Modifikasi Algoritma Advanced Encryption Standard (AES) Pada Proses SubBytes dan Mixcolumn Untuk Meningkatkan Performa dan Keamanan Pada Algoritma AES = Modification of Advanced Encryption Standard (AES) Algorithm on SubBytes and Mixcolumn Process to Improve Performance and Security in the AES Algorithm

Novita Angraini, author

Abstrak

Advanced Encryption Standard (AES) adalah suatu standar algoritma block cipher yang digunakan sebagai penerapan dari kriptografi. Perkembangan serangan pada algoritma AES mendorong banyaknya penelitian terkait modifikasi pada algoritma AES dengan tujuan untuk meningkatkan keamanan pada algoritma tersebut serta untuk menghasilkan alternatif dari algoritma enkripsi yang dapat digunakan untuk mengamankan data. Pada penelitian ini, telah dilakukan modifikasi terhadap algoritma AES dengan mengganti S-box menggunakan perfect SAC S-box pada proses SubBytes dan menggunakan matriks MDS involutary yang merupakan matriks M0 Clefia pada proses Mixcolumn. Perfect SAC S-box memiliki nilai rata-rata SAC yang tepat 0,5. Berdasarkan hasil pengujian didapatkan bahwa perfect SAC S-box memiliki hasil uji SAC yang lebih baik dengan nilai error terkecil sebesar 0,0469. Selanjutnya modifikasi AES dilakukan dengan menggunakan perfect SAC S-box dan matriks M0 Clefia. Hasil uji strict avalanche criterion (SAC) menggunakan variabel bebas kunci pada algoritma modifikasi AES round kedua memiliki nilai yang lebih baik dengan nilai error rata-rata sebesar 0,0002. Hasil uji avalanche weight distribution (AWD) menggunakan variabel bebas kunci dan plaintext pada algoritma modifikasi AES round kedua memiliki nilai yang lebih baik dengan nilai distorsi rata-rata sebesar 0,0371 dan 0,1529. Waktu kecepatan dekripsi pada modifikasi AES dengan 1.000.000 sampel memiliki waktu yang lebih cepat, yaitu 4,1690 seconds. Berdasarkan hasil uji yang dilakukan, algoritma modifikasi AES memiliki ketahanan keamanan dan performa yang lebih baik dibandingkan dengan algoritma AES asli.

.....Advanced Encryption Standard (AES) is a standard block cipher algorithm used as an implementation of cryptography. The development of attacks on the AES algorithm has encouraged a lot of research related to modifications to the AES algorithm with the aim of increasing the security of the algorithm and to produce alternatives to encryption algorithms that can be used to secure data. In this study, modifications have been made to AES by replacing the S-box using the perfect SAC S-box in the SubBytes process and using the involutary MDS matrix which is the M0 Clefia matrix in the Mixcolumn process. The Perfect SAC S-box has an exact SAC average value of 0.5. Results Based on the test, it was found that the perfect SAC S-box has a better SAC test result with the smallest error value of 0.0469. Furthermore, AES modification is carried out using the perfect SAC S-box and the M0 Clefia matrix. The results of the strict avalanche criteria (SAC) test using the key-independent variables in the second round of modified AES algorithm have an average error value of 0.0002. The results of the avalanche weight distribution (AWD) test using the key-independent variables and plaintext in the second round of modified AES algorithm have an average distortion value of 0.0371 and 0.1529. Decryption speed time on AES modification with 1,000,000 samples has a faster time, which is 4.1690 seconds. results Based on the tests, the modified AES algorithm has better performance and security resistance than the original AES algorithm