Abstract

In this paper conventional Playfair Cipher is being modified by encrypting the plaintext in blocks. For each block the keyword would be the same but the matrix will shift by some random value. As a result of which the diagram analysis would be very difficult which is done in the traditional Playfair Cipher to obtain the plaintext from the ciphertext. The shift value will be generated using SHA-1 which is very secure. Playfair Cipher method, based on polyalphabetic cipher is relatively easy to break because it still leaves much of the structure and a few hundred of letters of ciphertext are sufficient. To add to its security and to make it more usable we are using 6x6 matrix instead of 5x5 which will be able to cover 26 alphabets in English and ten numerals i.e. from 0 to 9. This 6x6 matrix eliminate the case of putting of 2 alphabets (I and J) together in the matrix as it was in the 5x5 matrix. Plaintext as well as key can be numeral, alphabetic or
combination of both.

References

- Anne-Canteaut(Editor)&apos;Ongoing Research Area in Symmetric Cryptography&amp;apos;; ENCRYPT, 2006.

Index Terms

Computer Science

Security

Keywords

Playfair Cipher Random number SHA-1 Polyalphabetic cipher