ABSTRAK

Saat terjadi proses transmisi data, diperlukan beberapa prosedur pengamanan agar keaslian data tetap terjaga dan tidak bocor ke pihak yang tidak memiliki kewenangan maupun kontrol atas data tersebut. Beberapa percobaan untuk mengamankan data pada saat proses transmisi telah dilakukan dalam penelitian sebelumnya, diantaranya menggunakan algoritma DES, ROT, dan RC6.

Penelitian ini menggunakan Algoritma AES, karena dalam penelitian yang dilakukan berfokus mengkaji sistem keamanan yang menjadi faktor penting saat melakukan proses transmisi data. Metode penelitian yang diusulkan pada penelitian ini terdiri dari dua bagian. Bagian metode yang pertama diusulkan yaitu proses enkripsi dan dekripsi yang masing-masing terdiri dari dua bagian. Bagian metode yang kedua diusulkan yaitu proses implementasi pada aplikasi berbasis web dan dilakukan proses pengujian, diantaranya pengujian waktu enkripsi pada beberapa jenis file, pengujian waktu dekripsi pada beberapa jenis file, pengujian hasil enkripsi ditransmisikan pada jaringan, pengujian waktu transmisi file yang sudah dienkripsi, pengujian waktu transmisi file tanpa enkripsi, pengujian serangan dengan metode Man-in-the-Middle, dan mengukur jumlah ketidakteraturan dengan entropi Shannon.

Penelitian ini dilakukan pada lingkungan yang berbeda, yaitu Windows dan Linux, menggunakan bahasa pemrograman yang sama yaitu PHP versi 7.4, Apache versi 2.4 sebagai web server dan OpenSSL versi 1.1.1b. Data uji diunduh dari situs https://file-examples.com/ dan menggunakan jenis berkas dengan ekstensi zip, mp4, png, jpg, mp3, pdf, ppt, docx, csv, xlsx, dan xml serta ukuran yang berbeda.

Keamanan data dalam penelitian ini menunjukan bahwa saat proses transmisi tersebut terjadi peningkatan dari hasil uji awal yang belum dienkripsi, serta pengukuran ketidakteraturannya juga mengalami peningkatan dari pengukuran ketidakteraturan sebelumnya dengan menggunakan entropy shannon.Kata kunci : AES, Keamanan Data, OpenSSL, Transmisi Data.