ABSTRACT

IMPLEMENTATION OF DOUBLE ENCRYPTION AND OPENSSL LIBRARY IN AES-256 AND RSA-BASED DATABASE SECURITY SYSTEM

By

Dimas Gumerang Ryandika

19102004

Data security is a very important aspect. Information security and confidentiality are important parts of information. The leak of BSI bank customer data by the LockBit hacker group in May 2023 explains how valuable data is and the importance of data security aspects. Data on the internet itself is stored in a database. A common attack on databases is SQL Injection. For this reason, a system is needed that can secure the contents of the stored database. One method that can be used is cryptography where the contents of the database will be scrambled in such a way according to certain mathematical algorithms used so that the contents of the database become random and difficult to read. This research uses two-stage encryption using AES-256 and RSA on a system built with PHP-based website objects and stored on web hosting and the use of MySQL as a database type with encryption implementation using the OpenSSL library and SQL Injection attacks as a testing model. The results show that AES-256 and RSA two-stage encryption can be implemented on the "credit" and "phone" columns as shown by the test results where the "credit" and "phone" columns are encrypted and read as ciphertext when tested using SQL Injection attacks on the website.

Keywords: ***encryption, database, AES, RSA, OpenSSL***