ISSN: 1391-8796
Proceedings of 8th Ruhuna International Science & Technology Conference
University of Ruhuna, Matara, Sri Lanka
February 17, 2021

A novel cryptographic scheme on a variation of hill cipher

Ranasinghe P. G. R. S.[1*], Wijesekara W. M. P. R.[2]

[1]*Department of Mathematics, Faculty of Science, University of Peradeniya, Sri Lanka*

[2]*Department of Mathematics, University of Ruhuna, Matara, Sri Lanka*

Cryptography has always been an active and engaging area of research. It is the science of keeping information secure by transforming into a form that unintended recipients cannot comprehend. In the world of today, making messages secret has become of paramount importance, especially with the advent of electronic messaging and the internet. Even there are many encryption algorithms exist, the need of new non-standard encryption algorithms is in much demand to address the advent of technology. In the present work, the main cryptography technique we use is the Hill cipher which was invented by Lester S. Hill in 1929. It is a polygraphic substitution cipher based on matrix theory in linear algebra. Here, the encryption algorithm takes plaintext letters as input and produces ciphertext letters for them. To encrypt a message, we first convert the keywords into key matrices. But every possible matrix is not a candidate for a possible key matrix since in order to decrypt, we need to have an inverse key matrix, and not every matrix is invertible. In order to be a usable key, the matrix must have a non-zero determinant which is co-prime to the length of the alphabet. Our method is better at securing data that will be transmitted in an open network as it uses different keys for each plaintext block instead of using one key matrix for all blocks. The main objective of our work is to encrypt a text more securely using a technique different from the conventional Hill Cipher. In conclusion, the key aspect of our algorithm is that the keys must be kept confidential. In future, we plan to explore more on this algorithm to dive into the security aspect as well as to incorporate the security and implement a computer program to handle longer texts.

Key words: *Cryptography, encryption, decryption, plaintext, ciphertext*

*Corresponding author: rajithamath@sci.pdn.ac.lk