ABSTRAK

Penggunaan algoritma kriptografi modern yang ditemukan dan dikembangkan masih banyak ditemui, algoritma kriptografi klasik masih digunakan untuk mengenkripsi suatu plainteks. Salah satu metode enkripsi dalam algoritma kriptografi klasik adalah Vigenere Cipher. Dalam penerapannya metode enkripsi dengan algoritma klasik masih sangat mudah dipecahkan menggunakan komputer canggih. Metode enkripsi gabungan berfungsi untuk memperkuat penyandian pesan menggunakan algoritma vigenere dan transposisi myszkowski. Kriptanalisis Hasil Enkripsi Algoritma Vigenere Cipher Dan Tranposisi Myszkowski dilakukan untuk menganalisis hasil kekaburan enkripsi gabungan vigenere dan transposisi myszkowski menggunakan matriks unjuk kerja *avalanche effect* dan operasi *XOR***.** Berdasarkan hasil penelitian, kombinasi algoritma vigenere dan transposisi myszkowski memiliki tingkat kekaburan yang lebih baik dibanding enkripsi algoritma vigenere. Kemudian untuk variasi pesan dan kunci 2 bit pada hasil enkripsi antara kombinasi algoritma vigenere dan transposisi myszkowski dengan algoritma vigenere lebih baik dari pada 1 bit pada hasil enkripsi.

Kata kunci : Vigenere Cipher, Transposisi Myszkowski, Kriptografi.

ABSTRACT

The use of modern cryptographic algorithms that are found and developed are still widely found, classical cryptographic algorithms are still used to encrypt a plaintext. One of the encryption methods in classical cryptographic algorithms is the Vigenere Cipher. The encryption method with the classical algorithm is still very easy to crack using sophisticated computers. The combined method works to strengthen the encoding of messages using the vigenere algorithm and myszkowski transposition. The cryptanalysis of the results of the encryption of the Vigenere Cipher Algorithm and Myszkowski Transposition was carried out to analyze the combined blurring of the vigenere and myszkowski transposition using the avalanche effect performance and XOR operation. Based on the research, the combination of vigenere algorithm and myszkowski transposition has a better level of obscurity than the encryption algorithm of vigenere. Then for the variation of the message and the 2-bit key in the encryption results between the combination of the vigenere algorithm and myszkowski transposition with the vigenere algorithm, it is better than 1 bit in the encryption result.

Keywords: Vigenere Cipher, Myszkowski Transposition, Cryptography.