P.Issn : 2808-859X
E.Issn : 2809-0853

DUAL SECURITY SYSTEM ON VIDEO WITH VIGNERE CIPHER ALGORITHM AND RAILFENCE CIPHER ALGORITHM

Zulfahmi Syahputra
Universitas Pembangunan Panca Budi, Medan, Sumatera Utara, Indonesia

Kewords:
Double Security; Videos; Vigenere Algorithm Cipher; Railfance Algorithm.

***Correspondence Address:**
zulfahmi@dosen.pancabudi.ac.id

Abstract: The vignere cipher algorithm is a classic algorithm and the railfance cipher algorithm is a modern algorithm. In this research, it combines the vignere cipher algorithm and the railfance cipher algorithm in securing video files with the aim of producing double security so that private video files can be secured with the system built. The research results obtained double security with the performance of encrypted video files that are not easy to break.

INTRODUCTION

Encryption is the science and art of maintaining the confidentiality of messages by encoding them in a form whose meaning cannot be understood. Encryption and decryption are part of cryptography itself, and the encrypted message is called plaintext. In cryptography, Vignere Chiper is a simple polyalphabetic encryption system. The polyalphabetic system encrypts text consisting of many characters at once. The Vignere-Chiper cipher uses a permutation shift function, similar to the Caesar cipher. The algorithm is a technique used when working on the Vigenere Cipher, which is almost the same as the Caesar Cipher. In other words, the plain text in the message is encrypted using the same techniques used to encrypt characters. Messages are encrypted based on the distance between alphabetic key values. Railfance or what is known as zigzag chipper is a way of coding character positions changing from diagonal down to maximum. This chipper changes the position and arrangement of characters. Because this cipher does not have a specific key, this cipher is usually systematic, so you need to pay attention to the writing level to complete it. Railfance Chipper users can apply this to secure MP4 videos, making it a security solution. However, before applying the Vignere Chipper and Railfance Chipper algorithms, the video was translated using Base64. The Base64 method is a technique for converting binary data to ASCII format.

RESEARCH METHODS

At this stage, researchers will investigate the cause of the problem and solve it later using the system. Then a diagram, or fishbone diagram, is created. The fishbone diagram is a diagram that is commonly used to identify, analyze and solve problems. The Ishikawa diagram (Fishbone diagram) is in the shape of a fish, and the structure consists of a fish head and fish bones. Fishheads contain the name or title of the identified problem. On the other hand, fish bones show the problem resulting from a different cause.

Figure 1. *Fishbone Diagram*

In the picture above, it can be seen that there are four categories causing the problems in this research, namely the Vignere Chiper algorithm, classic encryption that uses less secure substitution techniques in the information exchange process; This is an algorithm. Since classical algorithms are simpler for cryptanalysts, they must be combined with other cryptographic algorithms to make and maintain the information exchange process more secure. This research combines the Vignere chipper algorithm and the Railfance chipper algorithm. The functional requirements for a system that implements a combination of Vignere and Railfance encryption algorithms to protect video files are as follows:

1. Receiving plain text input The system searches for and reads files with the extension .mp4 and is stored on the device used or the system receives plain text input from the user manually. The system only reads video files. Next, convert using the Base64 method.
2. Key The system receives key input from the user or randomly generates a key which is used as a key for the Vignere encryption algorithm with the Railfance encryption algorithm to protect video files.

3. Message Encryption The system uses the Vignere encryption algorithm to encrypt messages with a key and generate ciphertext. Then it is encrypted again using the Railfance encryption algorithm to produce a new ciphertext.
4. Message decryption The system then reads and decrypts the stored message. The system decrypts the obtained ciphertext using keys from the Vignere and Railfance cryptographic algorithms.

RESULTS AND DISCUSSION

This system modeling uses Unified Modeling Language diagrams to describe how the system works, especially object-oriented systems. The UML diagrams used are use case diagrams, activity diagrams, and sequence diagrams.

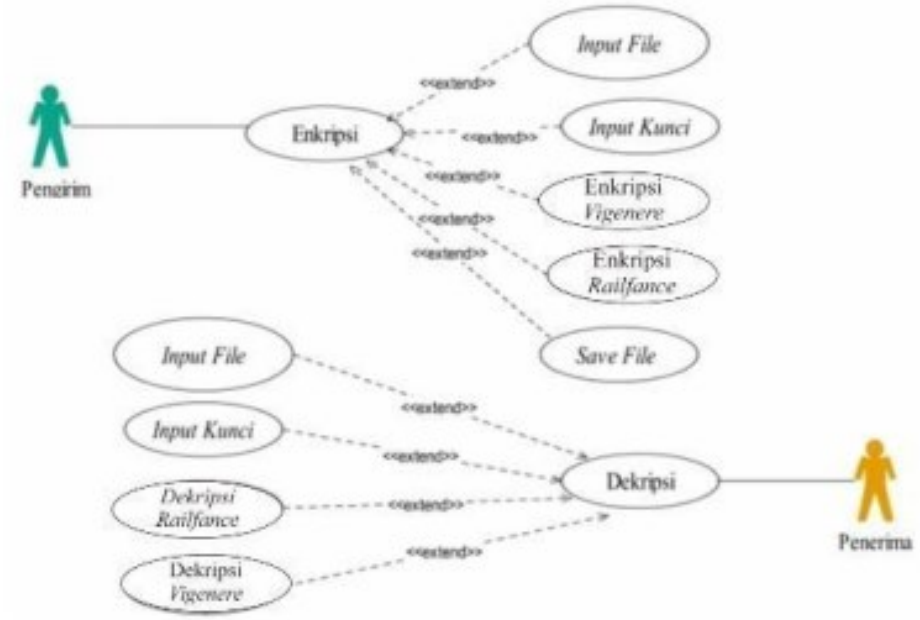

Figure 2. *Usecase Diagram*

The image above describes a workflow that sends and receives messages using the MP4 extension, represented in a use case diagram. This system is used by two actors: the sender and the recipient. The sender can carry out the encryption process, including the file entry process, key entry, Vigenere algorithm encryption, Railfance algorithm encryption, and can also save encrypted files, while the recipient can carry out the decryption process which includes: Previously encrypted saved file entry process, key

entry, Railfance algorithm encryption, and Vigenere algorithm encryption. Activity diagrams represent the flow of activities between users and systems and are created in detail and sequentially according to the interactions between users and the system they create.

System testing is carried out to find out whether the system built is in accordance with system analysis and system design. Apart from that, system testing is also intended to prove that the system being built can function properly. System encryption testing is carried out by inputting a video file, then the system automatically translates the video using Base64 technology. Results are available in plain text. After receiving the plaintext, the sender enters the key in the form of a combination of characters in the algorithm menu to decrypt the Vigenere cipher and produces ciphertext 1, after that the sender enters the key in the form of a combination of characters. Entering the Encryption and Decryption Railfence number algorithm menu will produce a ciphertext and then the data will be stored in the database and automatically generates unopenable video output.

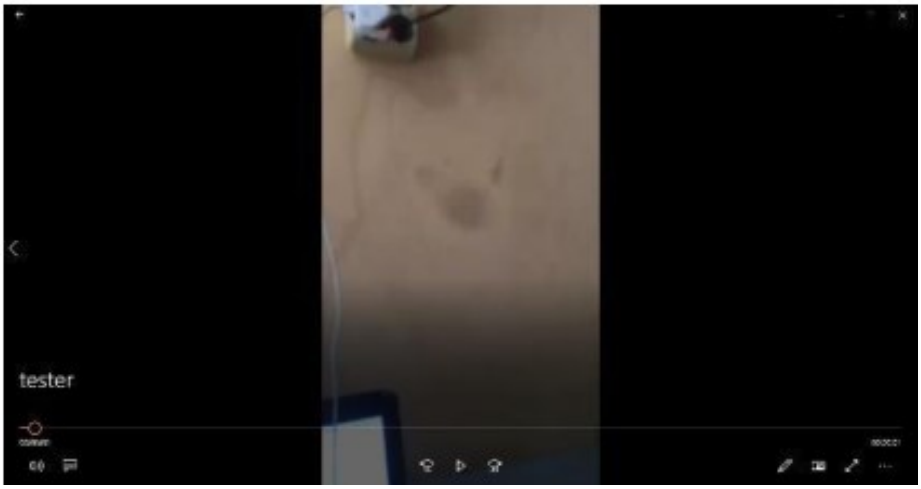

Figure 3. Testing Video

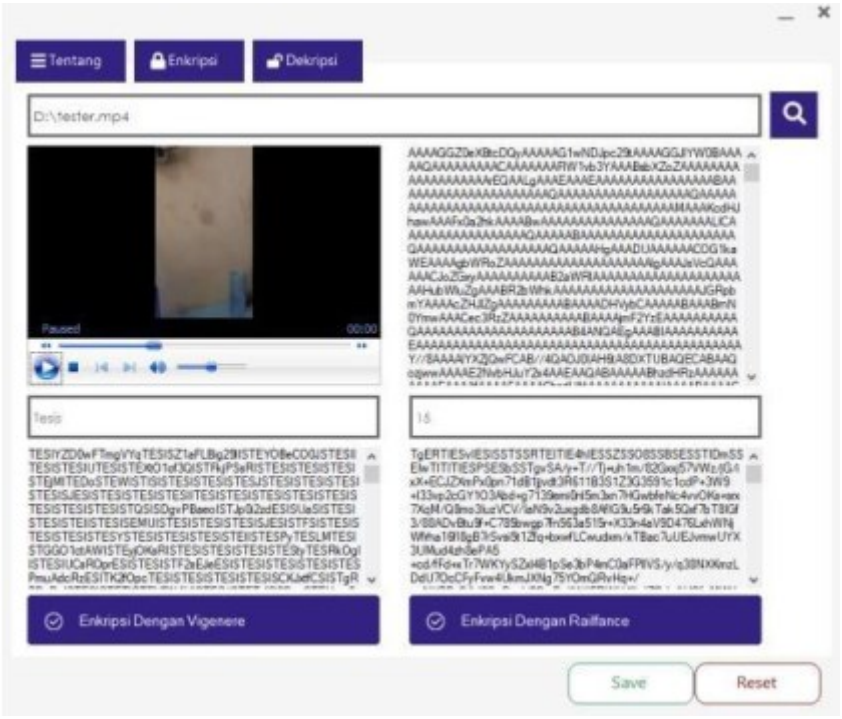

Figure 4. Encryption

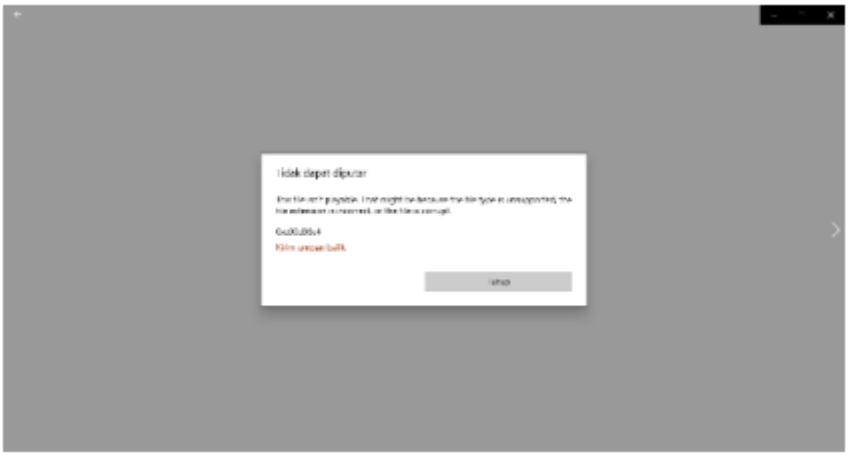

Figure 5. Encryption Result

The decryption system test was carried out by inserting an encrypted MP4 video file. The system then automatically translates the video using Base64 technology. Results are available in plain text. After receiving the plaintext, the sender enters the key in the form of a combination of numbers into the Railfence encryption algorithm menu, which decrypts it and produces the ciphertext. The sender then enters the key in the algorithm menu in the form of a combination of Vigenere Cipher characters, then it is decrypted and the ciphertext is generated, after that the data is stored in the database and a video output that can be opened is generated automatically.

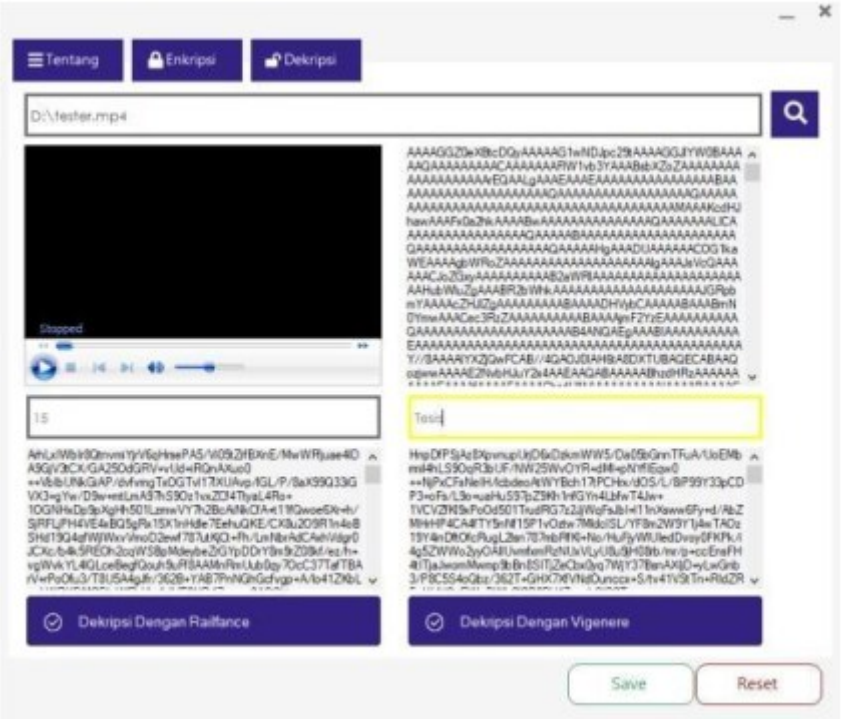

Figure 5. Decryption Result

CONCLUSION

In this research, we combine Vigenere encryption algorithm and Railfance encryption algorithm to protect MP4 files. MP4 files are converted to Base64 and encrypted with these two algorithms.

REFERENCE

Riyus, Dony., 2008, Pengantar Ilmu Analisis, Kriptografi: Teori, dan Implementasi. Penerbit Andi, Yogyakarta.

Arsyad, Azhar. 2013. Media Pembelajaran. Jakarta: Raja Grafindo Persada.

Bella Ariska, Suroso, Jon Endri., 2018. "Rancangan Kriptografi Hybrid Kombinasi Metode Vigenere Cipher Dan Elgamal Pada Pengamanan Pesan Rahasia" ITN Malang, 3 Pebruari 2018 ITN Malang, 3 Februari.

Kadir, Abdul. 2003. Pemrograman C++. Yogyakarta: Penerbit ANDI Yogyakarta.

Maulana, GG. 2017. "Pembelajaran Dasar Algoritma dan Pemrograman Menggunakan El-Goritma Berbasis Web," Jurnal Teknik Mesin, Vol. 06: 69.

Sanjaya, Dwi. 2003. Asyiknya Belajar Struktur Data di Planet C++. Jakarta: PT. Elex Media Komputindo.

Tsauri, MS. 2019. Implementasi Algoritma Kriptografi Railfance untuk Mengamankan Teks Ujian. Universitas Negeri Semarang.

Utami, Erna & Sukrisno. 2005. 10 Langkah Belajar Logika dan Algoritma, Menggunakan Bahasa C dan C++ di GNU/Linux. Yogyakarta: Penerbit ANDI Yogyakarta.

Pabokory, FN. Astuti, IF & Kridalaksana, AH. 2015 "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," Jurnal Informatika Mulawarman, vol. 10 No. 1, Februari.