ABSTRACT

Advanced Encryption Standard-128 (AES-128) is a widely used cryptographic algorithm for protecting electronic data in network communication systems, data storage, document encryption, cloud-based applications, and modern information systems. Improving encryption speed is a fundamental requirement in modern cryptography to ensure system responsiveness and efficient data processing. However, the MixColumns function in AES-128 has a high computational cost due to multiplication operations in the Galois Field. This study proposes a modification of AES-128 by replacing MixColumns with a dynamic key-dependent bit permutation based on a logistic chaotic map and reducing the number of rounds from 10 to 6, with the aim of improving encryption speed while maintaining ciphertext diffusion quality. The permutation table is generated through a combination of SHA-256, a logistic chaotic map with parameter r=3.99, and the Fisher-Yates shuffle using the encryption key as the seed, so that each key produces a unique permutation pattern. Testing was conducted on text files ranging from 10 KB to 1 MB and compared against standard AES-128, AES with static bit permutation, AES with static bit permutation and reduced rounds, and AES with Dynamic MixColumns based on a chaotic map. The results show that the proposed algorithm is capable of performing encryption approximately 10 times faster than standard AES-128 on a 1 MB file (3,100.528 ms vs. 31,049.094 ms), achieving an encryption Throughput of 330.266 KB/s, an Avalanche effect of 50.30% exceeding the Strict Avalanche Criterion (SAC 50%), an average Shannon entropy of 7.9939 equivalent to standard AES-128, and a Key sensitivity of 50.16%, which is the highest among all comparison algorithms. Statistical evaluations, including Frequency, Runs, and Chi-Square tests, also passed successfully. These results demonstrate that the proposed modification successfully improves encryption speed while maintaining the quality of ciphertext diffusion.

Keywords: *AES-128, bit permutation, reduced round, logistic chaotic map, speed, quality of ciphertext diffusion.*

ABSTRAK

AES-128 digunakan secara luas dalam sistem komunikasi jaringan, penyimpanan data, enkripsi dokumen, aplikasi berbasis cloud, dan sistem informasi modern. Peningkatan kecepatan enkripsi merupakan kebutuhan fundamental dalam kriptografi modern untuk menjaga responsivitas sistem dan efisiensi pemrosesan data. Namun fungsi *MixColumns* pada AES-128 memiliki beban komputasi tinggi akibat operasi perkalian dalam Galois Field. Penelitian ini mengusulkan modifikasi AES-128 dengan menggantikan *MixColumns* menggunakan dynamic *key-dependent bit permutation* berbasis *logistic chaotic map* serta mengurangi jumlah *round* dari 10 menjadi 6, dengan tujuan meningkatkan kecepatan enkripsi tanpa mengurangi kualitas difusi *ciphertext*. Tabel permutasi dibangkitkan melalui kombinasi SHA-256, *logistic chaotic map* dengan parameter r=3,99, dan *Fisher-Yates shuffle* menggunakan kunci enkripsi sebagai seed, sehingga setiap kunci menghasilkan pola permutasi yang unik. Pengujian dilakukan pada file teks berukuran 10 KB hingga 1 MB dan dibandingkan terhadap AES-128 standar, AES dengan *bit permutation* statis, AES dengan *bit permutation* statis dan *reduced round*, serta AES dengan *Dynamic MixColumns* berbasis *chaotic map*. Hasil menunjukkan algoritma yang diusulkan mampu melakukan enkripsi sekitar 10 kali lebih cepat dibandingkan AES-128 standar pada file 1 MB (3.100,528 ms berbanding 31.049,094 ms) dengan *Throughput* enkripsi mencapai 330,266 KB/s, *Avalanche effect* 50,30% melampaui *Strict Avalanche Criterion* (SAC 50%), rata-rata entropi Shannon 7,9939 yang setara dengan AES-128 standar, serta *Key sensitivity* 50,16% yang merupakan nilai tertinggi di antara seluruh algoritma pembanding. Pengujian statistik tambahan (*Frequency test*, *Runs test*, dan *Chi-Square test*) juga dinyatakan lulus. Hasil ini menunjukan bahwa modifikasi yang diusulkan berhasil meningkatkan kecepatan enkripsi tanpa mengurangi kualitas difusi *ciphertext*.

Kata kunci: AES-128, *bit permutation, reduced round, logistic chaotic map, kecepatan, kualitas difusi ciphertext*