Improving Security Using Refined 16 X 16 Playfair Cipher for Enhanced Advanced Encryption Standard (AES)

Ibukun Eweoya, Olawande Daramola, Nicholas Omoregbe
Covenant University, Ota, Nigeria
Email: ibukun.eweoya@covenantuniversity.edu.ng
olawande.daramola@covenantuniversity.edu.ng
nomoregbe@covenantuniversity.edu.ng

Abstract: The conventional playfair cipher has lost its potency due to the sophistication of modern systems that can break it by brute force. This work proposes an improved playfair encryption and decryption that will be hard to break by brute force procedure. It uses a 16 X 16 arrays of ASCII characters ensuring relevance in all computing fields instead of the conventional 26 upper case alphabets substitution. An implementation of the cryptographic concept was realized using PHP programming language and embedded in the Advanced Encryption Standard (AES) algorithm. We argue from the perspective of cryptanalysis that our proposed approach is stronger and will be more difficult to break. http://journals.covenantuniversity.edu.ng/cjict/published/Ibukun.pdf