ABSTRAK

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dari suatu data. Salah satu cara untuk menjaga keamanan dan kerahasiaan data tersebut adalah dengan menggunakan teknik penyandian yang disebut dengan kriptografi. Kriptografi sering diimplementasikan pada data teks. Oleh karena itu, pada Tugas Akhir ini yang dibahas yaitu tentang kriptografi pada *file* teks.

Sistem kriptografi pada Tugas Akhir ini adalah kriptosistem hibrida (*hybrid cryptosystem*) yang merupakan penggabungan kriptografi simetrik dengan kriptografi asimetrik. Kriptografi simetrik menggunakan algoritma DES (dengan menggunakan empat mode operasi *cipher* blok yaitu ECB, CBC, CFB dan OFB), sedangkan kriptografi asimetrik menggunakan algoritma RSA. Alasan pemilihan kriptosistem hibrida adalah untuk memproses data dengan cepat menggunakan algoritma simetrik dan mempermudah *key management* menggunakan algoritma asimetrik.

Dari data hasil pengujian diperoleh rata-rata waktu enkripsi per karakter dari kunci DES dengan menggunakan kunci RSA 512 bit dan 1024 bit sebesar 1.937 ms dan 5.537 ms. Sementara itu, rata-rata waktu enkripsi per karakter dari data teks dengan menggunakan mode ECB sebesar 0.041525 ms, sedangkan dengan mode CBC/CFB/OFB sebesar 0.044419 ms. Dari pengukuran tersebut disimpulkan bahwa semakin panjang kunci RSA maka waktu pembangkitan kunci RSA dan waktu proses enkripsi/dekripsi kunci DES akan semakin lama, dan kapasitas memori yang dipakai pun semakin besar. Sementara itu, *processing time* dan *memory usage* pada mode operasi diperoleh nilai: ECB<CBC≈CFB≈OFB. Sementara itu, dari hasil pengujian ketahanan sistem dengan menggunakan metode *avalanche effect* didapatkan hasil yang paling bagus yaitu pada mode operasi CBC. Berdasarkan hasil pengujian sistem secara *black box test* dan *beta test* maka dapat disimpulkan bahwa sistem sudah berjalan sesuai dengan kaidah algoritma yang digunakan yaitu DES dan RSA dengan contoh proses untuk mengamankan *file* data teks.

Kata kunci: kriptosistem hibrida, kriptografi, enkripsi, dekripsi, mode operasi *cipher* blok, RSA, ECB, CBC, CFB, OFB, simetrik, asimetrik.