V. KESIMPULAN

5.1. Kesimpulan

Berdasarkan analisis yang sudah dilakukan pada penelitian ini, dapat disimpulkan bahwa:

Implementasi modifikasi *SubBytes* pada metode AES menunjukkan keamanan yang lebih baik dibandingkan dengan metode AES sebelum dimodifikasi pada uji Performa, uji *Cryptanalysis*, dan uji *Randomness*.

5.2. Saran

Beberapa saran yang dapat diperhatikan untuk pengembangan penelitian dan sistem di masa mendatang adalah sebagai berikut:

1. Perlu dipertimbangkan untuk meningkatkan panjang kunci dari 256-bit menjadi lebih panjang. Dengan meningkatkan panjang kunci, jumlah kombinasi yang diperlukan untuk mendekripsi *ciphertext* akan bertambah, sehingga meningkatkan tingkat keamanan sistem secara keseluruhan.
2. Saat ini pengujian kinerja algoritma AES yang dimodifikasi dilakukan melalui simulasi perangkat lunak, dengan memperhitungkan waktu enkripsi dan dekripsi yang tergantung pada kecepatan memori laptop atau komputer yang digunakan. Namun, hasil pengujian seringkali dapat dipengaruhi oleh faktor-faktor lain, seperti jumlah aplikasi yang berjalan pada perangkat tersebut. Oleh karena itu, disarankan untuk melakukan analisis kompleksitas algoritma yang tidak bergantung pada kecepatan *hardware*.