PENERAPAN ALGORITMA HASH DAN ASIMETRIS UNTUK PENGAMANAN DOKUMEN DIGITAL

KATARINA PUTRI PRADITASARI
H1D020078

ABSTRAK

Pemalsuan ijazah masih menjadi permasalahan serius di Indonesia dan kerap dimanfaatkan untuk kepentingan pribadi. Salah satu kasusnya adalah dugaan penggunaan ijazah palsu oleh calon Wali Kota Palopo untuk memenuhi persyaratan pencalonan. Kasus ini menunjukkan lemahnya sistem verifikasi dokumen serta perlunya penguatan regulasi, khususnya terhadap ijazah, baik yang telah diterbitkan maupun yang akan dicetak. Penelitian ini bertujuan merancang sistem pengamanan dokumen digital dengan mengintegrasikan algoritma kriptografi hash dan asimetris. Proses diawali dengan pembacaan data dokumen menggunakan teknologi *Optical Character Recognition* (OCR). Algoritma MD5 digunakan untuk menghasilkan nilai hash sebagai pendeteksi perubahan data, sedangkan Elgamal berperan dalam mengamankan nilai hash tersebut melalui proses *signing*. Hasil proses *signing* kemudian dikonversi menjadi QR-Code yang disisipkan langsung ke dalam dokumen ijazah. Sistem diuji menggunakan tiga data ijazah dengan total 16 skenario pengujian, mencakup perubahan pada isi data, file, dan kombinasi kunci. Hasil pengujian menunjukkan bahwa kombinasi algoritma MD5 dan Elgamal mampu menjaga integritas dokumen secara efektif. QR-Code yang dihasilkan berisi *ciphertext* dan kunci publik, memungkinkan proses verifikasi tetap berjalan meskipun terjadi perubahan pada kombinasi kunci dalam sistem.

Kata kunci: Dokumen digital, Ijazah, Kriptografi, MD5, Elgamal, QR-Code, OCR

IMPLEMENTATION OF HASH AND ASYMMETRIC ALGORITHMS FOR DIGITAL DOCUMENT SECURITY

KATARINA PUTRI PRADITASARI
H1D020078

ABSTRACT

Diploma forgery remains a serious issue in Indonesia and is often exploited for personal purposes. One such case involved allegations of a forged diploma used by a mayoral candidate in Palopo to meet candidacy requirements. This case highlights the weaknesses in current document verification systems and the urgent need to strengthen regulations, particularly concerning diplomas, both previously issued and newly printed ones. This study aims to design a digital document security system by integrating hash and asymmetric cryptographic algorithms. The process begins with reading document data using Optical Character Recognition (OCR) technology. The MD5 algorithm is employed to generate a hash value that serves as an indicator of data alteration, while the Elgamal algorithm is used to secure the hash value through a digital signing process. The resulting signature is then converted into a QR code and embedded directly into the diploma document. The system was tested using three diploma samples across 16 testing scenarios involving changes to document content, file integrity, and key combinations. The results demonstrate that the combination of MD5 and Elgamal algorithms effectively preserves document integrity. The generated QR code contains both ciphertext and a public key, allowing the verification process to proceed even if there are changes to the key combinations within the system.

Keywords: *Digital document, Diploma, Cryptography, MD5, Elgamal, QR-Code, OCR*