Paper 181 – Technology

IMPLEMENTATION ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM AND HASH ALGORITHM TO IDENTIFY CERTIFICATE AUTHENTICITY

Moh. Mulki Ridho, Henki Bayu Seta and Theresia Wati
Universitas Pembangunan Nasional "Veteran" Jakarta
kii.ankii@gmail.com, henkiseta@upnvj.ac.id, theresia_waty@yahoo.com

ABSTRACT

Diploma Certificate is a symbol or sign for people who have completed the learning process which is taken in accordance with education level that are taken. Currently, there is a lot of fake diploma certificate. The diploma certificate can be regarded as a false certificate if the certificate issues has been out by the university or institute does not have accreditation or the certificate obtained without going through the learning process correctly. To avoid the use of fake certificate it should be required a technology that can do the checking process. The checking process carried out by applying the methods of encryption and decryption algorithms using the Advanced Encryption Standard (AES) as a security in a database and the hash algoritms on the Message Digest 5(MD5) as the integrity value from the certificate. In this study, MD5 can produce a digital fingerprint from the certificate information which is contained so can have a digital integrity to prove the authenticity of the certificate. But, integrity is not enough to secure the certificate. Therefore, this study applied the AES algorithm as security to safeguard the integrity value of this.

Keywords: Certificate, Message Digest 5 (MD5), Advanced Encryption Standard (AES), Hash Algorithm, Certificate Authenticity.