

ABSTRAK

IMPLEMENTASI KRIPTOGRAFI BERBASIS WEB DENGAN ALGORITMA AES 256 DAN KOMPRESI HUFFMAN UNTUK PENGAMANAN FILE DI SMK SATRIA

Oleh : NIZAMUDDIN AULIA KAFA (1511500579)

Keamanan dan kerahasiaan suatu data di zaman sekarang ini terutama bagi suatu instansi atau organisasi tertentu merupakan hal yang sangat penting. Ada data yang bersifat rahasia, artinya data yang bersifat rahasia akan sangat dijaga dan diperhatikan karena itu sangat penting menjaga kerahasiaan data tersebut. Menjaga keamanan data yang bersifat rahasia diperlukan suatu system yang digunakan untuk menyandikan data yang berupa *file* dan membukanya diperlukan kunci rahasia yang sifatnya sulit untuk dideteksi orang yang tidak berhak membukanya. Keamanan data pada Tata Usaha di SMK SATRIA yang bergerak dalam bidang pengolahan data yang berfungsi untuk mengatur pelaksanaan administrasi program dan anggaran sekolah, terutama pada data guru, siswa keuangan dan nilai yang penting untuk mendukung pembelajaran sekolah. Agar tidak terjadi manipulasi data maka diperlukan sebuah aplikasi kriptografi yang dapat mengamankan data dari terjadinya manipulasi data. Dalam penelitian ini membahas konsep yang dapat digunakan untuk menjaga keamanan data yaitu ilmu kriptografi. Metode kriptografi yang akan digunakan dalam penelitian tugas akhir ini adalah AES 256 sebagai algoritma kriptografinya dan metode kompresi *Huffman* sebagai mekanisme kompresi. Sehingga keamanan data akan lebih terhindar dari manipulasi data oleh pihak yang tidak berwenang dan data *file* tidak terlalu besar setelah dijalankan proses. Dokumen yang diuji adalah dokumen bertipe .doc, .docx, .xls, .xlsx, dan .pdf. Dari hasil implementasi dan pengujian didapat kesimpulan bahwa algoritma kriptografi AES 256 dan kompresi *Huffman* dapat diimplementasikan dalam menjaga kerahasiaan dan keamanan data.

Kata Kunci : Kriptografi, Kompresi, Algoritma, AES 256, *Huffman*

xiii + 68 halaman; 64 gambar; 11 algoritme; 8 table; 2 lampiran