

Abstrak

Layanan internet menjadi salah satu cara untuk mendapatkan berbagai macam informasi karena memudahkan pengguna untuk melakukan berbagai kegiatan. Fasilitas penyimpanan file secara online pada internet mempermudah proses pengaksesan data. File yang disimpan secara online tidak sepenuhnya aman, seharusnya keamanan penyimpanan mutlak diperlukan.

Salah satu algoritma kriptografi *cipher* blok adalah algoritma Rijndael. Rijndael merupakan algoritma kriptografi AES yang beroperasi dalam *byte*, bukan dalam *bit* dan mampu melakukan enkripsi terhadap *plain text* sebesar 16 *byte* atau 128 *bit*. Algoritma ini terdapat kunci internal yang disebut *round key* dimana pembangkitannya diambil dari *cipher key*, sehingga sangat cocok diterapkan dalam enkripsi file yang disimpan secara online. Salah satu cara untuk mengetahui tingkat keamanan suatu algoritma kriptografi dapat dilakukan dengan cara menghitung nilai *avalanche effect* dari file yang telah terenkripsi. Karena algoritma Rijndael beroperasi pada *byte*, maka *avalanche effect* cocok untuk mengetahui tingkat keamanan suatu algoritma kriptografi.

Perbedaan ukuran file yang di-*upload* berbanding lurus dengan waktu yang dibutuhkan untuk mengenkripsi file. Faktor-faktor yang mempengaruhi waktu enkripsi adalah ukuran file, tipe file, batas maksimum memori, maksimum waktu eksekusi. Tipe file yang paling rendah waktu enkripsinya adalah tipe text, sedangkan yang paling tinggi adalah tipe zip. Faktor-faktor yang berpengaruh terhadap hasil *ciphertext* adalah *plaintext* dan key. Perhitungan *avalanche effect* yang dihasilkan tidak sama disebabkan karena pengaruh dari penjadwalan kunci yang dilakukan dalam algoritma Rijndael.

Kata kunci: algoritma rijndael, *avalanche effect*, kriptografi, enkripsi, dekripsi, tipe file.