BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Informasi adalah asset berharga yang harus dilindungi dari ancaman kebocoran data. Selain Informasi terstruktur yang disimpan dan di kelola pada suatu database juga terdapat file-file rahasia yang perlu dilindungi kerahasiannya. Salah satu cara untuk melindungi database dan file rahasia adalah dengan penerapan teknik hybrid kriptografi. Metode hybrid kriptografi kinerjanya cukup bagus dan dapat diandalkan untuk mengenkripsi dan mendekripsi informasi rahasia. Penyelenggara sistem elektronik terutama yang berkaitan dengan infrastruktur informasi vital sudah seharusnya menerapkan kriptografi pada layanan sistem elektroniknya. PPATK sebagai salah satu penyelenggara sistem elektronik yang bertugas mencegah dan memberantas tindak pidana pencucian uang memiliki asset berharga berupa database dan file-file informasi intelijen keuangan yang bersifat rahasia. dari penelitian ini dapat diambil beberapa kesimpulan diantaranya adalah:

1. Metode Hybrid Kriptografi yaitu perpaduan antara kriptografi kunci simetrik dan kriptografi kunci asimetrik dapat memperkuat upaya pertahanan siber dari ancaman keboran data pada infrastruktur informasi vital sektor administrasi Pemerintah yang bertugas untuk mencegah dan memberantas tindak pidana pencucian uang dan pendanaan terorisme salah satunya pada aplikasi statistik penanganan TPPU dan TPPT.
2. Penerapan algoritma AES 256 dilanjutkan dengan mengenkripsi kunci menggunakan algoritma RSA dapat digunakan untuk melindungi informasi rahasia berupa file dan database sistem aplikasi statistik TPPU dan TPPT. Penerapan tersebut menjadi upaya peningkatan pertahanan siber yang dapat diandalkan dengan kecepatan rata-rata proses enkripsi file 521.088,2201 KB

/ Second dan proses mendekripsi file kecepatannya rata-rata 96.040,33614 KB / Second. / Second dan ringan prosesnya dijalankan pada laptop dengan spesifikasi prosesor Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz 2.30 GHz dan memori 32,0 GB.

3. Penerapan Hybrid kriptografi AES 256 dan RSA dapat berfungsi 100 % dengan baik pada sistem aplikasi statistik penanganan TPPU dan TPPT yang telah di uji coba menggunakan metode *black box testing*.
4. Pihak Internal Penyelenggara Sistem Elektronik maupun ekternal akan sulit membocorkan data yang terdapat pada Aplikasi Statistik Penanganan TPPU dan TPPT. Karena sudah diterapkan perimeter pada bagian database dan file rahasia dengan mengenkripsi data dan kuncinya.
5. Penerapan metode hybrid kriptografi AES 256 dan RSA dapat memberikan perlindungan lebih kuat karena selain mengenkripsi data atau file juga mengenkripsi kuncinya. Sehingga penulis mengusulkan penambahan fitur upload file agar dapat menyajikan data statistik penanganan TPPU dan TPPT yang valid dan akuntabel dengan tetap menjaga keamaan file dan database pada aplikasi.

5.2 Saran

1. Algoritma AES sudah bisa pecahkan melalui pendekatan *quantum computing*, oleh karena itu perlu dilakukan upaya untuk meningkatkan keamanan algoritma AES atau mengkombinasikan RSA dengan algoritma lain.
2. selain dengan menggunakan metode hybrid kriptografi perlu juga dilakukan penelitian enkripsi bertingkat baik dengan metode enkripsi sejenis maupun secara hybrid.

3. untuk tingkat kerahasiaan yang lebih tinggi perlu diteliti pada bagian protokol jaringan komunikasi data dan juga pada bagian hardware.
4. untuk mengelola file dan database tingkat kerahasiaan yang sangat tinggi perlu diteliti pada aspek teknologi secara konprehensif meliputi *hardware*, *software*, *person* dan transmisi.
5. Penelitian ini berfokus tentang teknik kriprografi pada file berupa dokumen dan database, karena keterbatasan waktu. Pada kesempatan berikutnya perlu diteliti mengenai aspek *crypt analyst*, steganografi dan manajemen kunci.