ABSTRAK

Sistem yang ada pada *black box* pesawat saat ini hanya sebatas sebagai media penyimpan segala bentuk aktivitas penerbangan. *Black box* pesawat belum memiliki kemampuan untuk mengirimkan informasi ke tempat lain serta jika ada proses pengiriman informasi, *black box* pesawat belum memiliki sistem keamanan. Keamanan data merupakan bagian yang sangat penting pada saat melakukan proses pertukaran informasi. Informasi yang dipertukarkan hanya boleh diketahui dan dimiliki oleh pengirim dan penerima yang telah ditentukan. Proses pertukaran tidak boleh melibatkan *man-in-the-middle attacker* atau pihak yang tidak dikenali oleh pengirim atau penerima. Oleh karena itu untuk menjaga keamanan, kerahasian dan autentikasi data perlu adanya implementasi kriptografi, yang merupakan ilmu dan seni untuk menjaga keamanan pesan.

Algoritma *stream cipher* yang digunakan adalah *Dragon* yang termasuk ke dalam kategori *synchronous* stream cipher dalam proses enkripsi dan dekripsi. Dragon merupakan algoritma kandidat *eStream Project*, yang dapat diimplementasikan pada *software* dan *hardware*.

Pada penelitian Tugas Akhir ini, dirancang suatu sistem pengamanan data suara pada *cockpit voice recorder,* dengan cara dienkripsi. Lalu memberikan hak akses secara aman untuk didekripsi oleh orang yang memiliki hak akses data tersebut. Hasil akhir yang didapat dari penelitian ini akan di uji performansi terkait waktu proses enkripsi dan dekripsi, *avalanche effect*, dan *keutuhan data*. Sehingga didapatkan satu algoritma yang memiliki sistem keamanan yang layak untuk *cockpit voice recorder*.

Keyword : Stream Cipher, dragon, cockpit voice recorder