ABSTRAK

PUTRI SUCI RENITA**.** Optimalisasi Algoritma *ECDSA* pada *QR-Code* Sertifikat Digital Menggunakan *Hash BLAKE2B* dan *SHA*-128. Dibimbing oleh FERDI CHAHYADI dan NOVRIZAL FATTAH FAHMITRA.

Sertifikat digital yang diterbitkan secara daring rentan terhadap pemalsuan dan manipulasi data, sementara instansi pemerintah daerah seperti Dinas Pendidikan, Kepemudaan dan Olahraga Kabupaten Lingga belum menerapkan tanda tangan digital dalam proses administrasinya. Penelitian ini bertujuan merancang dan mengimplementasikan sistem tanda tangan digital berbasis algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) pada sertifikat digital yang dilengkapi QR-Code, sekaligus mengoptimalkan sistem dengan mengombinasikan fungsi hash BLAKE2b dan SHA-128 serta membandingkan kinerjanya. Metode yang digunakan mencakup perancangan arsitektur sistem tanda tangan digital, implementasi empat skema algoritma (ECDSA tanpa hash, ECDSA+SHA-128, ECDSA+BLAKE2b, dan ECDSA+BLAKE2b&SHA-128), serta pengujian terhadap 2.000 data menggunakan parameter *Avalanche Effect*, waktu eksekusi, nilai efisiensi, dan reliabilitas. Hasil penelitian menunjukkan bahwa kombinasi ECDSA+BLAKE2b+SHA-128 menghasilkan performa terbaik dengan nilai *Avalanche Effect* sebesar 54,30% (melampaui ambang ideal 50%), waktu eksekusi 0,1178 ms yang lebih efisien dibanding BLAKE2b tunggal (0,2105 ms), nilai efisiensi 0,174 pts, serta reliabilitas 100%. Sistem *E-Sign* yang dibangun mencakup empat antarmuka fungsional yang seluruh fungsinya berhasil terverifikasi melalui pengujian *blackbox*. Kombinasi BLAKE2b dan SHA-128 terbukti mencapai keseimbangan optimal antara keamanan kriptografi dan efisiensi komputasi dalam penerbitan sertifikat digital.

Kata kunci: autentikasi, BLAKE2B, ECDSA, QR-Code, sertifikat digital.

ABSTRACT

PUTRI SUCI RENITA. Optimization of the *ECDSA* Algorithm on *QR-Code* Digital Certificates Using *BLAKE2B* and *SHA*-128 *Hash*. Supervised by FERDI CHAHYADI and NOVRIZAL FATTAH FAHMITRA.

Digital certificates issued online are vulnerable to forgery and data manipulation, while local government agencies such as the Education, Youth and Sports Office of Lingga Regency have not yet implemented digital signatures in their administrative processes. This study aims to design and implement a digital signature system based on the *Elliptic Curve Digital Signature Algorithm* (ECDSA) on *QR-Code*-integrated digital certificates, while optimizing the system by combining BLAKE2b and SHA-128 hash functions and comparing their performance. The methods employed include designing the digital signature system architecture, implementing four algorithm schemes (ECDSA without hash, ECDSA+SHA-128, ECDSA+BLAKE2b, and ECDSA+BLAKE2b+SHA-128), and testing against 2,000 data samples using the parameters of *Avalanche Effect*, execution time, efficiency value, and reliability. The results show that the ECDSA+BLAKE2b+SHA-128 combination yields the best performance, with an *Avalanche Effect* of 54.30% (exceeding the ideal threshold of 50%), an execution time of 0.1178 ms which is more efficient than standalone BLAKE2b (0.2105 ms), an efficiency value of 0.174 pts, and 100% reliability. The developed *E-Sign* system comprises four functional interfaces, all of which were successfully verified through *blackbox* testing. The combination of BLAKE2b and SHA-128 is proven to achieve an optimal balance between cryptographic security and computational efficiency in digital certificate issuance.

Keywords: authentication, *BLAKE2B*, *ECDSA*, digital certificate, *QR-Code*.