$$
$$Ci = E(L) = 11 + 7 \, mod \, 26 = 18 \rightarrow (S) \quad (14)$$
$$Ci = E(M) = 12 + 7 \, mod \, 26 = 19 \rightarrow (T) \quad (15)$$
$$Ci = E(I) = 8 + 7 \, mod \, 26 = 15 \rightarrow (P) \quad (16)$$
$$Ci = E(B) = 1 + 7 \, mod \, 26 = 8 \rightarrow (I) \quad (17)$$
$$Ci = E(C) = 2 + 7 \, mod \, 26 = 9 \rightarrow (J) \quad (18)$$

Cipherteks adalah $TIGSTPIJ$

2) Implementasi Program
   a) *Source Code*

Pada *source code*, peneliti menggunakan *source code* kombinasi dari Vigenere Cipher dan Caesar Cipher. Dimana Vigenere sebagai metode pertama dan Caesar menjadi metode kedua lihat Gambar 4 dan 5)

```
int("MENU :")
int("[1] Enkripsi")
int ("[2] Dekripsi")
 = 0
ile na==0:
  pilih = input("Pilih menu: ")

  if pilih =="1":
      na =1
      #vigenere
      def generateKey(string, key):
          key = list(key)
          if len(string)==len(key):
              return(key)
          else:
              for i in range(len(string) -
                             len(key)):
                  key.append(key[i%len(key)])
          return("". join(key))

      def cipherText(string,key):
          cipher_text = []
          for i in range(len(string)):
              x = (ord(string[i]) +
                   ord(key[i])) % 26
              x += ord('A')
              cipher_text.append(chr(x))
          return("". join(cipher_text))

      if __name__ == "__main__":
          string = input("Masukkan plainteks :")
          keyword = input("Masukkan kunci vigenere : ")
          key = generateKey(string, keyword)
          cipher_text = cipherText(string,key)
          #print("Ciphertext Vigenere :", cipher_text)
```

**Gambar 4.** *Source Code* Caesar dan Vigenere Cipher (1)

```
    #Caesar
    def enkripsi (text,s):
        result = " "

        for i in range (len(text)):
            char = text[i]

            if (char.isupper()):
                result += chr ((ord(char) + s-65) % 26 + 65)

            else :
                result += chr((ord(char) + s-97) % 26 + 97)

        return result
    text =(cipher_text)
    s = int(input("Masukkan kunci caesar : "))
    print ("Chipertext : " + enkripsi(text,s))

elif pilih =="2":
    na=2
    def dekripsi (text,s):
        result = ""

        for i in range (len(text)):
            char = text[i]

            if (char.isupper()):
                result += chr ((ord(char) - s-65) % 26 + 65)

            else :
                result += chr((ord(char) - s-97) % 26 + 97)

        return result
    text =input("Masukkan Chipertext : ")
    s = int(input("Masukkan kunci caesar : "))
    result = dekripsi(text,s)
    #print ("PLainteks Caesar: ", result )
```

```
#Vigenere
def generateKey(string, key):
    key = list(key)
    if len(string)==len(key):
        return(key)
    else:
        for i in range(len(string) -
                       len(key)):
            key.append(key[i%len(key)])
    return("". join(key))

def plainTeks(string,key):
    plain_teks = []
    for i in range(len(string)):
        x = (ord(string[i]) -
             ord(key[i])) % 26
        x += ord('A')
        plain_teks.append(chr(x))
    return("". join(plain_teks))

if __name__ == "__main__":
    string = (result)
    keyword = input("Masukkan kunci vigenere : ")
    key = generateKey(string, keyword)
    plain_teks = plainTeks(string,key)
    print("Plainteks : ", plain_teks)
```

**Gambar 5.** *Source Code* Caesar dan Vigenere Cipher (2)

Hasil implementasi kriptografi pada salah satu bahasa pemrogram yaitu dengan pemograman Python menggunakan Jupyter Notebook lihat Gambar 4 dan Gambar 5 *Source Code.*

**b. Pengujian**

Pengujian dilakukan 2 (dua) kali, pertama dengan menggunakan plainteks dengan syarat menggunakan huruf kapital dan yang kedua dilakukan dengan plainteks huruf kecil, dengan data keterangan sebagai berikut:

1) Pengujian Program

Plainteks : UTPJUARA
Kunci Vigenere : SIKC
Kunci Caesar : 7

Hasil Pengolahan Pengujian 1
Pengujian 1 dilakukan dengan plainteks huruf kapital

```
MENU :
[1] Enkripsi
[2] Dekripsi
Pilih menu: 1
Masukkan plainteks :UTPJUARA
Masukkan kunci vigenere : SIKC
Masukkan kunci caesar : 7
Chipertext :  TIGSTPIJ
```

**Gambar 6**. Proses Enkripsi Program

Hasil Pengolahan Pengujian 2
Pengujian 2 dilakukan dengan plainteks huruf kecil

```
MENU :
[1] Enkripsi
[2] Dekripsi
Pilih menu: 1
Masukkan plainteks :utpjuara
Masukkan kunci vigenere : SIKC
Masukkan kunci caesar : 7
Chipertext :  ZOMYZVOP
```

**Gambar 7.** Proses Enkripsi Program

Pada keterangan Gambar 6 menghasilkan hasil yang sama dengan perhitungan manual, kemudian terlihat pada Gambar 7 menghasilkan cipherteks yang berbeda. Sehingga dapat dibuat kesimpulan jika proses enkripsi dapat dilakukan jika menggunakan huruf alphabet capital atau huruf besar.

2) Kapasitas Informasi

**Tabel 3.** Kapasitas Informasi

| Pengujian | Kapasitas Informasi | | Keberhasilan | |
|---|---|---|---|---|
| | Plainteks | Cipherteks | Plainteks | Cipherteks |
| 1 | 50 karakter | 50 karakter | ✓ | ✓ |
| 2 | 100 karakter | 100 karakter | ✓ | ✓ |
| 3 | 150 karakter | 150 karakter | ✓ | ✓ |
| 4 | 200 karakter | 200 karakter | ✓ | ✓ |
| 5 | 250 karakter | 250 karakter | ✓ | ✓ |
| 6 | 300 karakter | 300 karakter | ✓ | ✓ |

| | | | | |
|---|---|---|---|---|
| 7 | 350 karakter | 350 karakter | ✓ | ✓ |
| 8 | 400 karakter | 400 karakter | ✓ | ✓ |
| 9 | 450 karakter | 450 karakter | ✓ | ✓ |
| 10 | 500 karakter | 500 karakter | ✓ | ✓ |
| 11 | 1000 karakter | 1000 karakter | ✓ | ✓ |
| 12 | 2000 karakter | 2000 karakter | ✓ | ✓ |
| 13 | 3000 karakter | 3000 karakter | ✓ | ✓ |
| 14 | 4000 karakter | 4000 karakter | ✓ | ✓ |
| 15 | 5000 karakter | 5000 karakter | ✓ | ✓ |

Pengujian pada Tabel 3 jika pemrograman dari kombinasi Vigenere dan Caesar Cipher dapat memproses banyak karakter hingga 5000 karakter.

## 5. Kesimpulan

Dari proses penyandian dan analisis yang dilakukan, maka dapat diambil beberapa kesimpulan. Dibuktikan bahwa dengan hasil dari enkripsi manual dan menggunakan program meghasilkan hasil atau cipherteks yang sama, dengan "UTPJUARA" sebagai plainteks dan menggunakan kunci "SIKC" dan pergeseran 7 huruf. Pada proses enkripsi program akan menghasilkan enkripsi sesuai dengan perhitungan manual jika menggunakan input huruf kapital sebagai planteks. Jika planteks menggunakan huruf kecil maka hasil dari proses enkripsi tidak akan sesuai dengan perhitungan manual. Pada 15 pengujian karakter dengan menggunakan algoritma gabungan Vigenere dan Caesar yang dilakukan dengan menggunakan 50 sampai 5000 karakter, menghasilkan kesimpulan bahwa jumlah kapasitas informasi pada plainteks sama dengan kapasitas informasi pada cipherteks dengan tingkat keberhasilan pengujian 100%.

## Referensi

[1] M. A. Maricar and N. P. Sastra, "Efektivitas Pesan Teks Dengan Cipher Substitusi, Vigenere Cipher, dan Cipher Transposisi," *Maj. Ilm. Teknol. Elektro*, vol. 17, no. 1, p. 59, 2018, doi: 10.24843/mite.2018.v17i01.p08.

[2] G. B. Minarto and M. Q. Khairuzzaman, "Penerapan Kriptografi Menggunakan Caesar Cipher Dan Vigenere Cipher," *Enter*, vol. 1, pp. 1–12, 2018, [Online]. Available: http://www.sisfotenika.stmikpontianak.ac.id/index.php/enter/article/view/787.

[3] Romindo, "Analisa Perbandingan Algoritma Monoalphabetic Cipher Dengan Algoritma One Time Pad Sebagai Pengamanan Pesan Teks," *Jurnal, Publ. Inform. Penelit. Tek. Medan, Politek. Ganesha*, vol. 2, no. 2, pp. 62–66, 2018.

[4] F. W. U. M. Ziaurrahman, Ema Utami, "Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakan One Time Pad Dengan Enkripsi Berlanjut," vol. 4, no. 1, p. (halaman 2), 2019.

[5] R. Munir, "Slide Kuliah Pengantar Kriptografi," *J. Ilmu Komput. dan Inform.*, 2019.

[6] V. C. Hardita and E. W. Sholeha, "Penerapan Kombinasi Metode Vigenere Cipher, Caesar Cipher Dan Simbol Baca Dalam Mengamankan Pesan," *J. SAINTEKOM*, vol. 11, no. 1, pp. 34–43, 2021, doi: 10.33020/saintekom.v11i1.202.

[7] D. Gautam, "An Enhanced Cipher Technique using Vigenere and Modified Caesar Cipher," *Cornell Univ. Libr.*, 2018.

[8] R. Rahim, M. A. Rosid, A. S. Fitrani, A. D. Gs, and N. L. W. S. R. Ginantra, "Enhancement three-pass protocol security with combination caesar cipher and vigenere cipher," *J. Phys. Conf. Ser.*, vol. 1402, no. 6, pp. 4–9, 2019, doi: 10.1088/1742-6596/1402/6/066045.

[9] A. B. Nasution, "Implementasi Pengamanan Data Dengan Menggunakan Algoritma Caesar Cipher Dan Transposisi Cipher," *J. Teknol. Inf.*, vol. 3, no. 1, p. 1, 2019, doi: 10.36294/jurti.v3i1.680.