MODIFIKASI ALGORITMA *PLAYFAIR CIPHER* DENGAN KONVERSI KODE ASCII-BINER UNTUK PENYANDIAN PESAN TEKS

Latisya 14117005

Pembimbing : Angga Wijaya, S.Si., M.Si.[1], Imam Ekowicaksono, S.Si., M.Si.[2]

ABSTRAK

Pertukaran informasi melalui internet sudah menjadi hal yang biasa dilakukan sehingga pengaksesan data dan informasi menjadi lebih mudah dan terbuka. Hal tersebut tentu berpengaruh pada keamanan informasi. Salah satu cara menangani hal tersebut adalah dengan menerapkan kriptografi.

Dalam kriptografi, salah satu algoritma klasik yang digunakan untuk pengamanan pesan yaitu Algoritma *Playfair Cipher*. Namun, terdapat beberapa kekurangan pada algoritma tersebut sehingga dirasa perlu untuk memodifikasi Algoritma *Playfair Cipher* dengan tujuan menghasilkan hasil enkripsi yang lebih baik.

Pada penelitian ini, dilakukan pengembangan terhadap Algoritma *Playfair Cipher* dengan melakukan proses enkripsi pada biner dari setiap karakter pesan dan mengubah karakter kedalam bentuk kode ASCII berjumlah 255 karakter. Pesan akan dienkripsi menggunakan kunci berupa permutasi angka. Proses enkripsi pesan dilakukan menggunakan matriks berukuran 4×4.

Hasil dari penelitian ini plainteks berhasil dienkripsi menjadi cipherteks berupa kode ASCII, pada pengujian *recovery* cipherteks dapat didekripsikan kembali secara utuh, pada analisis frekuensi monogram didapat nilai variansi *plaintext* sebesar 999,62 dan nilai variansi *ciphertext* sebesar 4612,38 sedangkan pada analisis frekuensi bigram didapat nilai variansi *plaintext* sebesar 1543,50 dan nilai variansi *ciphertext* sebesar 41623,16. Dari pengujian waktu komputasi rata-rata waktu yang didapat untuk proses enkripsi dengan algoritma *Playfair Cipher* biasa sebesar 0,42 detik sedangkan dengan algoritma *Playfair Cipher* ASCII – Biner sebesar 0,84 detik, untuk proses dekripsi dengan algoritma *Playfair Cipher* biasa

sebesar 0,46 detik sedangkan dengan algoritma *Playfair Cipher* ASCII – Biner sebesar 0,29 detik.

Pada penggunaan *resource* ukuran file pesan hasil enkripsi dengan algoritma *Playfair Cipher* biasa mengalami penurunan sebesar 35% sedangkan dengan algoritma *Playfair Cipher* ASCII – Biner mengalami kenaikan sebesar 119%.

Kata kunci : Keamanan Informasi, Enkripsi, Dekripsi, Kriptografi, *Playfair Cipher*

MODIFICATION OF THE PLAYFAIR CIPHER ALGORITHM WITH ASCII-BINARY CODE CONVERSION FOR ENCODING OF TEXT MESSAGES

Latisya 14117005

Supervisor : Angga Wijaya, S.Si., M.Si.[1], Imam Ekowicaksono, S.Si., M.Si.[2]

ABSTRACT

Information exchange via the internet has become a common practice so that accessing data and information becomes easier and more open. This certainly affects information security. One of the security methods is by implementing cryptography.

In cryptography, one of the classic algorithms used to secure messages is the Playfair Cipher Algorithm. However, there are some deficiencies in this algorithm so that it is necessary to modify the Playfair Cipher Algorithm in order to produce better encryption results.

In this study, the Playfair Cipher Algorithm was developed by encrypting the binary of each message character and converting the characters into an ASCII code of 255 characters. The message will be encrypted using a key in the form of a permutation number. The process of encrypting the message was carried out using a 4 × 4 matrix.

The results of this study were that the plaintext was successfully encrypted into a ciphertext in the form of ASCII, in recovery testing the ciphertext could be completely decrypted again, In the monogram frequency analysis, the plaintext variance value was 999.62 and the ciphertext variance value was 4612.38, while in the Bigram frequency analysis the plaintext variance value was 1543.50 and the ciphertext variance value was 41623.16. From testing the computation time the average time obtained for the encryption process with the usual Playfair Cipher algorithm is 0.42 seconds while the Playfair Cipher ASCII - Binary algorithm is

0.84 seconds, for the decryption process using the usual Playfair Cipher algorithm is 0.46 seconds while the Playfair Cipher ASCII - Binary algorithm is 0.29 seconds.

In the use of resource, the message file size of the encryption results with the usual Playfair Cipher algorithm has decreased by 35% while the Playfair Cipher ASCII - Binary algorithm has increased by 119%.

Keyword : *Information Security, Encryption, Decryption, Cryptography, Playfair Cipher*