Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.140 – 149

RESEARCH ARTICLE

Automated Cryptanalysis of Transposition Ciphers Using Cuckoo Search Algorithm

[1] Morteza Heydari*,[1] Mahdieh Nadi Senejani

[1]Department of Computer Engineering, College of Computer Science, Ashtian Branch,

Islamic Azad University, Ashtian, Iran

*E-mail: morteza2@gmail.com

Abstract

An approach of information security is Cryptography.Cryptanalysis is the science study to break cryptography without the encryption key. The present paper shows the benefits of the implementation of a novel genetic algorithm, the "Cuckoo Search" Algorithm (CSA) with new fitness function for the cryptanalysis of transposition cipher. The fitness function is evaluated based on the most common bigrams and trigrams. Results show that the algorithm proposed in this paper is effective for cryptanalysis of transposition cipher with long key lengths up to 30 due to its strong reliability and fast convergence speed.

Keywords: "Cuckoo Search" Algorithm (CSA), Cryptanalysis, Encryption key, Transposition Cipher.

Full Text: http://www.ijcsmc.com/docs/papers/January2014/V3I1201404.pdf