BAB I
PENDAHULUAN

1.1 Latar Belakang

Black box pesawat terdiri atas *flight data recorder*(FDR) ; berfungsi menyimpan data ketinggian, kecepatan, putaran mesin, tekanan kabin, temperature udara diluar radar, auto pilot dan lain-lain, sedangkan *cockpit voice recorder*(CVR) ; berfungsi menyimpan data percakapan di dalam ruang cockpit baik percakapan pilot dengan co pilot, atau dengan *air traffic controller*(ATC), pramugari dengan penumpang, serta suara mesin atau hujan.Sebelum seluruh data tersebut dikirim serta di simpan di *memory boards*, data tersebut terlebih dahulu di simpan sementara didalam *flight data acquisition*(FDAU) yang terletak di hidung pesawat[1].

Kemampuan black box pesawat yang terbatas dalam proses pengiriman informasi menjadi merepotkan jika terjadi kecelakaan pesawat terbang dan blackbox sulit ditemukan, karena semua fakta menyebabkan terjadinya kecelakaan ada di blackbox. Maskapai penerbangan Incident Malaysia 370 (MH70), Phoenix International Holdings, Inc menghabiskan 70 hari dengan menyelam lebih dari 5000 meter ke laut untuk menyelidiki kecelakaan tersebut[5].

Oleh karena itu ketika terjadi kecelakan pesawat terbang bagian yang paling utama dicari adalah *black box,* agar mendapatkan informasi keadaan pesawat dan penyebab kecelakaan. Maka dari itu diperlukan kemampuan mengirim data yang aman dari pihak tidak bertanggung jawab, salah satunya dengan metoda kriptografi. Kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Kriptografi terdiri atas tiga fungsi yaitu enkripsi, dekripsi dan kunci[2].

Algoritma yang akan diimplementasikan dalam sistem ini adalah Dragon, yang tergolong kepada kelompok stream cipher.Algoritma *stream cipher* adalah

algoritma kriptografi beroperasi pada plainteks/cipherteks dalam bentuk bit tunggal, yang dalam hal ini rangkaian bit dienkripsikan/didekripsikan bit per bit[2].

1.2 Rumusan Masalah

Masalah yang akan dibahas pada Tugas Akhir ini adalah sebagai berikut:

a. Blackbox pesawat saat ini yang belum di lengkapi dengan sistem keamanan data.
b. Enkripsi dan dekripsi dengan algoritma stream cipher untuk mengamankan cockpit voice recorder.
c. Performansi algoritma stream cipher untuk mengamankan sebuah rekaman suara dari cockpit voice recorder.

1.3 Tujuan

Dengan merujuk pada rumusan masalah diatas, maka tujuan yang dibahas yaitu :

a. Merancang dan membuat sistem yang dapat mengenkripsi dan mendekripsi data suara pada *cockpit voice recorder*.
b. Menerapkan algoritma *stream cipher Dragon* pada proses enkripsi dekripsi suara rekaman *cockpit voice recorder*.
c. Menganalisis hasil implementasi berdasarkan pengukuran parameter waktu proses enkripsi dan dekripsi, *avalanche effect*, dan keutuhan data.

1.4 Batasan Masalah

Tugas Akhir ini mempunyai batasan masalah yaitu :

a. Data suara rekaman *cockpit voice recorder* yang akan dienkripsi adalah suara dari rekaman *live* ATC.
b. Format data rekaman suara *cockpit voice recorder* yang akan di proses adalah wav.
c. Menerapkan algoritma *stream cipher*, Dragon.
d. Sistem ini tidak melakukan kompresi data.

e. Data *cockpit voice recorder* diproses hingga kondisi siap untuk dikirim, tanpa adanya proses pengiriman data.

1.5 Metologi Penelitian

Langkah yang ditempuh untuk menyelesaikan tugas akhir ini adalah:

a. Studi literature, mengumpulkan bahan referensi dari buku, jurnal, ebook dll yang berhubungan dengan tugas akhir ini.
b. Merancang diagram alir untuk implementasi sistem.
c. Melakukan pengujian untuk proses enkripsi dan deskripsi data rekaman suara *cockpit voice recorder* yang ditanamkan Algoritma Dragon.
d. Menganalisa hasil pengujian dan penarikan kesimpulan.
e. Penyusunan buku Tugas Akhir.

1.6 Sistematika penulisan

Tugas akhir ini dibagi dalam beberapa topik bahasan yang disusun secara sistematis dan terdiri dari:

BAB I. PENDAHULUAN

Bab ini berisi tentang latar belakang, rumusan masalah, tujuan masalah, batasan masalah, hipotesis dan sistematika penulisan.

BAB II. DASAR TEORI

Bab ini berisi tentang teori-teori dasar tentang *cockpit voice recorder*, kriptografi, algoritma kriptografi Dragon dari berbagai sumber terkait seperti buku, jurnal, artikel, dan lain sebagainya.

BAB III. PERANCANGAN SISTEM

Bab ini berisi tentang pemodelan dan perancangan sistem keamanan *cockpit voice recorder* serta penjelasan tiap-tiap prosesnya.

BAB IV. IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi tentang implementasi dari perancangan sistem dan pengujian berdasarkan parameter yang telah ditetapkan serta menganalisis hasil pengujian tersebut.

BAB V. KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dari penelitian yang telah dilakukan dan saran untuk penelitian selanjutnya.