BAB V
PENUTUP

5.1 Kesimpulan

Aplikasi pengamanan data ini berhasil mengimplementasikan metode Rivest Shamir Adleman dalam mengamankan file atau text perusahaan. Hal ini dibuktikan melalui hasil pengujian pada tabel 4.1 yang memperlihatkan bahwa semua file dan teks yg dienkripsi dapat berubah menjadi file berekstensi *(.encrypted)* yang tidak dapat dibuka tanpa kunci privat, serta dapat dikembalikan ke file aslinya dalam proses dekripsi dan tidak mengalami perubahan, dengan tingkat keberhasilan 100%.

Aplikasi web dengan kombinasi algoritma kriptografi AES dan RSA pada PT.XYZ memiliki waktu enkripsi dan dekripsi yang relatif cepat, dengan rata-rata waktu kurang dari 1 detik. Waktu enkripsi dan dekripsi yang efisien menunjukkan kinerja yang baik dari implementasi kriptografi dalam melindungi data dan informasi pada aplikasi ini.

Meskipun beberapa jenis file mengalami peningkatan ukuran setelah dienkripsi, hal ini terjadi terutama pada jenis file tertentu seperti PNG. Oleh karena itu, perlu diperhatikan bahwa penggunaan kriptografi pada jenis file tertentu harus dipertimbangkan dengan cermat untuk meminimalkan dampak peningkatan ukuran yang tidak diinginkan. Secara keseluruhan, penggunaan kriptografi dalam aplikasi ini berhasil mencapai tujuan pengamanan data pada PT.XYZ dengan efisien. Waktu enkripsi dan dekripsi yang cepat, serta peningkatan ukuran file yang relatif kecil pada sebagian besar jenis file, membuat aplikasi ini menjadi solusi yang efektif dalam melindungi dokumen prosedur dan metode kalibrasi dari akses yang tidak sah. Namun, perlu diperhatikan bahwa pemilihan algoritma kriptografi yang tepat untuk setiap jenis file harus dilakukan dengan hati-hati untuk mengoptimalkan kinerja dan efisiensi aplikasi.

5.2 Saran

Aplikasi pengamanan data ini hanya dapat melakukan proses *login* dengan memasukkan *password*, maka dari itu, untuk proses *login*, diharapkan dapat dikembangkan dengan menambahkan database sehingga *file* hasil enkripsi dan

dekripsi dapat tersimpan dalam satu akun pengguna dan tentunya file akan lebih aman dan terorganisir.

Salah satu penerapannya adalah, dengan membuat sistem yang membuat user dapat mengirim kunci tersebut kepada user lainnya, sehingga kunci publik dapat ditampilkan secara langsung untuk user yang berhak menerima kunci tersebut. Sehingga kunci tidak perlu ditransmisikan oleh user tersebut secara manual, sehingga dapat lebih efisien dan memudahkan user.

Selain itu, pada aplikasi ini dapat pula dilakukan klasifikasi antara user yang hanya dapat membangkitkan kunci, atau user yang hanya dapat melakukan enkripsi dan dekripsi, atau hanya salah satu dari proses tersebut. Sehingga, terdapat seorang admin pula yang dapat mengakses semua dan mengatur user yang berhak untuk melakukan proses-proses dari pembangkitan kunci, enkripsi dan dekripsi ini. Jadi dibuatnya beberapa jenis user ini dapat mencipatakan kenyamanan dan keamanan yang lebih optimal.