

ABSTRAK

Perkembangan teknologi informasi mendorong kebutuhan terhadap metode pengamanan data yang tidak hanya aman, tetapi juga efisien dari sisi performa. Penelitian ini bertujuan untuk menganalisis perbandingan waktu komputasi dan *throughput* algoritma kriptografi AES dan RSA dalam proses enkripsi data berdasarkan variasi ukuran kunci. Penelitian menggunakan pendekatan eksperimen komparatif dengan menerapkan AES-GCM dan RSA-OAEP pada enam dataset yang terdiri atas file CSV dan file gambar. Ukuran kunci yang digunakan pada AES-GCM adalah 128 bit, 192 bit, dan 256 bit, sedangkan RSA-OAEP menggunakan ukuran kunci 1024 bit, 2048 bit, dan 3072 bit. Setiap kombinasi algoritma, ukuran kunci, dan dataset diuji sebanyak lima kali. Parameter yang dianalisis meliputi waktu komputasi, *throughput*, dan jumlah *chunk*. Hasil penelitian menunjukkan bahwa AES-GCM memiliki rata-rata waktu komputasi sebesar 0,2168 ms dan rata-rata *throughput* sebesar 811,8232 MB/s. Sementara itu, RSA-OAEP memiliki rata-rata waktu komputasi sebesar 35,7400 ms dan rata-rata *throughput* sebesar 4,4142 MB/s. Pada RSA-OAEP, jumlah *chunk* memengaruhi waktu komputasi karena file perlu dibagi menjadi beberapa bagian sebelum dienkripsi. Berdasarkan hasil tersebut, AES-GCM lebih efisien untuk proses enkripsi data berukuran besar, sedangkan RSA-OAEP kurang efisien apabila digunakan untuk mengenkripsi file besar secara langsung.

Kata kunci: Kriptografi, AES, RSA, waktu komputasi, *throughput*.

ABSTRACT

The development of information technology increases the need for data security methods that are not only secure but also efficient in terms of performance. This study aims to analyze the comparison of computation time and throughput of AES and RSA cryptographic algorithms in the data encryption process based on key size variations. This research uses a comparative experimental approach by applying AES-GCM and RSA-OAEP to six datasets consisting of CSV files and image files. The key sizes used in AES-GCM are 128 bits, 192 bits, and 256 bits, while RSA-OAEP uses 1024-bit, 2048-bit, and 3072-bit keys. Each combination of algorithm, key size, and dataset was tested five times. The parameters analyzed include computation time, throughput, and the number of chunks. The results show that AES-GCM obtained an average computation time of 0.2168 ms and an average throughput of 811.8232 MB/s. Meanwhile, RSA-OAEP obtained an average computation time of 35.7400 ms and an average throughput of 4.4142 MB/s. In RSA-OAEP, the number of chunks affects computation time because files must be divided into several parts before encryption. Based on these results, AES-GCM is more efficient for encrypting large data, while RSA-OAEP is less efficient when used to encrypt large files directly.

Keywords: Cryptography, AES, RSA, computation time, throughput.