

ANALISIS PEBANDINGAN METODE ENKRIPSI KOMBINASI AES-TURBO CODE TERHADAP TIGA VARIASI KUNCI AES

Rendra Bayu Adi S.
(12.04.1.1.1.00038)

Pembimbing 1 : Dwi Kuswanto, S.Pd., M.T.
Pembimbing 2 : Yoga Dwitya Pramudita, S.Kom., M.Cs.

ABSTRAK

Komunikasi data merupakan suatu proses pengiriman suatu informasi dari dua titik atau lebih dengan menggunakan suatu kode biner. Di dalam komunikasi data terkadang tidaklah berjalan dengan lancar, adapun kendala dalam proses pengiriman suatu informasi diantara nya adalah pencurian data hingga rusaknya data Informasi terkena suatu *noise* yang ada di dalam proses tersebut. Oleh karena itu diperlukanlah suatu penerapan yang dapat memberikan keamanan informasi dan sekaligus terhindar dari rusaknya data akibat *noise*. Salah satu penerapan tersebut ialah dengan mengkombinasikan teknik kriptografi AES dengan dengan teknik *forward error correction* berupa Turbo code. Penelitian ini bertujuan untuk mengkombinasikan dua teknik tersebut dan menerapkan pada data teks serta menganalisa berdasarkan panjang kunci enkripsi yang dimiliki AES. Hasil analisa menunjukkan bahwa dengan algoritma kombinasi kriptografi AES-turbo dapat bekerja optimal dengan presentase data kembali 100% yaitu pada SNR 15 dB. Dalam pengujian *avalanche effect* juga menunjukkan bahwa panjang kunci 256-bit lebih aman, hal ini dibuktikan dengan uji coba Avalanche Effect sebesar 24,77362 %. Namun dalam pengujian waktu eksekusi data, semakin panjang kunci semakin lama waktu yang dibutuhkan untuk enkripsi dan dekripsi. Dengan demikian untuk pemilihan 3 variasi kunci AES yang lebih efisiensi dan efektifitas yaitu dengan menggunakan kunci 128-bit.

Kata Kunci : AES, Turbo code, AES-Turbo.



[HALAMAN INI SENGAJA DIKOSONGKAN]