Using Ants to Attack a Classical Cipher

Matthew Russell, John A. Clark, and Susan Stepney

Department of Computer Science, University of York, York, YO10 5DD, U.K.
{matthew,jac,susan}@cs.york.ac.uk

1 Introduction

Transposition ciphers are a class of historical encryption algorithms based on rearranging units of plaintext according to some fixed permutation which acts as the secret key. Transpositions form a building block of modern ciphers, and applications of metaheuristic optimisation techniques to classical ciphers have preceded successful results on modern-day cryptological problems. In this paper we describe the use of Ant Colony Optimisation (ACO) for the automatic recovery of the key, and hence the plaintext, from only the ciphertext.

2 Cryptanalysis of Transposition Ciphers

The following simple example of a transposition encryption uses the key 31524:

```
  31524 31524 31524 31524 31524
  THEQU ICKBR OWNFO XJUMP EDXXX
⇒ HQTUE CBIRK WFOON JMXPJ DXEXX
```

Decryption is straightforward with the key, but without it the cryptanalyst has a *multiple anagramming* problem, namely rearranging columns to discover the plaintext:

```
H Q T U E      T H E Q U
C B I R K      I C K B R
W F O O N  ⇒   O W N F O
J M X P U      X J U M P
D X E X X      E D X X X
```

Traditional cryptanalysis has proceeded by using a statistical heuristic for the likelihood of two columns being adjacent. Certain pairs of letters, or *bigrams*, occur more frequently than others. For example, in English, 'TH' is very common. Using some large sample of normal text an expected frequency for each bigram can be inferred. Two columns placed adjacently create several bigrams. The heuristic d_{ij} is defined as the sum of their probabilities; that is, for columns i and j, $d_{ij} = \sum_r P(i_r j_r)$, where i_r and j_r denote the rth letter in the column and $P(xy)$ is the standard probability for the bigram "xy".

Maximising the sum of d_{ij} over a permutation of the columns can be enough to reconstruct the original key, and a simple greedy algorithm will often suffice.

However, the length of the ciphertext is critical as short ciphertexts have large statistical variation, and two separate problems eventually arise: (1) the greedy algorithm fails to find the global maximum, and, more seriously, (2) the global maximum does not correspond to the correct key.

In order to attempt cryptanalysis on shorter texts, a second heuristic can be employed, based on counting dictionary words in the plaintext, weighted by their length. This typically solves problem (2) for much shorter ciphertexts, but the fitness landscape it defines is somewhat discontinuous and difficult to search, while the original heuristic yields much useful, albeit noisy, information.

3 Ants for Cryptanalysis

A method has been found that successfully deals with problems (1) and (2), combining both heuristics using the ACO algorithm Ant System [2]. In the ACO algorithm, ants construct a solution by walking a graph with a distance matrix, reinforcing with pheromone arcs that correspond to better solutions. An ant's choice at each node is affected by both the distance measure and the amount of pheromone deposited in previous iterations.

For our cryptanalysis problem the graph nodes represent columns, and the distance measure used in the ants' choice of path is given by the d_{ij} bigram-based heuristic, essentially yielding a maximising Asymmetric Travelling Salesmen Problem. The update to the pheromone trails, however, is determined by the dictionary heuristic, not the usual sum of the bigram distances. Therefore both heuristics have influence on an ant's decision at a node: the bigram heuristic is used directly, and the dictionary heuristic provides feedback through pheromone.

In using ACO with these two complementary heuristics, we found that less ciphertext was required to completely recover the key, compared both to a greedy algorithm, and also to other metaheuristic search methods previously applied to transposition ciphers: genetic algorithms, simulated annealing and tabu search [4, 3, 1]. It must be noted that these earlier results make use of only bigram frequencies, without a dictionary word count, and they could conceivably be modified to use both heuristics. However, ACO provides an elegant way of combining the two heuristics.

References

1. Andrew Clark. *Optimisation Heuristics for Cryptology.* PhD thesis, Queensland University of Technology, 1998.
2. Marco Dorigo, Vittorio Maniezzo, and Alberto Colorni. The Ant System: Optimization by a colony of cooperating agents. *IEEE Transactions on Systems, Man, and Cybernetics Part B: Cybernetics*, 26(1):29–41, 1996.
3. J. P. Giddy and R. Safavi-Naini. Automated cryptanalysis of transposition ciphers. *The Computer Journal*, 37(5):429–436, 1994.
4. Robert A. J. Matthews. The use of genetic algorithms in cryptanalysis. *Cryptologia*, 17(2):187–201, April 1993.