

ABSTRAK

Terdapat berbagai jenis multimedia yang dikembangkan seperti *musik*. Untuk menjaga hasil rekaman yang didapat dari kegiatan yang bersifat rahasia diperlukan sistem pengamanan *file musik* hasil rekaman tersebut. Salah satu cara untuk mengamankan data adalah dengan merubah data tersebut dalam bentuk data yang lain yang tidak dapat dimengerti oleh pihak lain, yaitu dengan cara penyandian. Dalam kriptografi terdapat beberapa algoritma yang dapat menyandikan data. Salah satu algoritma kriptografi yaitu AES dan Railfence. Algoritma kriptografi bernama Rijndael yang didesain oleh Vincent Rijmen dan John Daemen asal Belgia keluar sebagai pemenang kontes algoritma kriptografi pengganti DES yang diadakan oleh NIST (*National Institutes of Standards and Technology*) milik pemerintah Amerika Serikat pada 26 November 2001. Algoritma Rijndael inilah yang kemudian dikenal dengan *Advanced Encryption Standard* (AES). Algoritma Railfence adalah salah satu bentuk *cipher* transposisi yang sederhana yang diinspirasi dari model *Polybius square*. *Polybius square* adalah menyusun huruf sebagai matriks 5x5 dan mengkodekan huruf A sebagai 1-1, huruf B sebagai 1-2 dan seterusnya. Setiap karakter pada *Polybius square* diganti dengan indeks *cell* matriks tanpa menggunakan kunci khusus dan hanya merubah posisi sehingga teks tidak terbaca.

Kata kunci : Musik, AES, Rail Fence