

ABSTRAK

Data dapat menjadi salah satu aset penting dalam kelangsungan hidup perusahaan mana pun. Salah satu cara untuk mengamankannya dari kejahatan orang lain adalah mengenkripsinya. Algoritma kriptogenik yang digunakan pada Advanced Encryption Standard (AES) adalah algoritma *Rijndael*. AES menggunakan blok cipher simetris untuk proses enkripsi dan dekripsi yang dapat memproses data input 128 bit dengan menggunakan chipper key 128, 192 atau 256 bit.

Pada algoritma *Rijndael*, data input atau plaintext diproses melalui serangkaian transformasi, disebut Chipper, dan menggunakan kunci kriptogenik rahasia yaitu Chipper Key. Data yang dihasilkan chipper disebut Ciphertext dan akan diproses untuk dikonversikan kembali menjadi plaintext melalui serangkaian transformasi disebut Inverse Chipper.

Maksud dibuatnya tugas akhir ini adalah membuat perangkat lunak enkripsi dan dekripsi data menggunakan metode kriptografi AES dengan bahasa pemrograman visual basic 6.0, serta mengetahui kekuatan algoritma *Rijndael* terhadap serangan brute force.

Kata kunci : *enkripsi, dekripsi, data, metode kriptografi, aes*