

## ABSTRAK

# **APLIKASI PENGAMANAN *FILE* MENGGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) 128 BERBASIS WEB PADA TOKO KHAYANGAN OUTDOOR**

Oleh : Yayat (1511500199)

Khayangan Outdoor yang bergerak di bidang penjualan alat pendakian memiliki pendapatan yang cukup besar. Pendapatan mereka selalu dibukukan dan kemudian diketik ulang ke dalam komputer. File tersebut rentan dicuri dan rusak karena belum ada pengaman khusus. Sebuah data akan sangat berguna apabila digunakan dengan sebagaimana mestinya. Penyimpanan data sangat mudah untuk di sadap dan di susupi oleh orang yang tidak bertanggung jawab. Pencurian data dapat dilakukan dengan cara memindahkan langsung dari penyimpanan komputer ataupun melalui internet. Untuk itu diperlukan suatu aplikasi yang dapat menjaga kerahasiaan sebuah informasi. Salah satu cara yang dapat digunakan adalah kriptografi. Kriptografi adalah sebuah seni penyandian pesan. Aspek keamanan kriptografi adalah kerahasiaan, integritas, otentikasi dan penyangkalan. Kriptografi memiliki banyak teknik dalam mengenkripsi data, diantaranya adalah *Advances Encryption Standard* (AES). *Advances Encryption Standard* merupakan algoritma yang dapat mengamankan data. Keunggulan *Advances Encryption Standard* yaitu kebal terhadap serangan konvensional (*linear* dan *diferensial attack*) yang menggunakan statistik untuk memecahkan sandi. Dengan menggunakan aplikasi ini pengguna dapat menyimpan data dengan aman tanpa takut diketahui oleh pihak-pihak yang tidak berhak mendapatkan informasi tersebut.

Kata kunci : kriptografi, *Advances Encryption Standard*, XVII+74 halaman; 89 Gambar; 8 Tabel; 2 Lampiran