ABSTRAK

RSA merupakan salah satu algoritma asimetri yang digunakan dalam proses enkripsi dan dekripsi data. RSA pada umumnya sudah memiliki tingkat keamanan yang baik, namun masih memiliki beberapa kekurangan. Beberapa diantaranya adalah panjang kunci yang digunakan dan terpisahnya proses otentikasi terhadap proses enkripsi. Dimana jika menggunakan kunci yang pendek maka akan gampang difaktorkan. Dan terpisahnya proses otentikasi terhadap proses enkripsi mengakibatkan terjadinya kesamaan ciphertext yang diterima dari siapa saja jika pesan yang dienkripsi sama. Untuk mengatasi permasalahan tersebut, dalam Tugas Akhir ini dirancang sebuah sistem pengamanan dan otentikasi pengiriman pesan menggunakan modifikasi algoritma asimetri RSA.

Dalam perancangan Tugas Akhir ini, digunakan penggabungan fungsi modifikasi *n-prime* dalam pembangkitan kunci setiap *user* dan modifikasi penggabungan proses otentikasi dengan proses enkripsi pada sistem enkripsi dan dekripsi. Modifikasi n-prime memberikan user kebebasan memilih jumlah bilangan prima dalam pembangkitan pasangan kunci. Sedangkan modifikasi penggabungan proses otentikasi dengan proses enkripsi merupakan modifikasi dalam sistem enkripsi dan dekripsi. Dimana setiap pesan masukan diubah menjadi blok-blok angka. Panjang blok bergantung pada panjang nilai n pada kunci privat pengirim. Kemudian dilakukan proses otentikasi dengan masukan kunci privat pengirim. Hasil dari proses ini selanjutnya akan disusun menjadi blok-blok angka baru. Panjang blok bergantung pada panjang nilai n pada kunci publik penerima pesan. Hasil dari proses ini selanjutnya dienkripsi menjadi deretan ciphertext.

Sistem yang dirancang pada Tugas Akhir ini hanya dapat menerima masukan berjenis text yang berupa gabungan karakter huruf dan karakter angka. Dengan nilai hasil uji perancangan sistem pada tugas akhir ini dapat menghasilkan nilai *chi-square* lebih kecil dari 3,481, nilai rata-rata hasil *avalanche effect* kurang dari 50% , dan nilai rata-rata waktu kinerja sistem enkripsi yang dirancang 1,84 kali waktu kinerja sistem tanpa modifikasi dan 1,62 kali waktu kinerja sistem enkripsi RSA dengan penyisipan otentikasi Hash.

Kata kunci: kriptografi, enkripsi, otentikasi, modified RSA, n-prime