# ABSTRAK

# IMPLEMENTASI *DOUBLE ENCRYPTION* DAN *OPENSSL LIBRARY* PADA SISTEM KEAMANAN BASIS DATA BERBASIS ENKRIPSI AES-256 DAN RSA

Oleh

Dimas Gumerang Ryandika

19102004

Keamanan data merupakan aspek yang sangat penting. Keamanan dan kerahasiaan informasi sendiri adalah bagian penting dari informasi. Bocornya data nasabah bank BSI oleh kelompok *hacker* LockBit pada Mei 2023 lalu menjelaskan betapa berharganya data dan pentingnya aspek keamanan data. Data pada internet sendiri tersimpan pada *database*. Serangan yang umum terjadi pada *database* adalah *SQL Injection*. Untuk itu, diperlukan sistem yang dapat mengamankan isi dari *database* yang tersimpan. Salah satu metode yang dapat digunakan adalah kriptografi dimana isi dari *database* akan diacak sedemikian rupa sesuai dengan algoritma matematika tertentu yang digunakan agar isi dari database menjadi acak dan sulit dibaca. Penelitian ini menggunakan enkripsi dua tahap menggunakan AES-256 dan RSA pada sistem yang dibangun dengan objek situs web berbasis *PHP Native* dan tersimpan di web hosting serta penggunaan MySQL sebagai tipe *database* dengan implementasi enkripsi menggunakan library OpenSSL dan serangan SQL Injection sebagai model pengujian. Hasil penelitian menunjukkan enkripsi dua tahap AES-256 dan RSA dapat diimplementasikan pada kolom “credit” dan “phone” yang ditunjukkan dengan hasil pengujian dimana kolom “credit” dan “phone” terenkripsi dan terbaca sebagai *ciphertext* ketika dilakukan pengujian menggunakan serangan *SQL Injection* pada situs web.

**Kata kunci : *enkripsi, database, aes, rsa, openssl***