

## BAB 5. KESIMPULAN DAN SARAN

### 5.1. Kesimpulan

Penelitian ini telah berhasil dirancang dan diuji untuk membuat sistem pengaman file menggunakan enkripsi AES 256 dan RC4 untuk menghindari kebocoran data. Hasil simulasi dan pengujian yang diperoleh menunjukkan bahwa dokumen yang sudah di enkripsi tidak bisa dibuka dengan menggunakan aplikasi lain selain menggunakan sistem yang sudah dibangun. Hal ini bisa dilihat hasil yang sudah susun pada tabel 4.6 dan tabel 4.7, hasil tersebut juga didukung dengan metrik kualitatif tingkat keamanan penggunaan enkripsi.

Maka metode pengaman file dengan menggunakan algoritma enkripsi AES 256 untuk mengenkripsi isi dokumen dan algoritma enkripsi RC4 untuk mengenkripsi kunci cukup efektif untuk meningkatkan keamanan file dokumen berklasifikasi. Hal ini didukung dengan proses enkapsulasi data kunci yang sudah dienkripsi secara langsung ke dalam dokumen hasil enkripsi, sehingga pemilik dokumen tidak perlu mencatat atau mengingat kunci yang digunakan pada saat dekripsi. Pengaman dokumen dengan menggunakan metode yang di uji juga semakin meningkat dikarenakan kunci yang digunakan adalah kunci yang di bangkitkan oleh sistem, sehingga tidak bisa ditangkap oleh aplikasi keylogger. Dengan memanfaatkan teknologi enkripsi AES 256 dan RC4 secara bersamaan serta menggunakan *key generator* untuk membangkitkan kunci yang digunakan untuk enkripsi dan membungkus (*encapsulate*) semua data menjadi 1 data baru yang tidak mudah untuk dibaca dan dipecahkan menggunakan aplikasi lain, selain menggunakan sistem yang dirancang.

Dengan semakin maraknya kasus kebocoran dokumen yang terjadi terlebih dengan adanya kasus kebocoran data baru-baru ini di mana data-data dari lembaga pemerintahan seperti Kementerian Pertahanan mengalami kebocoran, diharapkan dengan adanya metode pengaman dokumen dengan menggunakan enkripsi seperti yang ditawarkan dalam penelitian ini, akan meminimalisasi penggunaan dokumen-dokumen tersebut meski mengalami kebocoran dokumen.

Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa sistem enkripsi file yang dikembangkan adalah sistem yang aman, andal, dan memiliki performa yang cukup baik. Sistem ini dapat digunakan untuk melindungi dokumen berklasifikasi pada infrastruktur informasi vital nasional.

## 5.2. Saran

Untuk meningkatkan keamanan, disarankan untuk meningkatkan keamanan akses pada sistem yang dikembangkan dengan cara sebagai berikut:

- a) Implementasikan kontrol akses untuk membantu membatasi akses ke sistem dan data.
- b) Lakukan pencadangan (*backup*) secara berkala untuk membantu memulihkan data jika terjadi serangan keamanan.
- c) Gunakan firewall dan antivirus untuk membantu melindungi sistem dari serangan malware.
- d) Lakukan audit keamanan secara berkala untuk membantu mendeteksi dan memperbaiki kelemahan keamanan pada sistem. dengan menggunakan kunci enkripsi yang panjang dan kompleks. Selain itu, disarankan untuk menyimpan kunci enkripsi di lokasi yang aman dan tidak diketahui oleh orang lain.

Untuk saran penelitian berikutnya dapat mencoba menggunakan kombinasi algoritma enkripsi yang lebih baik atau dengan melakukan pengacakan terhadap hasil enkripsi. Sehingga file enkripsi yang dihasilkan semakin sulit untuk dipecahkan, sehingga keamanan dokumen yang di enkripsi semakin meningkat.