International J.of Multidispl.Research & Advcs. in Engg.(IJMRAE),
ISSN 0975-7074, Vol. 3, No. II (April 2011), pp. 45-51

GENETIC ALGORITHM AND CRYPTOGRAPHY

RAAD A. MUHAJJAR

Abstract

Genetic algorithms (GAs) are one of the best ways to solve a problem for which little is known. They are a very general algorithm and so will work well in any search space. All you need to know is what you need the solution to be able to do well, and a genetic algorithm will be able to create a high quality solution. Genetic algorithms use the principles of selection and evolution to produce several solutions to a given problem. This paper dedicated to explain how GAs has been used in the Cryptographic area. The first part of this paper explains use GAs in encryption while the second part explains use GAs in decryption.

Keywords : Genetic Algorithms, Cryptography, Pseudo-random bit generator, stream cipher, Caesar