ABSTRAK

Aplikasi matriks pada permasalahan kriptografi, khususnya algoritma *Hill Chiper*, memerlukan matriks yang memiliki invers terhadap operasi perkaliannya sebagai kunci dan pengacak plainteks. Salah satu matriks tersebut adalah matriks Hadamard. Matriks Hadamard merupakan matriks yang memiliki entri 1 atau -1 dan setiap barisnya saling ortogonal. Terdapat lima sifat matriks Hadamard yang dibahas dalam penelitian ini. Pertama, determinan matriks Hadamard berorde n adalah $n^{\frac{n}{2}}$. Kedua, matriks ini menghasilkan n kali matriks identitas apabila dikalikan dengan matriks transposnya. Ketiga, matriks Hadamard memiliki invers terhadap operasi perkalian matriks. Keempat, hasil operasi transpos matriks Hadamard merupakan matriks Hadamard. Kelima, invers matriks Hadamard terhadap operasi penjumlahannya merupakan matriks Hadamard. Pengaplikasian matriks Hadamard pada permasalahan kriptografi dengan algoritma *Hill Chiper* memerlukan dua buah kunci, yaitu kunci publik dan kunci privat sedemikian sehingga proses enkripsi dan dekripsinya dimodifikasi dengan melibatkan operasi modulo. Syarat suatu matriks Hadamard dapat digunakan dalam algoritma tersebut adalah orde matriksnya harus relatif prima dengan operasi modulo yang digunakan.

Kata kunci: matriks Hadamard, *Hill Chiper*, enkripsi, dekripsi, modulo

ABSTRACT

The matrices application to cryptographic problems, especially with Hill Chiper algorithm, needs an invertible matrix as a key and a plaintext's difuser. One of the invertible matrices is a Hadamard matrix. Hadamard matrices are square matrices that have the entries of 1 or -1, so that every row is orthogonal to each other. There are five properties of Hadamard matrix discussed in this study. First, the determinant of Hadamard matrix of order n is $n^{\frac{n}{2}}$, Second, the multiplication between a Hadamard matrix and its transpose matrix equals to n times identity matrix I. Third, every Hadamard matrix is invertible. Fourth, the transpose of a Hadamard matrix is a Hadamard matrix. Fifth, the negative of a Hadamard matrix is a Hadamard matrix. The applications of Hadamard matrices to cryptographic problems with the Hill Chiper algorithm require two keys, namely public and private keys so that the encryption and decryption process are modified by involving modulo operation. Hadamard matrices can be used in this algorithm if and only if the order of the matrix is relatively prime to the modulo operation used.

Keywords: *Hadamard matrix, Hill Chiper, encryption, decryption, modulo*