ABSTRAK

Model pengamanan berkas adalah suatu model yang mengimplementasikan satu atau lebih algoritma keamanan, dalam hal ini kriptografi, untuk melindungi keabsahan, integritas, dan keamanan berkas. Sudah banyak penelitian yang mengusung model pengamanan berkas guna memenuhi kebutuhan akan perlindungan keamanan. Namun, berdasarkan penelitian sebelumnya, model pengamanan berkas masih dapat dikembangkan. Peneliti mengusung model pengamanan berkas baru menggunakan kriptografi asimetris RSA dan algoritma kompresi PPM. Kriptografi asimetri RSA dipilih dengan alasan kuatnya algoritma dalam mengamankan berkas. Algoritma kompresi PPM dipilih sebagai penyokong kelemahan RSA dengan mengurangi besarnya ukuran *file ciphertext* dikarenakan besarnya bilangan yang digunakan pada saat enkripsi. Penelitian ini bertujuan untuk mengukur performa dari model pengamanan berkas menggunakan kriptografi asimetris RSA dan algoritma kompresi PPM dari segi keamanan, waktu, dan ukuran berkas yang dihasilkan.

Kata kunci: Model pengamanan berkas, Kriptografi, Asimetri, RSA, Algoritma, Kompresi, PPM

ABSTRACT

File security model is a model used to implement one or more security algorithm, in this case cryptography, to ensure file's validity, integrity, dan safeness. There are a lot of study about file security model to secure a file. But, based on previous studies, a file secutiy model is still can be developed. Researcher is proposing a new file secutiy model using asymmetric cryptography RS dan PPM compression algorithm. Asymmetric cryptography RSA is choosen because of its safeness. PPM compression algorithm is used to help decreasing ciphertext file's size due to big numbers usage on encryption process. This study aims to measure the performance of the new file security model using asymmetric cryptography RSA dan PPM compression algorithm in terms of security, time, and file's size.

***Keywords**: File security model, Cryptography, Asymmetric, RSA, Algorithm, Compression, PPM*