ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.3 No.1 Tahun 2024
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-3 2024
Fakultas Teknik, Universitas Pelita Bangsa, Januari 2024

KOMBINASI PENERAPAN ALGORITMA *CAESAR CIPHER* DAN ALGORITMA *VIGENERE CIPHER* PADA PENGAMANAN DOKUMEN TEKS

COMBINED APPLICATION OF CAESAR CIPHER ALGORITHM AND VIGENERE CIPHER ALGORITHM ON TEXT DOCUMENT SECURITY

Muhammad Farhan, Satrio Pratama Wijaya[2], Bilal AlHafidz[3]
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa[3]
[1]mufhan623@gmail.com, [2]satrio7299@gmail.com*, [3]bilalhafidz17@gmail.com*

Abstract

Cryptography is a method of securing data using algorithms that have been continuously developed continuously until now[1],66 Securing information in text documents is crucial in this digital era. This research aims to improve the security level of text documents through the application of Vigenere and Caesar Cipher cryptographic algorithms. These two algorithms were chosen for their ability to encrypt text in an effective yet simple way. This research will explore the potential of combining Vigenere and Caesar Cipher to create a higher layer of security. In addition, it will also evaluate the performance and efficiency of using these two algorithms together in the context of securing text documents. The experimental methodology involves implementing the algorithms on various types of text documents and testing the resulting security levels. The results of this research are expected to provide a deeper understanding of text document security and provide new insights into the effectiveness of using a combination 5to improve the security of text documents in various contexts, including digital communication, data storage, and the exchange of confidential information. Thus, this research is expected to make a positive contribution to the development of information security technology[2].

Keywords: Cryptography, Caesar Cipher, Vigenere Cipher, Text Document

Abstrak

Kriptografi adalah metode pengamanan data menggunakan algoritma yang banyak dikembangkan secara berkelanjutan hingga sekarang[1], Pengamanan informasi dalam dokumen teks menjadi hal krusial dalam era digital ini. Penelitian ini bertujuan untuk meningkatkan tingkat keamanan dokumen teks melalui penerapan algoritma kriptografi *Vigenere Cipher* dan *Caesar Cipher*. Kedua algoritma ini dipilih karena kemampuan mereka dalam mengenkripsi teks dengan cara yang efektif namun sederhana. Penelitian ini akan menggali potensi kombinasi antara *Vigenere Cipher* dan *Caesar Cipher* untuk menciptakan lapisan keamanan yang lebih tinggi. Selain itu, penelitian ini juga akan mengevaluasi performa dan efisiensi dari penggunaan kedua algoritma ini secara bersamaan dalam konteks pengamanan dokumen teks. Metodologi eksperimental melibatkan implementasi algoritma pada berbagai jenis dokumen teks dan pengujian terhadap tingkat keamanan yang dihasilkan. Hasil dari penelitian ini diharapkan dapat memberikan pemahaman lebih mendalam terkait keamanan dokumen teks serta memberikan pandangan baru terkait efektivitas penggunaan kombinasi algoritma *Vigenere Cipher* dan *Caesar Cipher*. Implikasi praktis dari penelitian ini melibatkan penerapan hasil temuan untuk meningkatkan keamanan dokumen teks dalam berbagai konteks, termasuk komunikasi digital, penyimpanan data, dan pertukaran informasi rahasia. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi positif terhadap pengembangan teknologi keamanan informasi[2].

Kata Kunci : Kriptografi, *Caesar Cipher*, *Vigenere Cipher*, Dokumen Teks

Pendahuluan

Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data.[4]

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain. Seperti contoh algoritma kriptografi yaitu: algoritma *Caesar Cipher* dan *Vigenere Cipher*, algoritma *Caesar Cipher* dan *Vigenere Cipher* termasuk kriptografi klasik yang menggunakan plainteks, cipherteks dan kunci untuk melakukan proses enkripsi dan dekripsi dalam pengamanan data.[5]

Algoritma *Caesar Chiper* adalah teknik kriptografi yang dilakukan dengan mensubtitusi setiap abjad dari pesan yang akan dienkripsi melalui pergeseran susunan sebagai kuncinya. *Vigenere Cipher* setiap huruf pesan aslinya digeser sebanyak satu huruf pada kuncinya sedangkan pada *Caesar Cipher* setiap huruf pesannya digeser sebanyak 1 huruf yang sama.[3]

Dalam era digital yang gejolak ini, pengamanan informasi menjadi aspek krusial dalam menjaga kerahasiaan dan integritas data. Menurut Katz, kriptografi adalah studi ilmiah atau Teknik untuk mengamankan informasi digital, transaksi dan komputasi yang terdistribusi[10]. Oleh karena itu, penelitian ini bertujuan untuk meningkatkan tingkat keamanan dokumen teks melalui penerapan algoritma kriptografi *Vigenere Cipher* dan *Caesar Cipher*.

Vigenere Cipher dan *Caesar Cipher* dipilih sebagai fokus penelitian karena keduanya menunjukkan kemampuan yang signifikan dalam mengenkripsi teks dengan cara yang efektif namun relatif sederhana. Keunikan masing-masing algoritma memberikan dasar untuk mengeksplorasi potensi kombinasi mereka, dengan harapan menciptakan lapisan keamanan yang lebih tinggi bagi dokumen teks.

Penelitian ini tidak hanya bertujuan untuk menggali potensi kombinasi antara *Vigenere Cipher* dan *Caesar Cipher*, tetapi juga akan melakukan evaluasi terhadap performa dan efisiensi dari penggunaan kedua algoritma ini secara bersamaan. Metodologi eksperimental yang dilibatkan dalam penelitian ini mencakup implementasi algoritma pada berbagai jenis dokumen teks dan pengujian terhadap tingkat keamanan yang dihasilkan.

Dengan menghadirkan hasil penelitian ini, diharapkan dapat diperoleh pemahaman yang lebih mendalam terkait keamanan dokumen teks. Selain itu, penelitian ini juga diarahkan untuk memberikan pandangan baru terkait efektivitas penggunaan kombinasi algoritma *Vigenere Cipher* dan *Caesar Cipher* dalam meningkatkan keamanan informasi.

Implikasi praktis dari penelitian ini melibatkan penerapan temuan untuk meningkatkan keamanan dokumen teks dalam berbagai konteks, Dengan demikian, diharapkan bahwa kontribusi positif dari penelitian ini dapat membantu dalam pengembangan teknologi keamanan informasi yang relevan dan efektif di era digital ini.

Metode Penelitian

Penelitian ini menggunakan metode eksperimental untuk meningkatkan tingkat keamanan dokumen teks melalui kombinasi algoritma *Caesar Cipher* dan *Vigenere Cipher*. Berikut adalah langkah-langkah implementasi:

1. Pemilihan Kunci
   - Menentukan kunci untuk algoritma *Caesar Cipher* dan *Vigenere Cipher*. Kunci ini akan digunakan dalam proses enkripsi dan dekripsi.

2. Implementasi *Caesar Cipher*
   - Menerapkan algoritma *Caesar Cipher* pada dokumen teks dengan menggunakan kunci yang telah ditentukan.
   - Membuat tabel enkripsi *Caesar Cipher* untuk memudahkan proses enkripsi.

3. Implementasi *Vigenere Cipher*
   - Menerapkan algoritma *Vigenere Cipher* pada dokumen teks menggunakan kunci yang telah dipilih.
   - Membuat tabel enkripsi *Vigenere Cipher* untuk memudahkan proses enkripsi.

Kombinasi Algoritma

Menggabungkan hasil enkripsi dari *Caesar Cipher* dan *Vigenere Cipher* dengan memanfaatkan potensi kombinasi kunci yang telah disiapkan.

Konversi Hasil ke Format *PDF*

Mengonversi hasil dari kombinasi algoritma ke format dokumen *PDF* menggunakan metode konversi yang sesuai.

Pengujian Keamanan

Melakukan pengujian terhadap tingkat keamanan dokumen teks yang dihasilkan oleh kombinasi algoritma. Pengujian ini mencakup uji ketahanan terhadap metode kriptoanalisis.

Analisis Performa dan Efisiensi

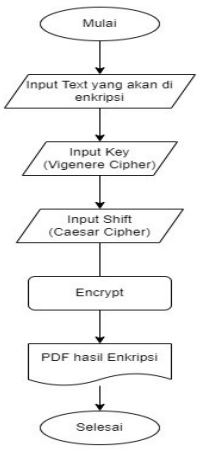
Mengevaluasi performa dan efisiensi dari penggunaan kedua algoritma secara bersamaan pada berbagai jenis dokumen teks.

Penerapan Praktis

Menerapkan hasil temuan penelitian dalam pembuatan dokumen teks *PDF* yang aman dan praktis digunakan dalam konteks komunikasi digital, penyimpanan data, dan pertukaran informasi rahasia.

Dengan langkah-langkah ini, diharapkan penelitian dapat memberikan kontribusi positif terhadap pengembangan teknologi keamanan informasi melalui penerapan kombinasi algoritma *Caesar Cipher* dan *Vigenere Cipher*.

Hasil dan Pembahasan



Flowchart Enkripsi

Flowchart enkripsi adalah sebuah diagram yang menggambarkan langkah-langkah yang dilakukan untuk melakukan enkripsi data. Enkripsi adalah proses mengubah data menjadi bentuk yang tidak dapat dibaca oleh orang lain yang tidak memiliki kunci enkripsi.

Flowchart enkripsi yang diberikan menunjukkan proses enkripsi data teks menggunakan dua metode, yaitu metode *Vigenere Cipher* dan metode *Caesar Cipher*.

Metode *Vigenere Cipher*

Metode *Vigenere Cipher* adalah metode enkripsi yang menggunakan kunci berupa kata atau frase. Kunci ini digunakan untuk melakukan transposisi huruf-huruf dalam data yang akan dienkripsi.

Proses enkripsi dilakukan dengan menulis kunci berulang kali sesuai dengan Panjang karakter pada pesan[6]. *Vigenere cipher* juga dapat menggunakan sebuah tabel untuk mengenkripsikan sebuah plainteks yang mana tabel tersebut terdiri dari 26 baris dan kolom *alfabet*, dan tiap barisnya akan di geser satu huruf ke kiri[7].

Proses enkripsi data teks dengan metode *Vigenere Cipher* dapat dijelaskan sebagai berikut:

1. *Input* data teks yang akan dienkripsi.
2. *Input* kunci enkripsi.
3. Mulai dari huruf pertama data teks, lakukan transposisi huruf tersebut dengan huruf pada kunci yang sesuai.
4. Lanjutkan proses transposisi hingga seluruh huruf dalam data teks telah dienkripsi.
5. Hasil enkripsi adalah data teks yang telah ditransposisi huruf-hurufnya.

Metode *Caesar Cipher*

Ceasar Cipher Algoritma kriptografi yang mula-mula digunakan oleh kaisar Romawi, *Julius Caesar* (sehingga dinamakan juga *caesar chiper*), untuk menyandikan pesan yang ia kirim kepada para gubernurnya. Caranya adalah dengan mengganti (menyulih atau mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet) [8] *Caesar Cipher* adalah menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks, Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya [9].

Metode *Caesar Cipher* adalah metode enkripsi yang menggunakan kunci berupa angka. Kunci ini digunakan untuk menggeser posisi huruf-huruf dalam data yang akan dienkripsi.

Proses enkripsi data teks dengan metode *Caesar Cipher* dapat dijelaskan sebagai berikut:

1. *Input* data teks yang akan dienkripsi.
2. *Input* kunci enkripsi.
3. Mulai dari huruf pertama data teks, geser posisi huruf tersebut ke kanan sesuai dengan kunci yang telah ditentukan.
4. Lanjutkan proses penggeseran hingga seluruh huruf dalam data teks telah dienkripsi.
5. Hasil enkripsi adalah data teks yang telah bergeser posisi huruf-hurufnya.

Penjelasan *Flowchart*

Flowchart enkripsi yang diberikan memiliki empat langkah utama, yaitu:

1. Mulai. Langkah ini merupakan awal dari proses enkripsi.
2. *Input* data teks yang akan dienkripsi. Langkah ini dilakukan untuk memasukkan data teks yang akan dienkripsi.
3. *Input* kunci enkripsi. Langkah ini dilakukan untuk memasukkan kunci enkripsi yang akan digunakan.
4. *Encrypt*. Langkah ini merupakan langkah enkripsi data teks yang dilakukan sesuai dengan metode enkripsi yang dipilih.

Penjelasan Detail

Penjelasan detail dari *flowchart* enkripsi dapat diuraikan sebagai berikut:

1) Langkah 1: Mulai
   Langkah ini merupakan awal dari proses enkripsi. Pada langkah ini, *flowchart* akan memulai proses enkripsi dengan memeriksa apakah *input* data teks dan kunci enkripsi telah tersedia. Jika *input* data teks dan kunci enkripsi belum tersedia, maka *flowchart* akan berhenti.

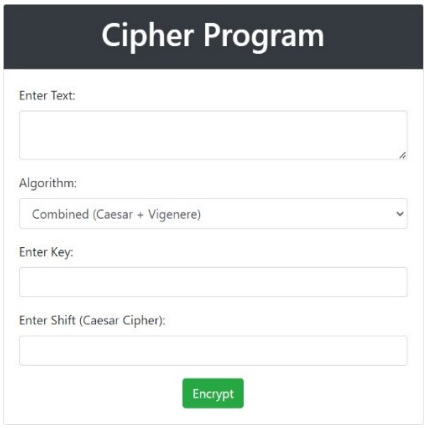
2) Langkah 2: *Input* data teks yang akan dienkripsi
   Pada langkah ini, pengguna akan memasukkan data teks yang akan dienkripsi. Data teks ini dapat berupa teks biasa, teks acak, atau kode.

3) Langkah 3: *Input* kunci enkripsi
   Pada langkah ini, pengguna akan memasukkan kunci enkripsi yang akan digunakan. Kunci enkripsi ini dapat berupa kata, frase, atau angka.

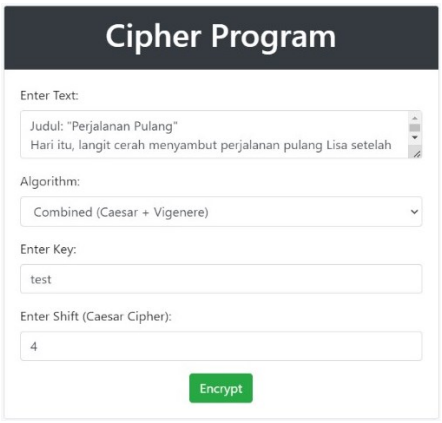
4) Langkah 4: *Encrypt*
   Pada langkah ini, data teks akan dienkripsi sesuai dengan metode enkripsi yang dipilih. Jika metode enkripsi yang dipilih adalah metode *Vigenere Cipher*, maka *flowchart* akan melakukan transposisi huruf-huruf dalam data teks sesuai dengan kunci enkripsi yang telah ditentukan. Jika metode enkripsi yang dipilih adalah metode *Caesar Cipher*, maka *flowchart* akan menggeser posisi huruf-huruf dalam data teks sesuai dengan kunci enkripsi yang telah ditentukan.

Penjelasan alur kerja :

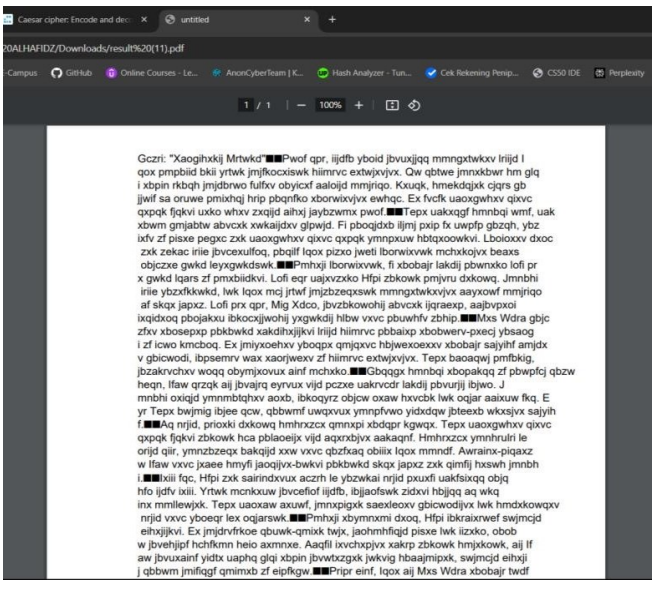
1) Pada halaman utama, akan terlihat formulir dengan tiga *input*, yaitu: "*Text*", "*Key*", dan "*Shift*".



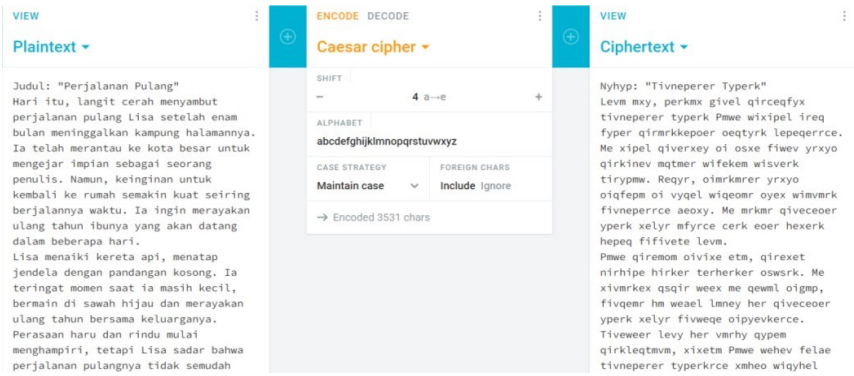
2) Isi teks yang ingin di enkripsi dalam kotak "*Text*". Dan isi kunci yang akan digunakan untuk enkripsi teks menggunakan algoritma *Caesar Cipher*. Dan pastikan untuk mengisi kolom "*Shif*" untuk menambahkan *double encryption* menggunakan *Caesar Cipher* + *Vigenere Cipher* pada text. Setelah mengisi semua *input*, klik tombol "*Encrypt*".



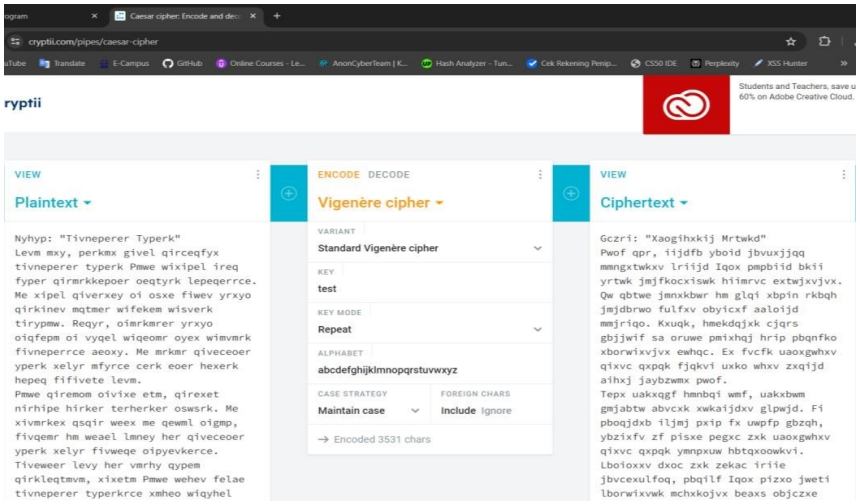
3) Aplikasi *Flask* kemudian akan mengolah *input*, melakukan enkripsi sesuai algoritma *Caesar Cipher* dan *Vegenere Cipher,* dan menghasilkan file *PDF* hasil enkripsi.



4) Lakukan pengecekan hasil enkripsi menggunakan *Caesar Cipher Encoder*.



5) Melakukan pengecekan *Double Encryption* menggunakan *Vigenere Cipher Encoder*.



Kesimpulan

Dalam penelitian ini, telah dilakukan eksplorasi terhadap pengamanan dokumen teks menggunakan kombinasi algoritma *Caesar Cipher* dan *Vigenere Cipher*. Dalam era digital yang penuh gejolak, keamanan informasi menjadi krusial, terutama dalam menjaga kerahasiaan dan integritas data. Pemilihan *Caesar Cipher* dan *Vigenere Cipher* sebagai fokus penelitian didasarkan pada kemampuan keduanya dalam mengenkripsi teks secara efektif namun relatif sederhana.

Langkah-langkah implementasi yang melibatkan pemilihan kunci, implementasi kedua algoritma, kombinasi hasil enkripsi, konversi ke format *PDF*, pengujian keamanan, dan analisis performa diharapkan dapat memberikan kontribusi positif terhadap pengembangan teknologi keamanan informasi. Penelitian ini tidak hanya sebatas pada eksplorasi potensi kombinasi antara *Caesar Cipher* dan *Vigenere Cipher*, tetapi juga mengukur performa dan efisiensi dari penggunaan kedua algoritma secara bersamaan.

Hasil penelitian ini memiliki implikasi praktis dalam penerapan temuan untuk meningkatkan keamanan dokumen teks dalam berbagai konteks, seperti komunikasi digital, penyimpanan data, dan pertukaran informasi rahasia. Diharapkan bahwa kombinasi algoritma ini dapat memberikan lapisan keamanan yang lebih tinggi, serta memberikan pandangan baru terkait efektivitas penggunaannya.

Flowchart enkripsi yang telah disajikan memberikan gambaran visual mengenai proses enkripsi data teks menggunakan metode *Caesar Cipher* dan *Vigenere Cipher*. Penjelasan detail dari *flowchart* tersebut memberikan pemahaman mendalam tentang langkah-langkah yang dilakukan dalam proses enkripsi.

Dengan demikian, keseluruhan penelitian ini diharapkan dapat memberikan sumbangan signifikan dalam pengembangan teknologi keamanan informasi di era digital, dan dapat menjadi dasar untuk penelitian lanjutan dalam bidang ini.

Daftar Rujukan

[1] Sarwo Budi, Arif Budimansyah Purba & Jajang Mulyana. (2019). Jurnal PENGAMANAN FILE DOKUMEN MENGGUNAKAN KOMBINASI METODE SUBTITUSI DAN VIGENERE CIPHER. ILKOM Ilmiah, 11 (3), 222-230.

[2] Priyono. (2016). PENERAPAN ALGORITMA CAESAR CIPHER DAN ALGORITMA VIGENERE CIPHER DALAM PENGAMANAN PESAN TEKS. Jurnal Riset Komputer (JURIKOM), 3 (5), 351-356.

[3] Hidayah, V., Mulyana, D., & Bachtiar, Y. (2023). Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian pesan teks. Journal on Education, 5 (3), 8563-8573.

[4] Munir, Rinaldi. (2006). Kriptografi, Bandung: Penerbit Informatika.

[5] Dony, Ariyus. (2009). Pengantar Ilmu Kriptografi, Yogyakarta: Penerbit Andi.

[6] Mendrofa, E., Purba, E., Siahaan, B., & Sembiring, R. (2017). Collaborative Encryption Algorithm Between Vigenere Cipher, Rotation of Matrix (ROM), and One Time Pad (OTP) Algoritma. Technology and Engineering Systems Journal, 13-21.

[7] Darmawan , M., & Windarto , W. (2018). Implementasi Algoritma Kriptografi Vigener Cipher Dan Affine Cipher Untuk Mengamankan Pesan Pada Aplikasi Chatting Berbasis Android. SKANIKA. Sistem Komputer dan Teknik Informatika, 24-32.

[8] Andriyanto. (2019). Implementasi Algoritma Caesar Cipher Untuk Keamanan Data Pada Kartu Ujian. JURNAL BUFFER INFORMATIKA, 1-7.

[9] Angriani, H., & Saharaeni, Y. (2019). Implementasi Algoritma Caesar Cipher Pada Keamanan Data Sistem E-Voting Pemilihan Ketua Organisasi Kemahasiswaan. Inspiration: Jurnal Teknologi Informasi dan Komunikasi, 123-126.

[10] Katz, j. & Lindell, Y. (2007). Inroduction to Modern Crypyography Chapman & Hall/CRC : United States.

[11] Efrandi. (2014). APLIKASI KRIPTOGRAFI PESAN MENGGUNAKAN ALGORITMA VIGENERE CIPHER. Jurnal Media Infotama, 10 (2), 120-128.

[12] Setyawati, N. Y., Adi N. Khofid, Alessandro U.B Rundi, & Vera Wati. (2021). Modifikasi Kriptografi Klasik Kombinasi Metode Vigenere Cipher dan Caesar Cipher. Journal of Smart System, 1 (1), 1-8.

[13] Saroha, V, Mor, S & Dagar, A. (2012). Enhancing Security of Caeser Cipher by Double Columnar Transposition Method, International Journal of Advanced Research Computer Science and Software Engineering, 2(10).

[14] A. B. Nasution. (2019). Implementasi Pengamanan Data Dengan Menggunakan Algoritma Caesar Cipher Dan Transposisi Cipher. J. Teknol.Inf. 3 (1), 1.

[15] Rahayu, T. P, Yakub, & Limiady, I. (2012). Aplikasi Enkripsi Pesan Teks (SMS) pada Perangkat Handphone dengan Algoritma Caesar Cipher, Seminar Nasional Teknologi Informasi dan Komunikasi (SENTIKA) Yogyakarta.