IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) DAN HASH UNTUK IDENTIFIKASI KEASLIAN IJAZAH

Moh. Mulki Ridho

Abstrak

Penelitian ini dilakukan untuk mengetahui keaslian suatu ijazah dengan cepat. Masalah pemalsuan ijazah merupakan salah satu aspek penting dari suatu studi yang telah dilakukan. Dalam hal ini, sangat terkait dengan betapa pentingnya keaslian ijazah tersebut sebagai salah satu bukti kelulusan seseorang dalam studi atau pendidikannya. Pada umumnya ijazah yang ada hanya memerlukan legalisasi untuk menyatakan keasliannya atau dengan cara menghubungi pihak atau lembaga yang mengeluarkan ijazah tersebut. Proses ini sangat membutuhkan waktu yang lama dan kurang efisien. Oleh karena itu, penelitian ini akan mengunakan fungsi *hash* dengan menggunakan algoritma MD5 sebagai nilai integritas dari ijazah tersebut dan memanfaatkan algoritma AES sebagai keamanan dalam basis data. Dalam penelitian ini, MD5 dapat menghasilkan sidik jari digital dari informasi ijazah yang ada sehingga mempunyai nilai integritas digital untuk membuktikan keaslian suatu ijazah tersebut. Akan tetapi nilai integritas ini belum cukup untuk mengamankan data ijazah. Maka dari itu penelitian ini menerapkan algoritma AES sebagai keamanan untuk menjaga keamanan nilai integritas ini.

Kata kunci : Ijazah, *Message Digest* 5 (MD5), *Advance Encryotion Standard* (AES).

IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) DAN *HASH* UNTUK IDENTIFIKASI KEASLIAN IJAZAH

Moh. Mulki Ridho

Abstract

This study was conducted to determine the authenticity of a certificate quickly. Certificate forgery problem is one of the important aspects of a study that has been done. In this case, it is related to the importance of the authenticity of the certificate as proof of someone that has already passed in the study or education. In general, certificate requires legalization process for stating its authenticity or by contacting the person or institution that published the certificate. This process takes a long time and inefficient. Therefore, this study will use the hash function by using the MD5 algorithm as the value of the integrity of the certificate and utilizing AES algorithm as security in the database. In this study, MD5 can produce a digital fingerprint of the existing certificate information that has value digital integrity to prove the authenticity of a certificate. But the integrity is not enough to secure the data certificate. Therefore, this study will implement the AES algorithm to maintain the security of this integrity value.

Keyword : Certificate, Message Digest 5 (MD5), Advance Encryotion Standard (AES).