ABSTRAK

Saat ini teknik kriptografi hill Cipher banyak di implementasikan pada berbagai aplikasi. Dalam implementasinya banyak ditemui kesalahan ataupun kecerobohan seperti kehilangan matriks kunci ataupun lupa menyimpanya dengan benar. Oleh karena itu dibutuhkan teknik kriptanalisis untuk mendapatkan kembali pesan yang terenkripsi tersebut. Teknik kriptanalisis pada kriptografi Hill Cipher yang telah diketahui adalah dengan menggunakan persamaan linier, metode serangan yang bisa dilakukan adalah *brute force attack* dan *known plaintext attack*. Dalam penelitian ini akan dilakukan kriptoanalisis menggunakan metode serangan *known plaintext attack*, sehingga dapat mengetahui kunci dari sebuah pesan yang terenkripsi.

ABSTRACT

Currently, hill Cipher cryptographic techniques are widely implemented in various applications. In its implementation, there are many errors or carelessness such as losing the key matrix or forgetting to store it properly. Therefore, a cryptanalysis technique is needed to retrieve the encrypted message. The cryptanalysis technique in Hill Cipher cryptography that has been known is to use linear equations, the attack methods that can be done are brute force attacks and known plaintext attacks. In this study, cryptanalysis will be carried out using the known plaintext attack method, so that it can find out the key of an encrypted message.