

## ABSTRAK

Di era digital, kriptografi menjadi solusi utama untuk melindungi informasi sensitif dari ancaman pembobolan data. Algoritma *Elliptic Curve Cryptography* (ECC) dalam kriptografi memberikan tingkat keamanan yang tinggi dengan ukuran kunci yang relatif lebih kecil, ECC diintegrasikan dengan *Diffie – Hellman* (DH) membentuk ECDH. Namun, pengelolaan kunci yang efisien menjadi tantangan utama dalam implementasi ECC. Oleh karena itu, penelitian ini difokuskan pada analisis latensi sistem yang melibatkan kedua algoritma tersebut dengan menggunakan dua struktur data yang berbeda, yaitu *HashMap* dan *ArrayList*. Penelitian ini mengukur latensi sistem berdasarkan berbagai skenario jumlah data *dummy* yang disimpan di *KeyServer* untuk menilai dampak penggunaan struktur data terhadap kinerja sistem. Hasil pengujian menunjukkan bahwa *HashMap* lebih efisien dan stabil dalam menangani jumlah data besar, dengan latensi yang relatif lebih rendah dibandingkan *ArrayList* yang mengalami peningkatan latensi signifikan seiring bertambahnya jumlah data. Hal ini mengindikasikan bahwa struktur data yang digunakan memiliki pengaruh besar terhadap efisiensi dan performa sistem kriptografi.

**Kata Kunci:** Kriptografi, *Elliptic Curve Cryptography* (ECC), *Diffie-Hellman* (DH), manajemen kunci, latensi, *HashMap*, *ArrayList*, keamanan komunikasi.

## ABSTRACT

*In the digital era, cryptography has become a primary solution for protecting sensitive information from data breach threats. The Elliptic Curve Cryptography (ECC) algorithm in cryptography provides high security with relatively smaller key sizes. ECC is integrated with Diffie – Hellman (DH), forming ECDH. However, efficient key management remains a major challenge in implementing ECC.*

*This study focuses on analyzing system latency involving both algorithms using two different data structures: HashMap and ArrayList. The system latency was measured based on various scenarios of dummy data stored in KeyServer to evaluate the impact of data structure selection on system performance. The results show that HashMap is more efficient and stable in handling large amounts of data, with relatively lower latency compared to ArrayList, which experiences significant latency increases as the data size grows. This indicates that the choice of data structure greatly affects the efficiency and performance of cryptographic systems.*

**Keywords:** *Elliptic Curve Cryptography (ECC), Diffie-Hellman (DH), key management, latency, HashMap, ArrayList, communication security, data structure, cryptographic systems.*

