International J. of Math. Sci. & Engg. Appls. (IJMSEA)
ISSN 0973-9424, Vol. 5 No. IV (July, 2011), pp. 19-23

A GENERALIZED HILL CIPHER USING MATRIX TRANSFORMATION

G. A. DHANORKAR AND A. P. HIWAREKAR

Abstract

An improvement of the Hill cipher is proposed in this paper. In the Hill cipher algorithm we required invertiable key matrix for encrypting the plane text. But, if the key matrix is not invertible, the encrypted text cannot be decrypted. Moreover, Hill cipher can be easily broken with a known plain text attack revealing weak security. The proposed variant of the Hill cipher that overcomes these disadvantages. To overcome the drawbacks, the proposed cryptosystem uses randomly generated matrix but which is invertible as an encryption key.

Key Words and Phrases : *Creation of invertible matrix, Cryptosystem, Decryption, Encryption, Hill Cipher, Multiplication of matrices, Some rules of number theory: The congruence modulo operator.*