Abstrak

Penggunaan internet saat ini didominasi oleh aplikasi-aplikasi yang berabasiskan website dan Aplikasi *Mobile*. Untuk menggunakan aplikasi seperti sosial media dan *e-commerce* diperlukannya sebuah akun yang sesuai dengan data pribadi dan telah didaftarkan sebelumnya. Sayangnya, masih ada pihak yang tidak bertanggung jawab yang dapat mencuri data pribadi tersebut, seperti menggunakan teknik *Key Logging,* *Pishing* dan *Social Engineering*. Salah satu cara yang dapat melindungi keamana data pribadi dari pencurian data adalah dengan menerapkan metode *One Time Password*. *One Time Password* merupakan metode otentikasi dimana kode otentikasi yang dikirimkan hanya berlaku satu kali dan hanya berlaku dalam waktu singkat. Kode otentikasi yang dikirimkan merupakan 6 digit angka acak. Kode tersebut dibuat dengan sebuah teknik tertentu, dimana teknik tersebut menggunakan algoritma kriptografi. Salah satu algoritma kriptografi yang memiliki tingkat keaman cukup baik yaitu algoritma RC6. Algoritma RC6 merupakan salah satu finalis yang telah diusulkan kepada NIST untuk menjadi *Advanced Encryption Standard* menggantikan DES yang dirasa sudah tidak aman. Algoritma RC6 yang digunakan adalah algoritma RC6 dengan panjang 128 bit dengan jumlah round sebanyak 12 putaran. Algoritma RC6 ini nantinya akan diuji menggunakan tes *Avalanche effect*. Tes *Avalanche effect* merupaka sebuah pengujian untuk mengetahui seberapa besar perubahan bit pada ciphertext.

Keyword – One Time Password, RC6, Cryptography, *Avalanche effect*