Sistem Kriptografi Stream Cipher Berbasis Fungsi Chaos untuk Keamanan Informasi

Oleh: Sahid1, Atmini Dhoruri2, Dwi Lestari3, Eminugroho RS4 dan M Fauzan5

ABSTRAK

Tujuan penelitian ini adalah menerapkan Fungsi chaos *Logistic Map* dalam meningkatkan keamanan pengiriman informasi. Fungsi chaos memiliki tingkah laku yang sangat kompleks, *irregular* dan *random* di dalam sebuah sistem yang deterministik. Chaos mempunyai sifat yang kacau atau acak, perubahan sedikit saja akan membangkitkan bilangan yang berbeda, hal ini berguna dalam membangkitkan kunci. Fungsi chaos *Logistic Map* akan digunakan untuk membangkitkan kunci. Selanjutnya, digunakan fungsi *sinus* berosilasi tinggi untuk meningkatkan keacakan bilangan. Dalam menentukan pembangkit kunci akan digunakan protokol perjanjian kunci stickel. Selanjutnya pembangkit kunci akan di proses menggunakan fungsi chaos *Logistic Map* dikombinasikan dengan fungsi *sinus* berosilasi tinggi dan akan diperoleh kunci yang akan digunakan untuk enkripsi serta dekripsi. Pada proses enkripsi dilakukan perhitungan dengan rumus mod 256, sedangkan proses dekripsi dilakukan perhitungan dengan rumus mod 256, dengan adalah Ciphertext, adalah Plaintext, serta adalah Kunci. Dengan menggunakan *Logistic Map* dan fungsi *sinus* pada pembangkit kunci diperoleh sifat chaos yang tinggi untuk nilai parameter tertentu, bersifat chaos hanya pada beberapa iterasi awal, selanjutnya error berkaitan dengan nilai . Untuk nilai-nilai parameter yang lain diperoleh barisan kunci yang konvergen setelah beberapa iterasi.

Kata Kunci: *Kriptografi, Fungsi Chaos, Logistic Map, fungsi sinus, keamanan informasi*