**A NEW CRYPTOGRAPHY METHOD BASED ON HILL AND RAIL FENCE ALGORITHMS**

**Ashty M. Aaref 1, Ann Z. Ablhd 2**

1, 2 Lecturer, Software Engineering Department college technology / Kirkuk, Iraq

ann\_zeki2001@yahoo.com 1, ashty\_06@yahoo.com 2

(Received: 29/12/2015; Accepted: 28/3/2016)

**ABSTRACT:**- Encryption has a great benefit, it provides privacy and security of all concepts of data transmitted across open networks. An urgent need for methods of strong encryption has become important with the rapid development of the computer, it detract from the strength of encryption; and because the increase computer speed means shortening the time that the computer needs to break or disclosure of specific encryption key.

Encryption may be strong or weak, to measure the encryption strength by the time and resources required for the process of detecting non-encrypted texts of encrypted texts. As a result of testing proposed system it appear that this system is strong encryption cipher text because it is hard to detect with the time or provide the necessary tools to detect the plain text.

Due to the wide use of broken cipher methods in Cryptography. There are many important information to be secure. It proposed a new approach of ciphering, by mixing a substitution followed by a transposition cipher methods to produce a new secure method difficult to break. This is a bridge from a classical to modern ciphers.

The substitution cipher algorithm that is used in this paper is Hill cipher, and the transposition cipher algorithm that is used is Rail fence.

The language that is used for this proposed algorithm is C++ with Object Oriented Programming. The proposed system is called RailHill.

***Keywords:*** *encryption, decryption, transposition, substitution.*