IMPLEMENTASI PENGAMANAN DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD-128 (AES-128)

MUHAMMAD HISYAM RIZKY FAIZAL
(Pembimbing : Heribertus Himawan, M.Kom)
Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro
www.dinus.ac.id
Email : 111201106253@mhs.dinus.ac.id

ABSTRAK

Kriptografi merupakan salah satu ilmu yang digunakan untuk menjaga keamanan dan kerahasiaan data atau informasi sehingga data tidak dapat diketahui oleh pihak-pihak yang tidak berwenang. Proses pertukaran data atau informasi sangat sering dilakukan sehingga aspek keamanan terhadap isi dokumen sangat perlu untuk mendapat perhatian khusus. Penelitian ini akan mengimplementasikan kriptografi algoritma AES-128 untuk menyandikan file digital, khususnya adalah file dokumen DOC, dokumen PDF, dokumen PPT, dokumen TXT, dan dokumen XLS. Enkripsi dilakukan dengan menggunakan kunci tertentu, sehingga menghasilkan cipherteks yang tidak dapat dibaca ataupun dimengerti. Cipherteks tersebut dikembalikan seperti semula jika di dekripsi menggunakan kunci yang sama sewaktu mengenkripsi file tersebut. Perangkat lunak yang digunakan untuk merancang aplikasi adalah Netbeans 7.4.0. Algoritma AES dipilih untuk metode pengimplementasian pengamanan data dokumen. Penelitian ini secara khusus akan mengamati kebutuhan waktu untuk proses enkripsi dan dekripsi, serta ukuran file yang dihasilkan dari proses tersebut.

Kata Kunci : Kriptografi, Algoritma AES-128, Enkripsi, Dekripsi, File Dokumen

IMPLEMENTATION OF DOCUMENT SECURITY USING ADVANCED ENCRYPTION STANDARD-128 (AES-128) ALGORITHM

MUHAMMAD HISYAM RIZKY FAIZAL
(Lecturer : Heribertus Himawan, M.Kom)
Bachelor of Informatics Engineering - S1, Faculty of Computer Science, DINUS University
www.dinus.ac.id
Email : 111201106253@mhs.dinus.ac.id

ABSTRACT

Cryptography is the science that is used to maintain the security and confidentiality of the data or information so that data can not be known by the parties were not authorized. Data or information exchange process is often done so that the security aspects of the content of the document is very necessary to get special attention. This research will implement cryptographic algorithms AES-128 to encrypt digital files, in particular is a DOC document files, PDF document, PPT document, TXT document and XLS document. Encryption is done using a specific key, resulting ciphertextcan not be read or understood. The ciphertext restored if it is decrypted using the same key when encrypting the file. The software used to design applications is Netbeans 7.4.0. AES algorithm selected for implementation of the method of data security document. Specifically the study will look at needs time to process the encryption and decryption, as well as the size of the file generated from the process.

Keyword : Cryptography, AES-128 algorithm, Encryption, Decryption, Document File