BAB V

SIMPULAN DAN SARAN

5.1 SIMPULAN

Dari hasil penelitian mengenai analisis penerapan kriptografi sebagai solusi kemanan informasi pada Sistem Perencanaan dan Akuntabilitas Kinerja Lembaga Sandi Negara, penulis dapat mengambil beberapa kesimpulan sebagai berikut:

a) SIPAK merupakan salah satu implementasi e-government yang diterapkan oleh Lembaga Sandi Negara dalam menunjang kemudahan dalam hal perencanaan, anggaran dan kinerja unit kerjanya. Dalam SIPAK terdapat beberapa aset yang dinilai perlu untuk diamankan sebagai identifikasi perlunya keamanan informasi diterapkan pada SIPAK. Aset-aset tersebut diantaranya yang berhubungan dengan informasi adalah database kinerja pogram, database anggaran dan database kegiatan. Selain itu aset yang berhubungan dengan perangkat keras adalah komputer, server, storage, router, telepon, printer. Untuk aset yang berhubungan dengan perangkat lunak adalah Open Source Software, Aplikasi Sipak dan E-mail. Sedangkan aset yang behubungan dengan infrastruktur adalah jaringan WAN/LAN, wireless dan internet. Kemudian aset yang berhubungan dengan layanan adalah portal informasi. Dalam penelitian ini aset yang teridentifikasi berkaitan dengan kriptografi adalah aset database kinerja program, aset database anggaran, aset database kegiatan, aset aplikasi SIPAK dan aset jaringan.

b) Berdasarkan analisis risiko yang dilakukan untuk mengetahui tingkat risiko dari aspek kerahasiaan, integritas, dan ketersediaan terhadap aset pada SIPAK, didapatkan ancaman yang bernilai *high, medium* dan *low* terhadap sistem. Untuk aspek kerahasiaan, ancaman dengan tingkat risiko yang paling tinggi adalah tindakan mengakses informasi melalui *network sniffing* oleh pihak yang tidak berhak dengan level resiko *high* dan yang paling

rendah adalah tindakan *brute force login dan dictionary attack* dengan tingkat resiko medium. Untuk aspek integritas, ancaman dengan tingkat risiko yang paling tinggi adalah modifikasi database oleh pihak tak berhak dengan tingkat resiko *high* dan yang terendah adalah modifikasi lalu lintas jaringan yang dilakukan pihak yang tidak behak yang berasal dari luar organisasi dengan tingkat resiko *low*. Selanjutnya untuk aspek ketersediaan, ancaman dengan tingkat risiko yang paling tinggi adalah *hacking, attacking, intruder* dengan tingkat resiko *high* dan yang terendah adalah penghapusan atau pengrusakan data pada databse oleh pihak yang tak berhak dengan tingkat resiko *high.*

c) Penanganan terhadap risiko yang timbul dalam SIPAK Lemsaneg dapat dijamin salah satunya dengan menggunakan kriptografi. Penggunaan kriptografi untuk keamanan database dapat menggunakan enkripsi menggunakan algoritma simetris yaitu AES-128. Untuk keamanan *password* saat ditransmisikan dan disimpan dapat dijamin dengan menggunakan algoritma hash yaitu SHA-256. Untuk keamanan data saat transmisi melalui jaringan dapat menggunakan SSL/TLS minimal versi 3.0 dan 1.0 atau versi yang lebih tinggi karena telah mendukung algoritma kriptografi, yaitu *public key cryptography*, algoritma simetrik, dan fungsi hash yang lebih aman dari versi sebelumnya

d) Spesifikasi komputer minimal yang dapat menjalankan AES-128, SHA-256 dan SSL/TLS 3.0 minimal adalah dengan menggunakan hardware yang menunjang pentium II. Namun saat ini Lemsaneg sudah menggunakan spesifikasi komputer yaitu *Processor Intel ®Core2Duo™* CPU 3.0 GHz (2MB, 800MHz FSB, Intel 3200 Chipset), RAM DDR2 1 GB dan HDD 640GB. Sehingga dapat disimpulkan bahwa spesifikasi komputer yang dimiliki Lemsaneg sekarang telah memenuhi standar minimal dari kebutuhan.

5.2 SARAN

Melihat hasil penelitian dan kesimpulan yang telah disampaikan penulis. Maka penulis merekomendasikan hal-hal sebagai berikut:

a) Untuk menjamin keamanan layanan *e-government* tidak hanya dapat dicapai dengan menggunakan kriptografi, namun perlu di dukung dengan jenis pengamanan lain, misal : pengamanan fisik, pengamanan personel, serta kesadaran keamanan informasi di lingkungan pemerintah, khususnya di Lembaga Sandi Negara.

b) Pengunaan rekomendasi algoritma kriptografi bersifat fleksibel, artinya seiring dengan perkembangan waktu dan kebutuhan keamanan, penggunaan algoritma kriptografi dapat disesuaikan dengan menggunakan kunci yang lebih panjang maupun algoritma baru yang lebih kuat. Hal ini juga didukung dengan makin berkembangnya teknologi informasi sehingga teknik dalam pemecahan kode pun semakin tinggi dan tidak ada jaminan bahwa algoritma yang sekarang dinilai kuat akan selamanya tidak terpecahkan.

c) Perlu dibuat standar pengamanan informasi dengan memanfaatkan kriptografi dalam pemerintah, sehingga layanan *e-government* dapat lebih terjamin keamanannya.