ABSTRAK

Pada dasarnya melakukan pengiriman data tanpa melakukan pengamanan pada konten dari data yang dikirim, dapat menyebabkan adanya penyadapan pada jalur pengirimannya. Data penting yang berformat .txt mudah sekali untuk disadap dan data berformat .doc dapat disandikan menggunakan password namun fitur tersebut memiliki kelemahan yaitu adanya aplikasi yang dapat digunakan untuk membobol file yang telah terenkripsi. Untuk itulah peranan teknologi keamanan informasi benar - benar dibutuhkan. Salah satu teknik untuk pengamanan data adalah dengan menggunakan algoritma penyandian data.

Algoritma *One Time Pad* merupakan algoritma sederhana dan *unbreakable* dikarenakan algoritma *One Time Pad* memiliki barisan kunci acak yang ditambahkan ke pesan plaintext yang tidak acak untuk menghasilkan chipertext yang seluruhnya acak. Kunci acak tersebut dibangkitkan menggunakan metode pembangkit bilangan acak antara lain *Mersenne Twister*. *Mersenne Twister* menghasilkan bilangan acak yang memiliki distribusi yang sangat bagus, pembangkitan bilangan yang sangat cepat dan menggunakan memori yang efisien.

Pada tugas akhir ini penulis mencari tahu presentase keberhasilan implementasi algoritma *One Time Pad* untuk mengenkripsi dan mendekripsi berkas dokumen dalam bentuk .txt,.doc.

Hasil penelitian yang dilakukan sebanyak 10 pengujian memperlihatkan bahwa presentase keberhasilan implementasi algoritma *One Time Pad* untuk mengenkripsi dan mendekripsi berkas dokumen dalam bentuk .txt,.doc adalah 100% serta lama proses enkripsi dekripsi didasarkan pada randomnya kunci acak yang digunakan dalam proses tersebut.

Kata Kunci : kriptografi, *Mersenne Twister, One Time Pad*

ABSTRACT

Basically perform data transmission without providing security on the content of the data sent, may cause tapping on shipping lanes. Important data format easy to be tapped .txt and .doc formatted data can be encrypted using a password but the feature has the disadvantage of their application that can be used to break into files that have been encrypted. For that role of information security technology really - really needed. One technique for data security is to use the data encryption algorithms.

One Time Pad algorithm is an algorithm because the algorithm is simple and unbreakable One Time Pad has rows of random keys that are added to the plaintext message that is not random to produce ciphertext which is entirely random. Random key is generated using a random number generator, among others Mersenne Twister. Mersenne Twister random number which has resulted in a very good distribution, generation numbers are very fast and uses memory efficiently.

In this thesis the author to find out the percentage of successful implementation of One Time Pad algorithm to encrypt and decrypt the document file in the form of .txt, .doc.

Results of research conducted as many as 10 test showed that the percentage of successful implementation of One Time Pad algorithm to encrypt and decrypt the document file in the form of .txt, .doc is 100% and the long process of encryption decryption randomnya based on random keys that are used in the process.

Keywords: cryptography, Mersenne Twister, One Time Pad