BAB 5
KESIMPULAN

5.1. Kesimpulan

Setelah melakukan pembahasan secara teoritis, implementasi algoritma, dan analisis hasil dari percobaan yang dilakukan penelitian ini berhasil menerapkan kombinasi algoritma AES dan Diffie-Hellman untuk mengamankan citra MRI dengan beberapa kesimpulan sebagai berikut :

a. Algoritma AES dapat digunakan dalam metode pengamanan citra digital medis. Hasil dari enkripsi menggunakan algortima AES menghasilkan file citra baru yang tidak dapat dibaca sebelum di dekripsi kembali sehingga *file* citra tersebut berhasil diamankan menggunakan algoritma ini.
b. Algoritma Diffie-Hellman dapat meningkatkan keamanan pada kunci AES. Hal ini dikarenakan kunci yang digunakan untuk proses enkripsi dan dekripsi AES tidak perlu ditukarkan di dalam jalur publik, sehingga tingkat kerentanan kebocoran kunci dapat diminimalisir. Algoritma Diffie-Hellman akan menjadi jembatan dalam proses pertukaran kunci. Kunci AES yang bersifat simetris akan dihasilkan dari proses pembangkitan dari dua buah kunci asimetris yang tidak perlu ditukarkan di dalam jalur publik.
c. Algoritma AES dapat digunakan untuk melakukan dekripsi citra MRI. Hasil dari citra yang di dekripsi sama dengan citra awal, hal ini diperkuat dengan nilai histogram citra dan perbandingan nilai *checksum* antara citra awal dan citra hasil dekripsi yang tidak mengalami perbedaan.
d. Proses enkripsi citra menggunakan kombinasi algoritma AES dan Diffie – Helllman lebih cepat dibandingkan dengan proses dekripsi citra tersebut.

e. Pada saat di enkripsi, file citra mengalami penambahan ukuran. Namun setelah mengalami proses dekripsi, ukuran file citra tersebut kembali seperti ukuran awal.
f. Nilai dari kunci yang digunakan pada enkripsi AES tidak berpengaruh terhadap perubahan ukuran dari citra hasil enkripsi. Nilai kunci tersebut berpengaruh pada isi dari *file* citra hasil enkripsi, hal ini dapat dilihat dari nilai *checksum* yang berbeda – beda dari hasil enkripsi dengan dua nilai kunci yang berbeda.

5.2. Saran

Berikut ini beberapa saran yang diberikan untuk pengembangan penelitian lebih lanjut mengenai enkripsi dan dekripsi pada pengamanan citra MRI menggunakan kombinasi algoritma AES dan Diffie-Hellman agar menjadi lebih baik dan aman, antara lain :

a. Mencari variabel lain yang bersifat temporer yang digunakan pada proses pembangkitan kunci dengan algoritma Diffie-Hellman.
b. Melakukan pengamanan pada database dimana proses penyimpanan data untuk proses pembangkitan dan pertukaran kunci terjadi.
c. Menerapkan algoritma lain seperti MD5 sebagai tambahan untuk menyembunyikan data – data yang diperlukan dalam pembangkitan kunci AES.
d. Melakukan analisis kombinasi AES dengan algoritma kriptografi lain untuk membandingkan tingkat efisiensi pada proses enkripsi dan dekripsi.