ABSTRAK

Flight Data Recorder (FDR) merupakan bagian dari *black box* yang mengumpulkan dan merekam data dari sensor pesawat, seperti, ketinggian, kecepatan arah, data mesin dan parameter lainnya. Data *black box* di analisis agar mengetahui penyebab kecelakaan pesawat, sehingga dapat menghindari dari kecelakaan serupa dimasa mendatang.

Penelitian ini bertujuan untuk merancang suatu sistem pengamanan data pada *Flight Data Recorder* hingga kondisi siap dikirim pada sistem yang ada di darat saat penerbangan berlangsung. Dilakukannya pengamanan data agar menghindari akses pengubahan dan pencurian data yang dilakukan oleh pihak yang tidak berwenang atau *man in the middle* saat proses transmisi berlangsung. Metode pengamanan yang digunakan adalah kriptografi.

Algoritma kriptografi yang akan diimplementasikan adalah algoritma *stream cipher Variably Modified Permutation Composition* (VMPC). Penelitian ini melakukan analisis algoritma stream cipher dalam hal waktu proses enkripsi dan dekripsi, *avalanche effect* dan keutuhan data. Berdasarkan penelitian tersebut *VMPC* memiliki nilai *avalanche effect* sebesar 44,19% untuk 100-part dan 44,11% untuk 250-part.

Keyword: stream cipher, Variably Modified Permutation Composition, Flight Data Recorder.