Abstract

This paper shows the possibility of exploiting the features of Genetic Algorithm with poly substitution methods in a linear way, to generate ASCII values of the given text and then applying conversion, transposition with the features of Cryptography.

In polyalphabetic substitution ciphers the plaintext letters are enciphered differently depending upon their placement in the text. As the name polyalphabetic suggests this is achieved by using several two, three keys and random keys combinations instead of just one, as is the case in most of the simpler crypto systems. Using two keys, we take 2 keys e1,e2 and let the ASCII values of e1 be 1 and e2 be 2 and take the text, add ASCII values of e1 to first character and ASCII values of e2 to second character. Alternatively add the value of e1 and e2 to consecutive characters.
We can use Poly substitution method combining the features of cryptography for text encryption by 2 keys and 3 keys and even more then 3 keys to make the decryption process more complicated.

Reference

- Darrell Whitley, 'A Genetic Algorithm Tutorial', Computer Science Department, Colorado State University, Fort Collins, CO 80523.
- Sean Simmons, 'Algebraic Cryptoanalysis of Simplified AES', October 2009; 33, 4; Proquest Science Journals Pg.305.

Index Terms

Computer Science Information Security

Key words

Encryption

Decryption

Genetic Keys

Mono Substitution

Poly Substitution