

ABSTRAK

Nama : Hasburrahman
NIM : 41519120055
Program Studi : Teknik Informatika
Judul Laporan Skripsi : Penerapan Algoritma Advanced Encryption Standard Untuk Pengamanan Dokumen Berbasis Website.
Pembimbing : Dr. Afiyati, S.Si., M.T

Kendala dalam penilaian ini yaitu tentang keamanan suatu informasi atau data yang merupakan hal sangat penting untuk diperhatikan dalam menjaga kerahasiaan informasi atau data, terutama informasi. Hal tersebut dikarenakan sering kalinya informasi atau data yang penting atau bersifat rahasia dapat di ambil oleh orang yang tidak bertanggung jawab.

Oleh karena itu penulis membuat aplikasi ini bertujuan untuk meng-enkripsi semua jenis file. Untuk mengirim suatu informasi atau data agar bisa sampai ke penerima dalam bentuk yang autentik diperlukan sebuah aplikasi enkripsi dan dekripsi untuk merahasiakan data yang dikirim tersebut. Untuk menerapkan sistem enkripsi dan dekripsi tersebut digunakan algoritma advanced encryption standard (AES). Penulis menggunakan metode blackbox sebagai pengujian terhadap aplikasi yang buat. Hasil yang di dapat berdasarkan pengujian aplikasi bahwa penerapan algoritma advanced encryption standard (AES) pada aplikasi pengamanan enkripsi dan dekripsi berjalan dengan baik dan jika hasil file enkripsi sesuai dengan size yang ditentukan maka enkripsi berhasil dilakukan, dan jika file enkripsi melebihi kapasitas size yang di tentukan maka enkripsi tidak dapat dilakukan. Demikian juga hasil file dekripsi jika enkripsi berhasil dilakukan maka dekripsi akan berhasil dilakukan juga, karena dekripsi file tergantung pada keberhasilan proses enkripsi.

Kata Kunci: Kriptografi, Algoritma AES, Enkripsi dan Dekripsi, Keamanan data

ABSTRACT

Name : Hasburrahman
NIM : 41519120055
Study Program : Informatics Engineering
Title Thesis : Implementation of Advanced Encryption Standard Algorithm for Document Security on Website-Based Platform.
Counsellor : Dr. Afiyati, S.Si., M.T

The constraint in this assessment revolves around the security of information or data, which is a crucial aspect to consider in maintaining the confidentiality of information, especially sensitive information. This is because frequently important or confidential information and data can be accessed by unauthorized individuals.

Therefore, the author developed this application with the aim of encrypting all types of files. To transmit information or data so that it reaches the recipient in an authentic form, an encryption and decryption application is needed to secure the transmitted data. The implementation of the encryption and decryption system utilizes the Advanced Encryption Standard (AES) algorithm. The author employed the blackbox method for testing the created application. The results obtained from the application testing indicate that the implementation of the Advanced Encryption Standard (AES) algorithm in the encryption and decryption security application operates smoothly. If the size of the encrypted file matches the specified size, the encryption is considered successful. Conversely, if the encrypted file exceeds the designated size capacity, encryption cannot be performed. Similarly, the decryption process will be successful if the encryption is performed successfully, as the decryption of the file depends on the success of the encryption process.

Keywords: Cryptography, AES Algorithm, Encryption and Decryption, Data Security