Cryptologia. Volume:37 Number: 1 Pages: 51-68. January 2013

Genetic algorithms and mathematical programming to crack the spanish strip cipher

F.A. Campos, A. Gascon, J.M. Latorre, J. R. Soler

Abstract— This article describes the application of modern algorithms to crack the official encryption method of the Spanish Civil War: the Strip Cipher. It shows the differences in efficiency and effectiveness between a genetic algorithm and mathematical programming, the optimisation methods known collectively as mathematical optimisation. Unlike the genetic algorithm, the programming approach has been seen to lead to high computational costs or to non-legible plain texts, which make it impractical. To improve the search for the genetic operators used, a dictionary is applied to identify possible words in each partially decrypted text and, thus, unblock the process. Results and conclusions have been obtained by analysing the outcome of the algorithms when attacking real ciphertexts found in the General Archive of the Spanish Civil War in Spain. Both the mathematical programming and the genetic algorithm approaches have merit, but the latter has considerable practical advantages.

Index Terms— genetic algorithms, mathematical programming, poly-alphabetic substitution cipher, Spanish Civil War, Strip Cipher

Citation:
Campos, F.A.; Gascon, A.; Latorre, J.M.; Soler, J. R.; "Genetic algorithms and mathematical programming to crack the spanish strip cipher", Cryptologia, vol.37, no.1, pp.51-68. January, 2013.