ABSTRAK

Internet adalah salah satu hasil dari perkembangan teknologi di bidang komputer yang memungkinkan orang di seluruh dunia saling berhubungan menggunakan komputer. Namun, kemajuan teknologi memiliki sisi buruk yaitu rawannya keamanan data. Salah satu cara untuk melakukan pengamanan data adalah dengan menggunakan teknik kriptografi. Kriptografi adalah ilmu yang berguna untuk mengacak data sedemikian rupa sehingga tidak bisa dibaca oleh pihak ketiga yang tidak memiliki wewenang. Dalam algoritma kriptografi terdapat beberapa metode utama, salah satunya adalah metode kunci simetrik. Standar yang biasa dipakai dalam metode kunci simetrik adalah DES (*Data Encryption Standard*) dan AES (*Advance Encryption Standard*) yang sekarang menggantikan standar DES. Salah satu algoritma yang termasuk dalam AES adalah algoritma Twofish.

Dalam tugas akhir ini, sistem kriptografi dibuat dalam bentuk komponen pengaman data untuk enkripsi dan dekripsi saja, dengan menggunakan algoritma Twofish dan SHA1. Proses enkripsi pada Twofish terdiri dari 3 operasi, yaitu *Input Whitening*, 16 putaran fungsi F, dan *Output Whitening*. Proses dekripsi merupakan kebalikan dari proses enkripsi. Proses pembentukan message digest dengan algoritma SHA1 terdiri dari 2 operasi utama yaitu *Padding* dan 80 putaran proses dasar algoritma SHA1.

Komponen yang akan dibuat, dibagi menjadi dua. Komponen SHA1 digunakan untuk menghasilkan message digest yang digunakan sebagai kata kunci masukkan untuk algoritma Twofish. Komponen Twofish yang dibangun, digunakan untuk melakukan enkripsi dan dekripsi string maupun file teks. Komponen - komponen ini dibangun untuk framework .NET, dan sudah diuji serta diverifikasi dengan menggunakan data yang memiliki ukuran bervariasi. Dari hasil uji coba yang dilakukan, dapat ditarik kesimpulan bahwa komponen yang dibuat dapat melakukan enkripsi dan dekripsi dengan baik untuk dtring text maupun file yang berukuran lebih kecil atau sama dengan 40 mega byte.

Kata kunci: Twofish, SHA1, Kriptografi, Pengaman Data