ABSTRAK

PENGAMANAN FILE MENGGUNAKAN KRIPTOGRAFI DENGAN METODE AES-128 BERBASIS WEB DI KOMITE NASIONAL KESELAMATAN TRANSPORTASI

Oleh : Dian Widyawan (1511502963)

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya. Data adalah catatan atas kumpulan fakta atau suatu *variable* yang bentuknya dapat berupa angka, kata-kata atau citra. Namun, terkadang data yang bersifat *private* sering terjadinya kebocoran dan kehilangan data. Penggunaan komputer menjadi suatu kebutuhan yang tidak dapat dipisahkan lagi untuk disetiap kegiatan, tidak terkecuali dalam Komite Nasional Keselamatan Transportasi bekerja dibidang investigasi. Demi kelancaran dalam melakukan investigasi untuk itu dibutuhkan suatu aplikasi yang dapat menjaga kerahasiaan data tersebut. Penelitian ini bertujuan untuk menghasilkan aplikasi untuk membantu dalam proses pengamanan data. Aplikasi ini dibangun berbasis *web* dan menggunakan php sebagai bahasa pemrogramannya dan menggunakan metode *Advanced Encryption Standard* (AES) 128 bit. Metode *Advanced Encryption Standard* (AES) merupakan standar enkripsi dengan kunci-simetris dengan ukuran kunci yang bervariasi yaitu 128 bit, 192 bit, dan 256 bit. Dari hasil implementasi diperoleh kesimpulan bahwa aplikasi mampu mengamankan *file* investigasi dari yang semula berbentuk *plaintext* menjadi *chipertext* dengan hasil akhir *file* yang tidak dapat dimengerti lagi maknanya.

Kata kunci : *Kriptografi, Advanced Encryption Standard, File*

xiii+59 halaman; 67 gambar; 25 tabel; 2 lampiran