PLAGIAT MERUPAKAN TINDAKAN TIDAK TERPUJI

ABSTRAK

Keamanan data merupakan hal penting dalam menjaga kerahasiaan data-data tertentu yang hanya boleh diketahui oleh pihak yang memiliki hak saja. Apabila pengiriman data dilakukan melalui jaringan, maka kemungkinan data tersebut diketahui oleh pihak yang tidak berhak, menjadi besar

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara mengubahnya dari satu bentuk ke bentuk lainnya yang tidak dapat dimengerti lagi artinya. *Columnar transposition* merupakan salah satu bagian dari cipher transposisi dengan metode kriptografi dimana pesan dituliskan berderet dari suatu panjang yang ditetapkan, lalu dibaca kembali kolom per kolom dengan urutan pembacaan berdasarkan suatu kata kunci. Panjang deret ditentukan oleh panjang kata kunci. Urutan pembacaan kolom berdasarkan urutan kolom. Berbagai metode kriptanalisis terus dikembangkan. *Brute force attack* dan metode *kasiski* adalah metode untuk melakukan kriptanalisis.

Dalam Tugas Akhir ini penulis melakukan penelitian proses kriptanalisis terhadap algoritma transposisi Columnar dengan menggunakan metode *brute force attack* untuk mencari kunci dan metode *kasiski* untuk mengestimasi panjang kunci. Hasil akhir penelitian ini *brute force attack* mampu membongkar pola kunci dengan panjang kunci 7 dari algoritma *columnar transposition* dan metode *kasiski* tidak bekerja untuk mengestimasi panjang kunci pada algoritma *columnar transposition*.

Kata kunci : kriptografi, *columnar transposition*, kriptanalisis, *brute force attack*, *kasiski*

PLAGIAT MERUPAKAN TINDAKAN TIDAK TERPUJI

ABSTRACT

Data security is considered as an important thing to keep data which is only known by certain people who have right. When the data delivering was done by connection network, it will make a big possibility for the other people who have not have the right to discover the data.

Cryptography is the science and art to keep a confidentiality of the message by changing one type to another type which cannot be understood. Columnar transposition is a part of a transposition cipher which uses cryptographic method where the messages is written in a line using a specified length, then it is re-read in a specified order for each colomn based on a keyword. The length of line is based on the length of the keyword. The order of the colomn reading is based on the order of the colomns. Some methods of cryptanalysis have being continued to be developed. The brute force attack and *kasiski* method are the methods which are used in the cryptanalysis.

In this final project, the writer studied the process of the columnar transposition cryptanalysis of the algorithm using a brute force attack to find the keyword and *kasiski* method to predict the length of the keyword. As the result; the brute force attack was able to reveal the key patterns on the columnar transposition with key lenght 7 of the algorithm, and the *kasiski* method was ineffective to predict the length of the keyword on the columnar transposition of the algorithm.

Keywords: cryptography, columnar transposition, cryptanalysis, brute force attack, *kasiski*