

ABSTRAK

IRWAN SAPUTRA. Implementasi Algoritma *AES-128* Untuk Pencegahan Pemalsuan Sertifikat *ETP* (Studi Kasus : UPA Bahasa UMRAH). Dibimbing oleh MUHAMAD RADZI RATHOMI dan ERWIN BERTA SLAM.

Pemanfaatan Sertifikat *English Test Program* (ETP) dalam bentuk digital di Unit Penunjang Akademik (UPA) Bahasa Universitas Maritim Raja Ali Haji (UMRAH) masih menghadapi permasalahan keamanan karena penggunaan *QR Code* yang dibuat secara manual sehingga rentan terhadap duplikasi dan pemalsuan. Penelitian ini bertujuan mengimplementasikan algoritma *Advanced Encryption Standard* (AES-128) sebagai mekanisme pengamanan data sertifikat melalui integrasi *ciphertext* ke dalam *QR Code* untuk mencegah pemalsuan dokumen.

Penelitian ini menggunakan pendekatan implementasi sistem dengan mengembangkan aplikasi berbasis web menggunakan React, Node.js, MongoDB, dan pustaka CryptoJS. Data sertifikat yang meliputi NIM, nama mahasiswa, serta skor ETP dienkripsi menggunakan AES-128, kemudian hasil enkripsi dalam format Base64 disematkan ke dalam *QR Code* pada sertifikat digital. Pengujian sistem dilakukan menggunakan metode *Black Box Testing*, pengujian *avalanche effect*, serta simulasi berbagai skenario pemalsuan sertifikat. Hasil penelitian menunjukkan bahwa seluruh fungsi sistem berjalan sesuai kebutuhan dengan tingkat keberhasilan *Black Box Testing* sebesar 100%, sedangkan pengujian *avalanche effect* menghasilkan nilai rata-rata 49,87% yang menunjukkan karakteristik keamanan AES-128 telah terpenuhi. Sistem juga berhasil mendeteksi seluruh skenario pemalsuan, termasuk modifikasi dokumen, penggantian maupun pembuatan *QR Code* tiruan, serta pemalsuan total sertifikat. Dengan demikian, implementasi algoritma AES-128 yang diintegrasikan ke dalam *QR Code* terbukti efektif meningkatkan keamanan, menjaga integritas data, serta mendukung proses verifikasi keaslian Sertifikat ETP secara cepat, akurat, dan andal di lingkungan UPA Bahasa UMRAH.

Kata kunci: *AES-128*; Kriptografi; QR Code; Sertifikat ETP; Pemalsuan Dokumen;

ABSTRACT

IRWAN SAPUTRA. *Implementation of AES-128 Algorithm for the Prevention of ETP Certificate Forgery (Case Study: UPA Bahasa UMRAH). Supervised by MUHAMAD RADZI RATHOMI and ERWIN BERTA SLAM.*

The implementation of digital English Test Program (ETP) certificates at the Language Support Unit (UPA Bahasa) of Universitas Maritim Raja Ali Haji (UMRAH) still faces security challenges due to the use of manually generated QR Codes, which are vulnerable to duplication and forgery. This study aims to implement the Advanced Encryption Standard (AES-128) algorithm as a data protection mechanism by embedding encrypted certificate data into QR Codes to prevent certificate forgery.

This research employed a system implementation approach by developing a web-based application using React, Node.js, MongoDB, and the CryptoJS library. Certificate information, including student identification number, student name, and ETP scores, was encrypted using the AES-128 algorithm, and the resulting Base64-encoded ciphertext was embedded into the QR Code displayed on the digital certificate. System evaluation was conducted through Black Box Testing, avalanche effect analysis, and simulations of various certificate forgery scenarios. The results indicate that all system functionalities operated successfully with a 100% success rate in Black Box Testing. Furthermore, the avalanche effect achieved an average value of 49.87%, demonstrating that the AES-128 implementation satisfies the security characteristics of symmetric cryptography. The system also successfully detected all simulated forgery attempts, including document modification, QR Code replacement, counterfeit QR Code generation, and complete certificate forgery. Therefore, the integration of AES-128 encryption with QR Code technology effectively enhances certificate security, preserves data integrity, and provides a reliable, accurate, and efficient certificate verification mechanism for the ETP certification system at UPA Bahasa UMRAH.

Keywords: AES-128; Cryptography; QR Code; ETP Certificate; Document Forgery;