A Modified Version of Hill Cipher

A.F.A.Abidin, O.Y.Chuan
Faculty of Informatics
Universiti Sultan Zainal Abidin
21300 Kuala Terengganu, Terengganu, Malaysia.

M.R.K.Ariffin
Institute for Mathematical Research
Universiti Putra Malaysia
43400 Serdang, Serdang, Malaysia.

Abstract—The Hill cipher is the first polygraph cipher which has a few advantages in data encryption. However, it is vulnerable to known plaintext attack. Besides, an invertible key matrix is needed for decryption. It may become problematic since an invertible key matrix does not always exist. The objective of this paper is to modify the existing Hill cipher to tackle these two issues. In this paper, a robust Hill algorithm (Hill++) has been proposed. The algorithm is an extension of Affine Hill cipher. A random matrix key, RMK is introduced as an extra key for encryption. An algorithm proposed by Bibhudendra et al. for involutory key matrix generation is also implemented in the proposed algorithm. A comparative study has been made between the proposed algorithm and the existing algorithms. The encryption quality of the proposed algorithm is also measured by using the maximum deviation factor and correlation coefficient factor. The results showed that Hill++ is a better algorithm compared to the existing Hill algorithms.

Keywords: Affine cipher, Cryptography, Hill cipher, involutory matrix.