

ABSTRAK

Smart Card adalah alat yang digunakan untuk transaksi data dengan cepat dan praktis yang berbentuk chip yang ditanamkan pada kartu. Kartu tersebut sangat membantu proses identifikasi dan administrasi seperti kartu pasien pada rumah sakit terutama pada keadaan darurat. Data pasien hanya dapat diakses oleh orang tertentu oleh karena itu dibutuhkan mekanisme keamanan seperti algoritma kriptografi untuk mengamankan data pada kartu tersebut. Algoritma yang dibutuhkan untuk kartu pasien adalah algoritma yang memiliki kemampuan proses yang cepat tingkat keamanan yang tinggi. Pada paper ini telah diimplementasikan algoritma Tiny Encryption Algorithm pada Smart Card dan dihitung waktu proses serta tingkat keamanannya berdasarkan Avalance Effect.

Berdasarkan dari hasil pengujian pada penelitian ini waktu proses enkripsi dan dekripsi data pasien dengan jumlah 600 baris riwayat pasien yang berukuran 30,6 Kb menghasilkan rata-rata waktu enkripsi sebesar 20,17 ms sedangkan dekripsi dibutuhkan waktu sebesar 17,21 ms yang menunjukkan waktu proses yang sangat kecil. Pengujian Avalance Effect yang dilakukan pada proses enkripsi TEA menghasilkan Avalance Effect sebesar 77% yang menunjukkan data yang dienkripsi memiliki hasil ciphertext yang sangat acak sehingga isi data terjaga kerahasiaannya dengan tingkat keamanan yang tinggi. Hasil pengujian waktu proses dan AE tersebut dapat disimpulkan bahwa TEA merupakan algoritma yang memiliki proses mengamankan data yang cepat dengan keamanan yang tinggi dan waktu yang dapat ditoleransi oleh user smart card.

Kata Kunci: Smart Card, TINY ENCRYPTION ALGORITHM, TEA, Kriptografi, Enkripsi, Dekripsi.