PERANCANGAN PROGRAM ENKRIPSI FILE MENGGUNAKAN TEKNIK KRIPTOGRAFI SIMETRIS

Abstrak

Perkembangan teknologi informasi sangat cepat, sehingga informasi dapat lebih mudah dan murah untuk disebarkan atau diperoleh. Komunikasi semakin mudah dengan adanya *internet* yang sangat populer menghubungkan manusia di seluruh dunia. Tetapi dengan semakin mudah dan terbukanya hubungan maka kerahasiaan dan keamanan menjadi semakin berkurang. Perusahaan yang ingin menikmati kemudahan akses harus mempertaruhkan keamanan data-data atau informasi perusahaan yang bersifat rahasia. Teknik kriptografi dikembangkan untuk melindungi data, dan sudah digunakan sejak dahulu dengan mengalami perkembangan teknik yang digunakan. Kriptografi pada dasarnya bertugas untuk menyandikan data (enkripsi). Salah satu teknik kriptografi dinamakan Kriptografi Kunci Simetris atau bisa disingkat Kriptografi Simetris. Teknik tersebut menggunakan hanya satu kunci untuk proses enkripsi dan dekripsi. Pada saat ini kekuatan kriptografi harus terletak pada kerahasiaan kuncinya bukan algoritmanya.

Pada Tugas Akhir ini membahas penggunaan Teknik Kriptografi Simetris untuk proses enkripsi dan dekripsi data. Teknik Kriptografi Simetris yang digunakan adalah Teknik Kriptografi Simetris *Block Cipher* dengan memakai tiga algoritma yaitu : Twofish, Rijndael dan Serpent. *Block Cipher* melakukan enkripsi data dengan panjang tertentu pada sekali prosesnya. Pembahasan meliputi analisis dan penggambaran proses-proses enkripsi dan dekripsi pada ketiga algoritma tersebut.

Ketiga algoritma tersebut diimplementasikan untuk melakukan enkripsi dan dekripsi data *file* menggunakan bahasa pemrograman Visual Basic 6. Perangkat lunak enkripsi file dapat melakukan enkripsi file untuk semua jenis file dengan menggunakan ketiga algoritma tersebut di atas dan menyediakan demo untuk penggunaan enkripsi kata atau huruf dan heksadesimal. Ketiga algoritma tersebut mempunyai kemampuan algoritma yang baik untuk menjaga keamanan data. Tetapi dari sudut efisiensi Twofish mempunyai kemampuan yang lebih baik dan sama pada semua pilihannya, sedangkan pada ragam pilihannya Rijndael lebih bervariasi dengan kemampuan yang lebih baik pada panjang blok 256 bit.

Kata Kunci : Enkripsi, *File*, Teknik Kriptografi Simetris, *Block Cipher*, Twofish, Rijndael, Serpent