ABSTRAK

Pada era teknologi informasi dan komunikasi sekarang, umumnya pertukaran informasi digital terjadi melalui jaringan publik seperti *E-mail*, *SMS* dan aplikasi *messenger* lainnya. Hal ini mengakibatkan rawan terjadinya pencurian informasi oleh pihak yang tidak bertanggung jawab. Sehingga diperlukan suatu mekanisme keamanan yang memberikan jaminan terhadap keamanan informasi yang terdapat pada pesan. Pada tugas akhir ini telah dibangun suatu aplikasi yang berguna untuk meningkatkan keamanan informasi yang terkandung dalam pesan berupa teks pada komunikasi melalui *smartphone* Android. Hal ini dapat dilakukan dengan adanya proses enkripsi-dekripsi yang dijalankan pada *smartphone* Android.

Pada tugas akhir ini menggunakan dua algoritma yakni algoritma Rijndael atau AES *(Andvanced Encryption Standard)* dan AES yang telah termodifikasi. Penggunaan algoritma AES yang telah termodifikasi ini dimaksudkan untuk mengetahui kapabilitas performansi dari algortima tersebut. Apakah lebih baik dari algoritma AES itu sendiri, mengingat algoritma AES telah digunakan lebih dari sepuluh tahun.

Hasil yang diperoleh dari pengujian yang dilakukan pada tugas akhir ini performansi dari sistem yang menggunakan algoritma AES hampir sama dengan performansi dari sistem yang menggunakan algoritma AES termodifikasi. Kedua sistem memiliki nilai *avalanche effect* yang hampir sama yakni berkisar 0.5 dan durasi waktu yang dibutuhkan untuk melakukan *brute force attack* yakni 2.6×10^{21} tahun. Namun berbeda waktu komputasi dan performansi *robustness* pada kedua sistem. Waktu komputasi pada sistem yang menggunakan algoritma AES lebih cepat dibandingkan sistem yang menggunakan algoritma AES termodifikasi. Sedangkan pada *robustness test*, performansi sistem yang menggunakan algoritma AES termodifikasi lebih baik dibandingkan sistem yang menggunakan algoritma AES.

Kata kunci: Android, enkripsi, dekripsi, AES.