

APLIKASI PENGAMANAN FILE DAN PESAN TEKS MENGUNAKAN ALGORITMA AES 256 DAN SHA 256 BERBASIS ANDROID

Hadi Fajar Wiguno

Abstrak

Enkripsi dan Dekripsi dalam Kriptografi merupakan pengamanan yang tepat untuk melindungi data agar tidak mudah dibuka atau dilihat oleh orang yang tidak berwenang. Salah satu teknik Enkripsi dan Dekripsi adalah Algoritma AES yang merupakan algoritma yang menggunakan kunci simetri. Algoritma ini mempunyai nama asli yaitu Algoritma Rijndael. Aloritma Rijndael merupakan pemenang kompetisi yang diselenggarakan oleh NIST (National Institutes of Standards and Technology) dan menjadi algoritma AES (Advanced Encryption Standar). Dengan Menggunakan Algoritma AES, aplikasi ini dapat melakukan Enkripsi dan Dekripsi data berupa dokumen, pesan teks, gambar, suara, dan video. Dalam penelitian ini menggunakan AES 256 dan SHA 256. Aplikasi ini dibangun untuk perangkat dengan sistem operasi android dan bahasa pemrograman java.

Kata Kunci: AES-256, Dekripsi, Enkripsi, Kriptografi, SHA-256

APLIKASI PENGAMANAN FILE DAN PESAN TEKS MENGUNAKAN ALGORITMA AES 256 DAN SHA 256 BERBASIS ANDROID

Hadi Fajar Wiguno

Abstract

Encryption and decryption in cryptography is the proper safeguards to protect the data from being easily opened or viewed by unauthorized persons. One of the techniques of encryption and decryption Algorithm is AES which is the algorithm that the key uses symmetry. This algorithm has the original name is the Rijndael algorithm. Rijndael alorithm is the winner of the competition was organized by NIST (National Institutes of Standards and Technology) and becomes the algorithm AES (Advanced Encryption Standard). By using the AES Algorithm, this application can perform the encryption and decryption of data in the form of documents, text messages, images, sounds, and videos. In this study using AES 256 and SHA 256. This application is built for devices with the android operating system and java programming language.

Keywords: AES-256, Cryptography, Decryption, Encryption, SHA-256