ABSTRACT

DATABASE SECURITY SYSTEM DESIGN USING MERKLE–HELLMAN KNAPSACK ENCRYPTION AND ADVANCED ENCRYPTION STANDARD (AES)

by

AZIZ TRI NUGROHO

19102253

The information aspect needs to implement security so that data leakage does not occur. according to BSSN (National Cyber and Crypto Agency), Lieutenant General TNI (Purn) Hinsa S. has revealed that cyber attacks are increasing every year, especially in 2019 which experienced 182,034,863 cyber attacks while in 2020 it had reached 423,244. 053 attacks. This is of course a signal that digital security must be improved. Security has an important role in a system. One of them is securing databases or databases. This problem inspired researchers to conduct this research. This study uses two-stage encryption using merkle-hellman knapsack and AES 256 on a system built with PHP Native-based website objects stored on web hosting and using MySQL as the database type with implementation of encryption using the OpenSSL library. The results of this test produce two-stage encryption. merkle-hellman knapsack and AES 256 I can be implemented on a column other than id_member which is shown where the column other than id_member is encrypted and an error occurs when doing SQL injection on a website.

Keywords: Encryption, Database, Merkle-Hellman Knapsack, AES, openssl