PENGGABUNGAN MODIFIKASI *HILL CIPHER* DAN *ELLIPTIC CURVE CRYPTOGRAPHY* UNTUK MENINGKATKAN KEAMANAN PESAN

ABSTRAK

Seiring perkembangan teknologi, pesan rahasia semakin rentan untuk diretas. Oleh karena itu, pengamanan terhadap pesan rahasia perlu ditingkatkan. Kriptografi mempelajari teknik atau algoritma untuk mengamankan pesan, diantaranya adalah *hill cipher* dan *elliptic curve cryptography* (ECC). *Hill cipher* merupakan suatu kriptosistem yang menggunakan matriks sebagai kuncinya, dengan kunci matriks yang umum digunakan merupakan suatu matriks berukuran$n \times n$. *Elliptic curve cryptography* menggunakan titik-titik pada kurva eliptik yang merupakan suatu lapangan atas bilangan prima dengan operasi penjumlahan titik. Dalam penelitian ini disajikan pengembangan kriptosistem *hill cipher* dan *elliptic curve cryptography* dengan cara menggabungkan kedua kriptosistem tersebut. Dalam penggabungan tersebut, dilakukan suatu modifikasi sehingga *hill cipher* yang digunakan dapat memiliki suatu kunci matriks yang berukuran $m \times n$. Kriptografi gabungan *hill* cipher dan *elliptic curve cryptography* ini menggunakan 95 karakter dari bilangan ASCII. Selain itu, hasil penelitian diimplementasikan menjadi suatu program komputer. Penggabungan kedua kriptosistem ini bertujuan untuk meningkatkan keamanan suatu pesan yang bersifat rahasia sehingga pesan tersebut lebih sulit untuk diretas.

Kata kunci: *Hill Cipher*, Modifikasi *Hill Cipher*, *Elliptic Curve Cryptography*

COMBINATION OF MODIFIED HILL CIPHER AND ELLIPTIC CURVE CRYPTOGRAPHY TO STRENGHTHEN THE SECURITY OF MESSAGE

ABSRACT

As technology develops, secret messages are increasingly vulnerable to be hacked. Therefore, security level of the messages needs to be improved. The studies of Cryptography show several techniques or algorithms to secure the messages, including hill cipher and elliptic curve cryptography (ECC). Hill cipher is a cryptosystem that use matrices as the keys, which it is usually use $n \times n$ matrices. Elliptic curve cryptography uses points on elliptic curve, which are a field over prime numbers with addition operation. This research develop a cryptosystem by combining both hill cipher and elliptic curve cryptography. The study modified the hill cipher such that it is able to use $m \times n$ matrices as the keys. Moreover, the developed cryptosystem uses 95 character from ASCII numbers. Finally, the developed of hill cipher and elliptic curve cryptography is implemented into a computer program. Hence, the combined cryptosystem is expected to be able to strengthen the security of message, therefore it is difficult to be hacked.

Keywords: *Hill Cipher*, *Modified Hill Cipher*, *Elliptic Curve Cryptography*