

INTISARI

Kemajuan era digitalisasi meningkatkan intensitas pertukaran data melalui internet. Berkembangnya teknologi juga dapat meningkatkan kerentanan keamanan dalam jaringan, sehingga keamanan dan kerahasiaan data saat ini harus semakin dijaga. Beberapa macam cara dan metode dapat digunakan dalam menjaga kerahasiaan data yang akan dikirimkan, salah satunya adalah dengan menggunakan kriptografi. Seperti halnya pada sistem autentikasi yang memuat data rahasia berupa *password*, data tersebut harus dilindungi agar tidak digunakan oleh seseorang yang tidak bertanggung jawab. Pemilihan algoritma kriptografi harus dipilih sesuai dengan kebutuhan dalam menjaga kerahasiaan data yang dimiliki. Caesar Cipher, Vigenere Cipher, dan AES (*Advanced Encryption Standard*) adalah algoritma kriptografi yang dapat digunakan dalam menjaga keamanan data. Setiap algoritma pastinya akan mengamankan data, namun kombinasi dari ketiga algoritma tersebut pastinya akan meningkatkan keamanan dari data tersebut. Penelitian ini akan menguji kombinasi gabungan algoritma terbaik dari Caesar Cipher, Vigenere Cipher, dan AES. Algoritma yang dianggap memiliki keamanan yang baik akan diimplementasikan pada sistem autentikasi sederhana. Keamanannya akan semakin baik apabila waktu dekripsi kombinasi algoritma semakin lama dan akan lebih efektif apabila memiliki waktu komputasi yang singkat. Penelitian ini bertujuan untuk mengusulkan metode kombinasi algoritma kriptografi agar dapat meningkatkan keamanan data

Kata Kunci: Kriptografi, Algoritma, Caesar Cipher, Vigenere Cipher, AES, Sistem Autentikasi Sederhana

ABSTRACT

The advancement in the digitalization era increases data transmission through the internet. Technology development can also increase the security vulnerability in the network, therefore security and confidentiality of data must be protected more. Several ways can be used to keep the security of data that will be sent, one of the methods is using cryptography. As well in an authentication system that contains sensitive content like passwords, that data must be protected to not be used by someone who does not deserve it. The algorithm of cryptography must be chosen by needs in the keep of data security. Caesar Cipher, Vigenere Cipher, dan AES (Advanced Encryption Standard) are algorithms of cryptography that can be used to keep the security of data. Each algorithm definitely will secure the data, but the combination of the three algorithms can increase the security of data. This research will be testing the best combination based on three algorithms from Caesar Cipher, Vigenere Cipher, and AES. The best algorithm that has good security will be implemented in a simple authentication system. Security of data will be better if the time of decryption is getting longer and will be effective if the time of computation is getting shorter. The final result that wants to be reached in this research is cryptography algorithm combination method can increase data security.

Keyword: *Cryptography, Algorithm, Caesar Cipher, Vigenere Cipher, AES, Simple Authentication System*