A Review on Pangamanan Pesan Menggunakan Kriptografi Caesar Cipher dan Steganografi EOF pada Citra

JOFAN FATHURAHMAN[1]

Program Studi Teknik Informatika, Fakultas Ilmu Komputer
Universitas Duta Bangsa Surakarta

ABSTRACT

Security in the protection of sending messages is a matter that must be considered, because the more the development of the age, the more sophisticated the technology. So that security in sending messages and data communication should be of more concern. Therefore we need a method or algorithm that can protect the message to be sent to the recipient of the message. The algorithm that can be used in encrypting is Caesar Cipher, as a cryptographic coding technique for messages so that messages that look difficult to read and solve. As for the method of inserting messages on encrypted image media using the End of File (EOF) steganography method, which is the method used directly at the end of the file. In the work of securing techniques of messages on this system, using various sizes of images or images that will be inserted a coded secret message or encryption whose capacity is not much different from the photos or images to be used. The conclusion of this study is that the application of the Caesar Cipher Algorithm can be used as a message security technique even though the algorithm is so simple but the level of security is assisted by the End of File (EOF) method to insert the encryption results from the Caesar Cipher algorithm so that the security level it has is sufficient to protect message information to be safe from eavesdroppers or hackers of the message that is not responsible or as a protection of data held.

Keywords: Caesar Chiper, end of file, Message Security

ABSTRAK

Keamanan dalam perlindungan pengiriman pesan merupakan hal yang harus diperhatikan, dikarenakan semakin berkembangnya zaman maka semakin canggih pula teknologi. Sehingga keamanan dalam pengiriman pesan maupun komunikasi data harus menjadi perhatian yang lebih. Oleh sebab itu dibutuhkan suatu metode atau algoritma yang dapat melindungi pesan yang akan dikirimkan kepada penerima pesan. Adapun Algoritma yang dapat digunakan dalam pengenkripsian yaitu Caesar Cipher, sebagai teknik kriptografi pengkodean pesan agar pesan yang terlihat sulit dibaca dan dipecahkan. Sedangkan untuk metode penyisipan pesan pada media gambar yang telah dienkripsi menggunakan steganografi metode End Of File (EOF), yaitu metode yang digunakan langsung pada akhir file. Dalam pengerjaan teknik pengamanan pesan pada system ini, menggunakan berbagai ukuran citra atau gambar yang akan disisipkan pesan rahasia yang telah dikodekan atau enkripsi yang kapasitasnya tidak jauh beda dengan foto atau gambar yang akan digunakan. Kesimpulan dari penelitian ini adalah bahwa penerapan Algoritma Caesar Cipher bisa dijadikan teknik pengamanan pesan dengan baik walaupun algoritmanya yang begitu sederhana namun tingkat keamanannya dibantu dengan metode End Of File (EOF) untuk menyisipkan hasil enkripsi dari algoritma Caesar Cipher sehingga tingkat keamanan yang dimiliki cukup untuk melindungi pesan informasi agar aman dari para penyadap atau peretas pesan yang tidak bertanggung jawab maupun sebagai perlindungan data-data yang dimiliki

Kata kunci: **Caesar Chiper, end of file, Message Security**

1. PENDAHULUAN

1.1. Latar Belakang

Keamanan dalam perlindungan pengiriman pesan merupakan hal yang harus diperhatikan, dikarenakan semakin berkembangnya zaman maka semakin canggih pula teknologi. Kerentanan dalam system layanan online berpotensi diserang peretas, serangan pada layanan online dapat terjadi kapan saja dan butuh solusi untuk

memperbaikinya[1]. Layanan-layanan mesin pencari selalu berkembang yang berdampak pada privasi pengguna termasuk opsi fitur untuk menjelajahi Internet secara pribadi[2]. Sehingga keamanan dalam pengiriman pesan maupun komunikasi data harus menjadi perhatian yang lebih. Aktifitas manusia saat ini sebagian besar berhubungan dengan data, informasi, dan komunikasi, serta dalam kegiatannya secara langsung maupun tidak langsung akan berhubungan dengan perangkat teknologi computer[3]. Teknologi yang semakin canggih menjadi bagian yang tidak bisa lepas dari kehidupan masyarakat, tidak hanya melakukan kegiatan- kegiatan positif namun kegiatan-kegiatan negatif[4]. Sehingga celah-celah dalam pembobolan pengiriman pesan dizaman sekarang mudah terlihat dengan menggunakan berbagai macam penunjang baik tools aplikasi maupun melalui peretasan jaringan komunikasi data. Penjahat dunia maya terus mengubah strategi mereka untuk menargetkan media sosial yang berkembang pesat dan pengguna pesan yang ketat[5]. Manfaat teknologi memberikan banyak kemudahan kepada manusia dalam hal komunikasi. Walaupun memberikan dampak positif, kemajuan teknologi informasi dan telekomunikasi juga memberikan dampak negative juga yaitu banyaknya kejahatan yang berkaitan dengan aplikasi internet[6]. Dampak dari banyaknya kejahatan menggunakan teknologi informasi khususnya menggunakan Internet, dapat kita lihat dari beberapa kejahatan sering dilakukan dalam bentuk serangan yang terjadi dalam lembaga atau lembaga tertentu[7]. Oleh sebab itu dibutuhkan suatu metode atau algoritma yang dapat melindungi pesan yang akan dikirimkan kepada penerima pesan. Sehingga pesan yang hendak dikirimkan dapat dilindungi privasinya. Adapun Algoritma yang dapat digunakan dalam pengenkripsian yaitu Caesar Cipher, sebagai teknik kriptografi pengkodean pesan agar pesan yang terlihat, sulit dibaca dan dipecahkan. Sedangkan untuk metode penyisipan pesan pada media gambar yang telah dienkripsi menggunakan steganografi metode End Of File (EOF), yaitu metode yang digunakan langsung pada akhir file. Kriptografi sudah ada sejak dahulu sebelum masa digital berkembang, yang digunakan untuk keamanan privasi agar lebih aman, contohnya militer, utusan-utusan negara dan mata-mata, yang digunkan untuk menjaga kerahasiaan komunikasi yang dilakukan agar tidak tersebar atau tidak diketahui oleh pihak lain. Namun dizaman digital sekarang kriptografi tidak hanya sekedar keamanan komunikasi akan tetapi juga bisa digunakan untuk pengamanan data integritas, keaslian dan pemalsuan atau manipulasi [8]. Kriptografi Caesar Cipher merupakan salah satu teknik enkripsi yang terkenal dan sederhana dalam penanganan pengamanan pesan didunia. Sandi Caesar merupakan sandi subtitusi dimana.

2. Pembahasan

2.1. Pengumpulan Data

Tahap awal yang dilakukan adalah pengumpulan data mengenai kebutuhan yang dilakukan terhadap permasalahan yang akan diangkat atau dianalisa. Pengumpulan data disini berupa jurnal terkait sebagai pembanding atau referensi tambahan yang dapat melengkapi penelitian dan buku sebagai penjelasan komperehensif terhadap penelitian yang dilakukan.**Pengertian Informasi**

Informasi adalah data yang telah diklasifikasi atau diolah atau diinterprestasi untuk digunakan dalam proses pengambilan keputusan. (Tumini & Fitria, 2021)

2.2. Analisis Sistem

Referensi terkait merupakan hal penting dalam pendalaman masalah yang akan dilakukan sebagai rujukan atau perbandingan berupa Jurnal terkait yang berhubungan dengan Steganografi dan Kriptografi khususnya metode EOF dan Algoritma Caesar Cipher. Jurnal terkait digunakan untuk pengembangan atau pembanding yang diambil berdasarkan intisari bacaan yang dilakukan dalam penelitian ini

2.3. Alur Penelitian

Alir penelitian adalah tahapan-tahapan yang dikerjakan dalam penelitian mulai dari awal, proses dan akhir. Konsep yang dibangun alir penelitian adalah penyesuaian yang dilakukan dalam analisa sistem sesuai dengan algoritma yang dibangun mulai dari pemilihan stego image (wadah penampung), proses enkripsi menggunakan algoritma Caesar Cipher kemudian encode ciphertext menggunakan metode End of File (EOF), sebagaimana dalam Gambar 1

2.4. Analisis Terkait

Setelah membaca dan memahami jurnal terkait maka setelah itu akan dilakukan analisa masalah mengenai bidang Kriptografi dan Steganografi. Analisa dilakukan dengan cara memahami kelemahan-kelemahan yang terdapat dalam Jurnal penelitian sebelumnya dan mengambil pemahaman

2.5. . Enkripsi Caesar Cipher

kutnya dari susunan alphabet. Caesar cipher tidak memiliki kunci, keamanan algoritma terletak pada kerahasiaan algoritmanya (hanya raja Julius Caesar para gubernurnya yang tahu). Dalam buku Practical Workbook: Information Theory, 4th edition, Department of Computer & Information System Engineering NED University of Engineering & Technology, Karachi, Pakistan [15], dijelaskan bahwa metode Caesar cipher yang digunakan menggunakan prinsip modulo 26

2.6. . Metode End of File (EoF)

Dalam metode EOF memiliki tahapan-tahapan dalam penyisipan pesan agar pesan dapat disisipkan dengan baik dan tertata sesuai dengan sifat dari metode EOF. Adapun tahapan encode dari metode EOF yaitu, mengubah pesan menjadi nilai desimal, mencari letak nilai akhir dari piksel citra, memberikan sebuah tanda khusus sebagai pengenal pada pesan rahasia dan juga memberikan tanda desimal. Adapun pada tahapan proses decode atau pengungkapan pesan rahasia, maka proses yang dibutuhkan adalah mengetahui letak tanda pengenal dan mengambil nilai decimal dari pesan rahasia kemudian mengubah nilai desimal menjadi sebuah pesan. Tahapan encode pesan rahasia

3. Penutup

Memberikan pernyataan bahwa apa yang diharapkan sebagaimana dinyatakan dalam “Pendahuluan” akhirnya dapat diperoleh hasil dalam “Hasil dan Pembahasan”, sehingga terdapat kesesuaian. Selain itu dapat juga ditambahkan prospek pengembangan dari hasil penelitian dan aplikasi lebih jauh yang menjadi prospek kajian berikutnya. Kesimpulan dari penelitian ini adalah bahwa penerapan Algoritma Caesar Cipher bisa dijadikan teknik pengamanan pesan dengan baik walaupun algoritmanya yang begitu sederhana dikarenakan algoritma yang digunakan adalah Kriptografi Klasik namun tingkat keamanannya dibantu dengan metode EOF untuk menyisipkan pesan rahasia dari algoritma Caesar Cipher sehingga tingkat keamanan yang dimiliki cukup untuk melindungi pesan informasi agar aman dari para penyadap atau peretas pesan yang tidak bertanggung jawab maupun sebagai perlindungan data-data yang dimiliki. Untuk pengembangan selanjutnya bisa menggunakan algoritma yang kompleks atau Kriptografi moderen contohnya, DES, Triple DES, AES, RC4, A5, dan sebagainya. Begitupun untuk Metode Steganografi bisa menggunakan metode lainnya. Kemudian pada program yang ingin dibuat bisa menggunakan dalam bentuk visual yang lebih baik lagi dalam bentuk aplikasi.