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

Penerapan Kriptografi Caesar Cipher dan Transposisi Cipher Pada Bot Aplikasi Pesan Telegram

Implementation of Caesar Cipher and Transposition Cipher Cryptography on Telegram Bot

[1]Bhagas Shaib Pramono, [2]Alwan Luthfi, [3]Delfian Ruly Havatilla
[123]Informatika, Teknik, Universitas Pelita Bangsa
bhagasshaibp@mhs.pelitabangsa.ac.id[1], alwan@mhs.pelitabangsa.ac.id[2], delfiansteel@mhs.pelitabangsa.ac.id[3]

Abstract

This research objective is to enhance the security of communication in the Telegram chatting application through the implementation of cryptographic methods, specifically Caesar Cipher and Transposition Cipher. The primary focus of this study is to observe the security level of messages sent and received by users of the application, with the goal of preventing potential information leaks and safeguarding user privacy. The methods employed involve the analysis of cryptographic theory and the development of an effective cryptographic model for chatting applications. The research design is experimental, with direct application to the Telegram application. The results of this study are expected to provide a better understanding of the effectiveness of the Caesar Cipher and Transposition Cipher cryptographic methods in improving communication security in the Telegram apps.

Keywords: *Telegram, Cryptographic, Security Level of Messages, Caesar Cipher, Transposisi Cipher*

Abstrak

Penelitian ini bertujuan untuk meningkatkan keamanan komunikasi pada aplikasi chatting Telegram melalui implementasi metode kriptografi, khususnya Caesar Cipher dan Transposisi Cipher. Fokus utama penelitian ini adalah untuk mengamati tingkat keamanan pesan yang dikirim dan diterima oleh pengguna aplikasi, dengan tujuan mencegah potensi kebocoran informasi dan menjaga privasi pengguna. Metode yang digunakan melibatkan analisis teori kriptografi dan pengembangan model kriptografi yang efektif untuk aplikasi chatting. Desain penelitian ini bersifat eksperimental dengan penerapan langsung pada aplikasi Telegram. Hasil penelitian ini diharapkan dapat memberikan pemahaman yang lebih baik tentang efektivitas metode kriptografi Caesar Cipher dan Transposisi Cipher pada meningkatkan keamanan komunikasi di aplikasi chatting Telegram.

Kata kunci: Telegram, Kriptografi, Keamanan Pesan, Caesar Cipher, Transposisi Cipher

Pendahuluan

Caesar Cipher merupakan salah satu teknik kriptografi klasik yang menggunakan metode substitusi sederhana. Setiap huruf dalam pesan digeser sejumlah langkah tertentu dalam alfabet. Meskipun mudah diimplementasikan, Caesar Cipher memiliki kelemahan karena pola pergeseran tetap. Oleh karena itu, penggunaan Caesar Cipher dapat memberikan tingkat keamanan dasar pada pesan. Transposisi Cipher melibatkan perubahan posisi huruf dalam pesan tanpa mengubah huruf itu sendiri. Teknik ini dapat memberikan keamanan tambahan dengan mempersulit pola pesan yang dapat dipahami oleh pihak yang tidak berhak. Transposisi Cipher sering melibatkan penggunaan tabel atau matriks untuk mengubah urutan huruf.

Dalam era digital yang semakin berkembang, komunikasi daring melalui aplikasi chatting telah menjadi bagian integral dari kehidupan sehari-hari. Oleh karena itu, penerapan teknologi kriptografi menjadi suatu kebutuhan untuk menjaga integritas dan kerahasiaan pesan yang dikirimkan melalui aplikasi chatting. Salah satu pendekatan kriptografi yang diterapkan pada aplikasi chatting adalah penggunaan metode Caesar Cipher

dan Transposisi Cipher. Caesar Cipher, sebagai teknik substitusi sederhana, dan Transposisi Cipher, yang mengubah urutan huruf dalam pesan, memberikan lapisan keamanan tambahan terhadap potensi serangan dan penyadapan. Penelitian ini akan membahas penerapan kedua teknik kriptografi ini pada salah satu platform chatting terkemuka, yaitu Telegram.

Dengan mempertimbangkan tingkat keamanan yang diberikan oleh Caesar Cipher dan Transposisi Cipher, aplikasi Telegram dapat memperkuat perlindungan terhadap pesan pengguna dari potensi risiko eksternal. Selain itu, keberlanjutan dan efisiensi dalam penggunaan teknik ini perlu dijaga agar pengalaman pengguna tetap optimal tanpa mengorbankan kinerja sistem secara signifikan.

Metode Penelitian

Penelitian ini menggunakan metode penelitian eksperimental, menggabungkan analisis teori kriptografi dan penerapan langsung pada aplikasi Telegram. Langkah pertama melibatkan studi literatur untuk memahami dasar teori kriptografi, khususnya Caesar Cipher dan Transposisi Cipher, serta mengeksplorasi konsep keamanan informasi dalam konteks aplikasi chatting.

Partisipan pada penelitian ini adalah teks pesan yang dikirim kepada bot telegram yang dibuat. Pesan dapat berupa kalimat maupun paragraf. Penelitian ini menggunakan dua algoritma, yaitu. Algoritma caesar kemudian hasilnya di enkripsi kembali menggunakan algoritma transposisi dengan tujuan mendapatkan hasil double enkripsi dari dua algoritma yang digunakan.

Batasan penelitian ini melibatkan keterbatasan pada pengguna aplikasi Telegram sebagai subjek utama. Analisis dan implementasi metode kriptografi Caesar Cipher dan Transposisi Cipher difokuskan pada keamanan pesan yang dikirim dan diterima dalam konteks aplikasi chatting ini. Walaupun demikian, aspek-aspek ini dapat dijadikan titik awal untuk penelitian lanjutan yang lebih luas dalam bidang keamanan informasi.

A. Kriptografi

Kriptografi adalah cabang ilmu yang bertujuan melindungi keamanan informasi dengan menggunakan berbagai teknik untuk mengamankan pesan atau data sehingga hanya dapat diakses oleh pihak yang sah. Proses kunci dalam kriptografi melibatkan dua elemen penting, yaitu enkripsi dan dekripsi. Enkripsi melibatkan perubahan pesan atau data menggunakan algoritma tertentu, dan hanya dapat dikembalikan ke bentuk semula oleh pihak yang memiliki kunci enkripsi yang sesuai. Kunci ini dapat bersifat simetris atau asimetris. Dekripsi adalah proses mengubah kembali informasi atau pesan yang telah dienkripsi menjadi bentuk semula atau aslinya. Di mana pesan atau data diubah menggunakan algoritma kriptografi dan kunci enkripsi untuk menjaga kerahasiaan. Dengan demikian, kriptografi memainkan peran sentral dalam menjaga kerahasiaan, integritas, dan otentikasi informasi dalam lingkungan komunikasi modern.

B. Caesar Cipher

Caesar Cipher adalah metode enkripsi sederhana yang telah digunakan sejak zaman Romawi kuno. Dalam metode ini, setiap huruf dalam teks biasa digantikan dengan huruf lain dengan pergeseran tetap, yang biasanya disebut sebagai kunci. Misalnya, dengan pergeseran tiga tempat ke kanan, huruf "A" akan digantikan oleh "D", "B" menjadi "E", dan seterusnya. Meskipun Caesar Cipher sangat sederhana dan mudah dimengerti, ia memiliki kelemahan besar karena hanya memiliki 25 kemungkinan pergeseran (dengan abjad Inggris), sehingga rentan terhadap serangan dengan metode pengujian seluruh kemungkinan (brute-force attack). Meskipun begitu, Caesar Cipher memberikan dasar konseptual bagi banyak teknik enkripsi lebih kompleks yang digunakan dalam kriptografi modern.

C. Transposisi Cipher

Transposisi Cipher adalah metode enkripsi yang mengubah urutan karakter dalam sebuah pesan tanpa mengubah karakter itu sendiri. Dalam teknik ini, urutan karakter pesan diubah sesuai dengan

suatu aturan tertentu, seperti dibaca dari kiri ke kanan atau dari atas ke bawah dalam blok-blok tertentu. Hasil dari proses transposisi ini adalah pesan yang secara esensial tetap mempertahankan karakter-karakter aslinya, tetapi susunan atau urutannya telah diubah sesuai dengan aturan yang telah ditetapkan. Namun, seperti halnya dengan banyak teknik kriptografi klasik, transposisi cipher juga rentan terhadap serangan dengan teknik analisis frekuensi atau metode kriptanalisis lainnya.

D. Implementasi Metode

Implementasi metode mengacu pada penerapan teknik atau algoritma kriptografi untuk melindungi informasi dari akses tidak sah. Proses implementasi metode kriptografi dimulai dengan pemilihan metode yang tepat sesuai dengan kebutuhan keamanan dan karakteristik sistem yang digunakan. Setelah itu, algoritma kriptografi tersebut diintegrasikan ke dalam perangkat lunak atau perangkat keras yang relevan. Pemilihan dan pengelolaan kunci juga merupakan aspek penting dalam implementasi, di mana kunci enkripsi dan dekripsi harus dikelola dengan aman dan efisien.

E. Pengujian Program

Pengujian program adalah proses sistematis yang dilakukan untuk mengevaluasi keberfungsiannya dan memastikan bahwa program tersebut berjalan sesuai dengan spesifikasi yang telah ditetapkan. Tujuan dari pengujian program adalah untuk menemukan dan mengidentifikasi bug atau kesalahan, memverifikasi bahwa program memenuhi kebutuhan fungsional dan non-fungsionalnya, serta memastikan kehandalan dan kinerja program sebelum dirilis secara resmi. Pengujian program dapat mencakup berbagai metode, seperti pengujian fungsional yang memeriksa apakah program memberikan output yang benar sesuai dengan input yang diharapkan, dan pengujian non-fungsional yang menilai aspek-aspek seperti keamanan, kinerja, dan skalabilitas. Selama proses pengujian, tim pengembangan menggunakan berbagai teknik, seperti pengujian unit, pengujian integrasi, pengujian sistem, dan pengujian penerimaan pengguna.

Hasil dan Pembahasan

A. Implementasi Kriptografi pada Teks Pesan

Implementasi kriptografi dengan menggunakan algortima caesar dan algoritma transposisi melibatkan pengenkripsian pesan kedalam cipher teks. Proses ini bertujuan untuk menjaga kerahasiaan informasi dari teks yang dikirimkan, Berikut adalah penjelasan langkah - langkah implementainya :

1. Penerapan Caesar Cipher

   Enkripsi caesar cipher mengubah plainteks menjadi cipherteks, Pesan dienkripsi melalui pergeseran karakter dalam alfabet, Penyesuaian Panjang kunci dan pergeseran kunci dapat diatur sesuai kebutuhan.

2. Penerapan Transposisi Cipher

   Dari hasil caesar cipherteks di enkripsi kembali menggunakan Transposisi cipher. Pada transposisi chipher kita menentukan sebuah kunci, angka kunci ini menentukan bagaimana urutan karakter dalam pesan akan diubah.

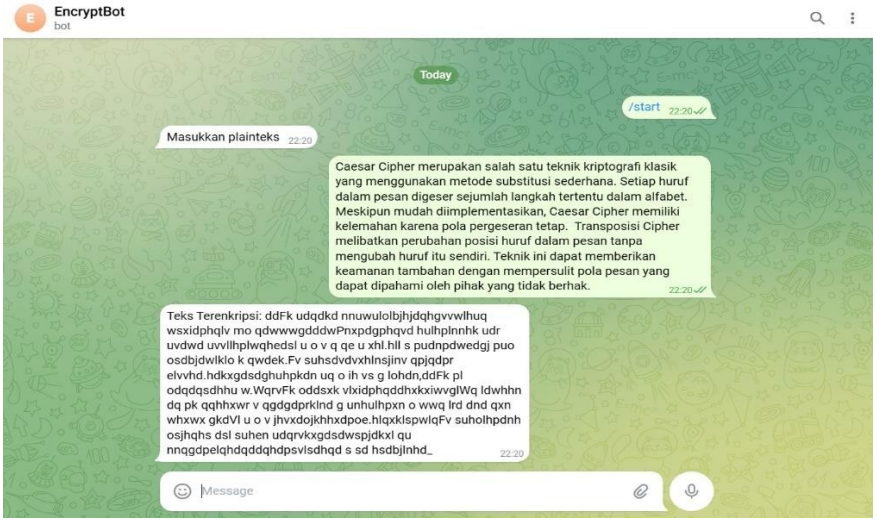
3. Keamanan

   Keuntungan dari menggunakan algoritma caesar dan algoritma transposisi dalam mengamankan teks pesan dapat meningkatkan keamanan dan privasi teks sehingga pihak yang tidak berwenang tidak bisa melihat dan mengakses pesan.

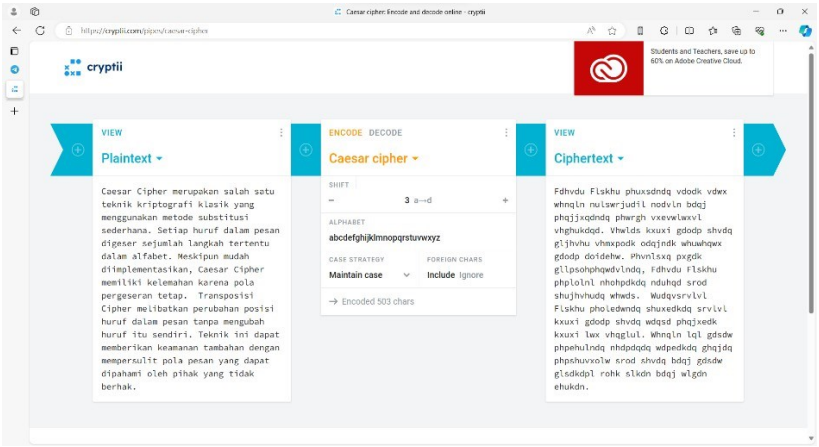
4. Pengujian dan Validasi

Uji coba dilakukan 5 kali percobaan oleh beberapa orang dengan meng*input* plainteks kedalam Bot pesan pada telegram

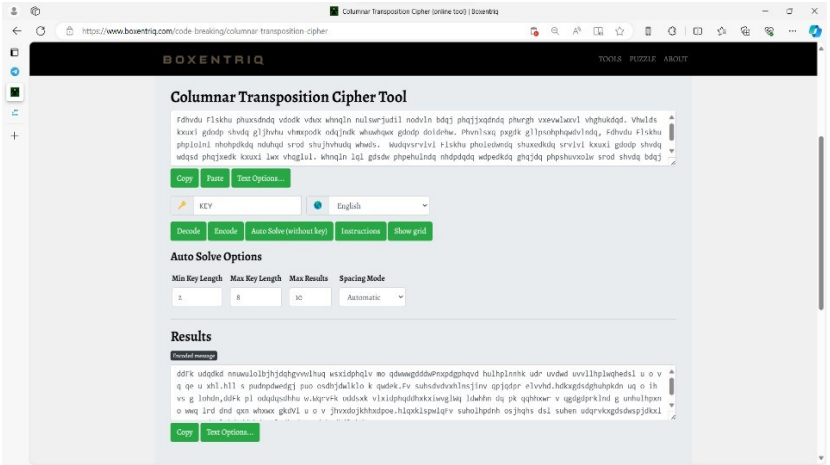
B. Output Program Kriptogafi Caesar Cipher dan Transposisi Cipher pada Aplikasi Chatting Telegram



Gambar 1. Rancangan Antarmuka EncryptBot Telegram



Gambar 2. Proses enkripsi plainteks menggunakan caesar cipher



Gambar 3. Proses Enkripsi caesar cipherteks menggunakan transposisi cipher

Kesimpulan

Pada Penelitian ini, Kami berhasil menerapkan kriptografi untuk mengenkripsi pesan teks pada aplikasi Telegram. Dengan menggabungkan algoritma Caesar Cipher dan Transposisi Cipher dapat meningkatkan keamanan pesan yang dikirim sehingga pihak tidak berwenang tidak dapat mengakses pesan tersebut.

Dengan menerapkan Caesar Cipher, pesan-pesan dienkripsi melalui pergeseran karakter dalam alfabet, memberikan tingkat keamanan dasar yang dapat melindungi pesan dari pihak yang tidak berwenang. Meskipun Caesar Cipher sederhana, penggabungannya dengan Transposisi Cipher memberikan lapisan keamanan tambahan dengan mengacak urutan karakter dalam pesan, meningkatkan kompleksitas enkripsi.

Keamanan komunikasi dalam aplikasi pesanTelegram sangat tergantung pada keamanan penyimpanan dan manajemen kunci enkripsi. Diperlukan upaya untuk melindungi kunci enkripsi agar tidak jatuh ke tangan yang tidak berwenang, karena kunci ini menjadi peran utama untuk mendekripsi pesan. Meskipun penggunaan Caesar Cipher dan Transposisi Cipher dapat meningkatkan keamanan.

Secara keseluruhan, Penelitian ini memberikan kontribusi di bidang kriptografi, dengan pendekatan yang efektif dan aman dalam mengenkripsi pesan teks pada aplikasi pesan telegram. Dengan menggabungkan Algoritma Caesar Cipher dan Transposisi Cipher, Penelitian ini masih dapat dikembangkan lebih lanjut dalam mengamankan komunikasi digital dan melindungi privasi khususnya pada aplikasi pesan Telegram.

Daftar Rujukan

[1] Sholehah, Alfiatus (2022) Modifikasi Caesar Cipher untuk menghasilkan Readable Ciphertext.

[2] Amrulloh, Muhammad Karim (2021) Penyandian model kriptografi playfair cipher dengan menggunakan metode shiftrows.

[3] Hasibuan, N.R (2022) Implementasi Algoritma Simple Columnar Transposition Dalam Mengamankan Informasi.

[4] Prabowo, Ridho (2022) Penerapan Metode Affine Cipher Untuk Peningkatan Keamanan Dokumen dengan Teknik Kongruensi Linear. Other thesis, Fakultas Sain dan Teknologi.

[5] Agustina, Laura (2021) Membangun super enkripsi dengan Vigenere Cipher dan Bifid Cipher menggunakan pemrograman python untuk mengamankan pesan. Undergraduate thesis, Universitas Islam Negeri Maulana Malik Ibrahim.

[6] Saputro, Firdaus Adji (2020) Implementasi algoritma One Time Pad Cipher dan transformasi Rail Fence Cipher pada pesan teks. Undergraduate thesis, Universitas Islam Negeri Maulana Malik Ibrahim.

[7] Arifanda, Muhammad Dendy (2021) Modifikasi Rail Fence Transposition Cipher Dengan Chess Board Pattern. Undergraduate thesis, Universitas Islam Negeri Maulana Malik Ibrahim.

[8] Hana, Muhammad Yusrul (2021) Implementasi algoritma One Time Pad Cipher dan transformasi Myszkowski Cipher pada pesan teks. Undergraduate thesis, Universitas Islam Negeri Maulana Malik Ibrahim.

[9] Hasibuan, Chyndy Astika Dani (2021) Implementasi Kriptografi Dalam Penyisipan Pesan Pada Citra Digital Menggunkan Metode Playfair Cipher Dan Least Significant Bit (LSB). Skripsi thesis, Universitas Islam Negeri Sumatera Utara Medan.

[10] Nasution, Adnan Buyung. (2019). "IMPLEMENTASI PENGAMANAN DATA DENGAN MENGGUNAKAN" 3 (1): 1–6.

[11] Adangbain, J. K., & Bata, E. S. (2021). PEMANFAATAN BOT TELEGRAM SEBAGAI MEDIA INFORMASI

DAN LAYANAN AKADEMIK DENGAN METODE WEBHOOK.

[12] R. Feraldi, A. Khairuna, M. A. Hasan, R. Rezky, and H. Ramadhan, "KOMBINASI ALGORITMA KRIFTOGRAFI CAESAR CIPHER DAN PERMUTATION CIPHER UNTUK PESAN TEKS MENGGUNAKAN PYTHON", RJOCS , vol. 7, no. 1, pp. 76–86, Jan. (2021).

[13] Gusmana, R., Haryansyah, & Adimulya Dyas Wibisono. (2023). Implementasi Algoritma Hill Cipher Menggunakan Kunci Matriks 2x2 Dalam Mengamankan Data Teks.

[14] Chaerul Umam, Lekso Budi Handoko, Christy Atika Sari, Eko Hari Rachmawanto, Lucky Arif Rahman Hakim (2022). "Kombinasi Vigenere dan Autokey Cipher dalam Proses Proteksi SMS Berbasis Android"

[15] Zailani, R., Khairil, K., & Akbar, A. (2023). Android-Based Cryptography Applications Using The Rail Fence Cipher Algorithm