

ABSTRAK

Kriptografi adalah ilmu yang mempelajari teknik–teknik matematika yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integrasi data, serta autentikasi data. Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan tersebut, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain.

Algoritma Noekeon merupakan algoritma yang menggunakan skema block-cipher. Noekeon menggunakan pemakaian kunci yang sama pada setiap roundnya. Pada tugas akhir ini akan dibahas proses penggunaan penjadwalan kunci sehingga terjadi pemakaian kunci yang berbeda pada setiap roundnya.

Dari percobaan yang dilakukan menghasilkan bahwa modifikasi algoritma yang dilakukan tidak lebih baik dari algoritma Noekeon itu sendiri. Hal ini dibuktikan dari hasil perhitungan kecepatan waktu, nilai *avalanche effect*, dan probabilitas karakteristik *differential attack* menunjukkan hasil modifikasi algoritma Noekeon dibawah nilai metode algoritma Noekeon itu sendiri.

Kata kunci : Kriptografi, Algoritma Noekeon, Block-cipher.