**ABSTRAK**

Sandi Hill pada umumnya menggunakan matriks persegi yang invertibel atas $Z\_{26}$ sebagai kunci. Karena digunakan atas $Z\_{26}$ yang tidak field, maka sandi ini akan lebih terbatas dalam pemilihan kuncinya. Dengan berdasar pada teori Matriks Invers Tergeneralisasi akan diteliti syarat dan ketentuan agar dapat memperluas sandi hill supaya memungkinkan untuk memakai kunci matriks persegi panjang atas $Z\_{P}$ dimana *P* adalah bilangan prima. $Z\_{P}$ merupakan bilangan yang field, sehingga dalam pemilihan kuncinya akan lebih tidak terbatas.

Sandi hill memanfaatkan metode perkalian matriks dalam proses enkripsi dan dekripsi. Penyandian pesan dimulai dengan melakukan proses enkripsi sedangkan dalam menerjemahkan pesan dapat dilakukan dengan proses dekripsi yang memanfaatkan invers dari sebuah matriks.

Pengembangan metode sandi hill ini, diharapkan dapat memberikan keamanan pesan yang lebih baik jika dibandingkan metode sandi hill yang hanya menggunakan matriks persegi yang invertible pada Z26.

Kata kunci : sandi hill, matriks invers tergeneralisasi, enkripsi, dekripsi.

**ABSTRACT**

Cipher Hill in general use square matrix invertibel on $Z\_{26}$ as key. Because that used on $Z\_{26}$ is not field, then the cipher will be more limited in the selection key. One based on the generalized inverse matrix theory terms and conditions will be examined in order to expand the Cipher Hill that makes it possible to use a rectangular matrix keys on $Z\_{P}$ where P is a prime number. $Z\_{P}$ is a number field, resulting in the selection of the key would be unlimited.

Cipher Hill utilizing matrix multiplication method in the process of encryption and decryption. Encoding of the message begins with the translation of the encryption process whereas a message can be done by utilizing the inverse decryption process of a matrix.

Development of methods Cipher Hill, is expected to provide safety messages better than the method using only passwords hill square matrix invertible in $Z\_{26}$.

Keyword : cipher hill, generalized inverse of matrices, encryption, decryption.