Algorithms in Classical Cryptanalysis

François Morain

LIX, École polytechnique

November 23, 1998

Abstract

Till the end of World War I, cryptographic methods required only paper and pencil. Since this glorious period, machines first and then computers replace man in complicated cyphering and decyphering processes. It is interesting to consider this period with an algorithmic viewpoint and seek computer algorithms to break those old cyphers.

This talk describes algorithmic tools that can be used to break as automatically as possible cryptosystems based on mono- or polyalphabetical substitutions as well as transpositions. In particular, the talk will focus on combinatorial optimization methods, such as genetic algorithms. New ideas are also presented, that make it possible to break some systems with ease.