A novel enhancement technique of the hill cipher for effective cryptographic purposes.

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. In this study, 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 for involutory key matrix generation is also implemented in the proposedalgorithm. Results: 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 proposed algorithm introduced a random matrix key which is computed based on the previous ciphertext blocks and a multiplying factor. A modified of Hill Cipher is free from the all-zero plaintext blocks vulnerability. Usage of involutory key for encryption and decryption managed to solve the non invertible key matrix problem. It also simplify the computational complexity in term of generating the inverse key matrix.

Keyword: Affine cipher; Cryptography theory; Hill cipher; Involutory matrix; Polygraph cipher; Data encryption; Symmetric cryptosystem; Advanced Encryption Standard (AES); Data Encryption Standard (DES); Initi Vector (IV); Proposed algorithm.