ABSTRAK

ANALISIS PERBANDINGAN ALGORITMA RIJNDAEL DAN ALGORITMA TWOFISH PADA PROSES PENGIRIMAN DATA TEKS MENGGUNAKAN JARINGAN LAN (LOCAL AREA NETWORK)

Oleh

Ridhky Oktavian Pradana

10107364

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Di mana kebenaran dan keaslian suatu informasi sangat penting baik pada saat pengiriman ataupun pada saat informasi tersebut diterima. Pesan, data, atau informasi tidak akan berguna lagi apabila pada saat pengiriman informasi tersebut disadap atau dibajak oleh orang yang tidak berhak atau berkepentingan.

Dengan bertitik tolak pada masalah tersebut maka akan dicoba untuk membandingkan dua algoritma kriptografi yaitu algoritma *Rijndael* dan algoritma *Twofish*. Di mana kedua algoritma tersebut termasuk dalam kategori kunci *chipper blok* yang banyak digunakan pada saat ini. Kedua algoritma ini beroperasi pada blok bit dan kedua algoritma ini banyak digunakan karena merupakan algoritma kunci simetri yang kuat terhadap serangan (*attack*). Maka dari itu akan dilakukan perbandingan terhadap kedua algoritma tersebut pada jaringan *Local Area Network (LAN)* di beberapa komputer untuk mengetahui algoritma mana yang paling cepat dalam proses pengamanan data teks melalui jaringan *Local Area Network (LAN)*.

Dari hasil pengujian yang telah dilakukan, dari segi proses waktu enkripsi dan dekripsi untuk algoritma *Rijndael* selalu memakan waktu yang cukup lama daripada algoritma *Twofish*. Karena algoritma *Rijndael* memiliki cara penjadwalan kunci dan pembangkitan *S-Box* yang cukup rumit dibandingkan dengan algoritma *Twofish*. Maka dari itu dari kedua algoritma tersebut yang paling bagus dan tahan lama dari serangan kriptanalis adalah dengan memakai algoritma *Rijndael*.

Kata Kunci : Algoritma, *Rijndael, Twofish,* Pengiriman Data