

BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilaksanakan dengan hasil yang diperoleh, maka diambil kesimpulan sebagai berikut:

1. Penerapan kunci simetris *Advanced Encryption Standard* (AES) dan algoritma kunci asimetris Rivest Shamir Adleman (RSA) dalam aplikasi berbasis Android untuk mengamankan dokumen telah berhasil dibuat.
2. Kombinasi dari algoritma AES dan algoritma RSA untuk mengamankan dokumen dilakukan dengan tiga tahapan, yaitu bangkitkan kunci publik dan kunci rahasia, kemudian enkripsi dokumen lalu enkripsi kata sandi (kunci simetris).
3. Waktu yang dibutuhkan proses dekripsi bergantung dari ukuran dokumen yang digunakan. Sedangkan proses enkripsi cukup dinamis jika ukuran dokumen masih di bawah 1 MB.
4. Kombinasi antara algoritma AES dan algoritma RSA untuk mengamankan dokumen memiliki tingkat keamanan yang lebih terjamin karena ada dua tahapan enkripsi yang dilakukan. Waktu proses enkripsi lebih cepat dibanding algoritma RSA, tetapi tidak jauh lebih cepat dari algoritma AES. Dengan hasil rata-rata AES selama 141,4 *milliseconds*, Kombinasi algoritma selama 152,6 *milliseconds* dan RSA selama 164,5 *milliseconds*.

5.2 Saran

Saran pengembangan atau penelitian selanjutnya bisa dilakukan sebagai berikut:

1. Untuk kedepannya diharapkan dapat ditambahkan fitur *online integrated* pada algoritma AES yang bisa meng-otomatis enkripsi dan dekripsi tanpa perlu bertukar kunci simetris.
2. Penambahan fitur untuk mereset atau membangkitkan ulang kunci publik dan kunci rahasia.
3. Menambahkan kombinasi algoritma, selain AES dan RSA.