TITLE

ANALISIS PERBANDINGAN KEAMANAN KRIPTOGRAFI KLASIK PADA ALGORITMA MODIFIKASI PLAYFAIR CIPHER BERBASIS MATRIKS 8X8 DAN 16X16

ABSTRACT

Algoritma Playfair Cipher telah banyak dimodifikasi oleh para peneliti kriptografi, salah satunya melalui ukuran matriks kunci. Pada penelitian Tugas Akhir ini, algoritma Playfair Cipher yang diteliti adalah Playfair Cipher berbasis matriks kunci 8x8 dan 16x16. Tujuan penelitian ini yaitu mengimplementasikan dan menganalisis perbandingan keamanan kedua algoritma tersebut berdasarkan waktu proses enkripsi dan dekripsi secara komputasi, baik melalui proses konversi karakter acak menjadi angka ASCII maupun yang tidak dikonversi. Selanjutnya, dilakukan analisis waktu generate matriks terhadap panjang kunci tertentu, analisis perbandingan ukuran file input/output hasil enkripsi dan dekripsi, analisis keamanan terhadap brute force attack (waktu, jumlah kombinasi kunci dan nilai peluang) dan analisis frekuensi kemunculan digraf. Hasil pengujian menunjukkan bahwa waktu yang dibutuhkan untuk proses enkripsi dan dekripsi dengan dilakukan konversi lebih lama dibandingkan dengan non konversi. Ukuran file hasil enkripsi yang dihasilkan dengan proses konversi pun lebih besar dibandingkan dengan non konversi. Total karakter untuk melakukan brute force attack adalah sebanyak 256! (faktorial), lebih banyak dari Playfair Cipher 8x8 yaitu sebanyak 64! (faktorial). Nilai peluang untuk dapat menerka suatu panjang kunci pada Playfair Cipher 16x16 lebih kecil, karena waktu yang dibutuhkan lebih lama dan jumlah kombinasi kunci yang dapat diterka lebih banyak. Total digraf yang dibutuhkan untuk melakukan ciphertext-only attack juga lebih banyak, yaitu 65.536 digraf. Berdasarkan hasil analisis tersebut, penerapan algoritma Playfair Cipher 16x16 dinilai lebih baik dan lebih aman bila dibanding dengan Playfair Cipher 8x8.
Kata kunci: Playfair Cipher 8x8, Playfair Cipher 16x16, konversi ASCII