**An investigation into the Zodiac Ciphers using Genetic Algorithms**

Final Report for CS39440 Major Project

*Author*: Martin Key ([mak18@aber.ac.uk](mailto:yourid@aber.ac.uk))

*Supervisor*: Dr. Richard Jensen ([mkj@aber.ac.uk](mailto:mkj@aber.ac.uk))

20 April 2014

Version 1.0 (Draft)

This report is submitted as partial fulfilment of a BSc degree in

Computer Science (G400)

Department of Computer Science

Aberystwyth University

Aberystwyth

Ceredigion

SY23 3DB

Wales, UK

**Declaration of originality**

In signing below, I confirm that:

* This submission is my own work, except where clearly indicated.
* I understand that there are severe penalties for plagiarism and other unfair practice, which can lead to loss of marks or even the withholding of a degree.
* I have read the sections on unfair practice in the Students’ Examinations Handbook and the relevant sections of the current Student Handbook of the Department of Computer Science.
* I understand and agree to abide by the University’s regulations governing these issues.

Signature ……………………………………………. (Martin Key)

Date …………………………………………………

**Consent to share this work**

In signing below, I hereby agree to this dissertation being made available to other students and academic staff of the Aberystwyth Computer Science Department.

Signature ……………………………………………. (Martin Key)

Date …………………………………………………

# Abstract

Contents

1 Introduction 4

1.1. Overview 4

1.2. Aims 4

2 Background 5

2.1. Substitution Ciphers 5

2.2. Zodiac Ciphers 5

2.3. Genetic Algorithms 5

3 Analysis 6

3.1. Ciphers 6

3.2. Genetic Algorithms 6

4 Design 7

4.1. Overview 7

4.2. Management 7

4.3. Population Generation 7

4.4. Chromosomes 7

4.5. Fitness 7

4.6. Selection 7

4.7. Genetics 7

4.8. Termination 7

5 Implementation 8

5.1. Management 8

5.2. Population Generation 8

5.3. Chromosomes 8

5.4. Fitness 8

5.5. Selection 8

5.6. Genetics 8

5.7. Termination 8

6 Testing 9

6.1. Unit 9

6.2. Functional 9

7 Methods 10

7.1. Substitution 10

7.2. Z408 10

7.3. Z340 10

8 Results 11

8.1. Substitution 11

8.2. Z408 11

8.3. Z340 11

9 Conclusions 12

9.1. Substitution 12

9.2. Z408 12

9.3. Z340 12

10 Critical Evaluation 13

11 Bibliography 14

12 Appendices 15

# Introduction

## Overview

In the \*late 1960s\* a man who named himself the 'Zodiac' first sent three letters, Vallejo Times, the San Francisco Examiner and the San Francisco Chronicle respectively. Each of these letters contained one part of a cipher which claimed responsibility for a number of murders, and plans for further attempts. Decrypted by a couple, Donald and Bettye Harden, this cipher did not contain enough information to identify the perpetrator.

## Aims

# Background

## Substitution Ciphers

## Zodiac Ciphers

## Genetic Algorithms

# Analysis

## Ciphers

## Genetic Algorithms

# Design

## Overview

## Management

## Population Generation

## Chromosomes

## Fitness

## Selection

## Genetics

## Termination

# Implementation

## Management

## Population Generation

## Chromosomes

## Fitness

## Selection

## Genetics

## Termination

# Testing

## Unit

## Functional

# Methods

## Substitution

## Z408

## Z340

# Results

## Substitution

## Z408

## Z340

# Conclusions

## Substitution

## Z408

## Z340

# Critical Evaluation

# Bibliography

1. Anon., 2014. *Zodiac Ciphers Wiki.* [Online]   
   Available at: http://zodiackillerciphers.com/wiki/index.php  
   [Accessed April 2014].
2. Anon., n.d. *Feature Driven Development Processes.* [Online]   
   Available at: http://www.nebulon.com/articles/fdd/download/fddprocessesUSLetter.pdf  
   [Accessed 4 February 2014].
3. Atkins, T., 2014. *Substitution Cipher.* [Online]   
   Available at: http://rumkin.com/tools/cipher/substitution.php  
   [Accessed 20 April 2014].
4. Basavaraju, P. K., 2009. *Heuristic Search Cryptanalysis of the Zodiac 340 Cipher,* San Jose State University, California: Unpublished Master's Thesis.
5. Carrol, J. M. & Martin, S., 1986. The Automated Cryptanalysis of Substitution Ciphers. *Cryptologia,* 10(4), pp. 193-209.
6. Clarke, A. & Dawson, E., 1997. A Parallel Genetic Algorithm for Cryptanalysis of the Polyalphabetic Substitution Cipher. *Cryptologia,* 21(2), pp. 129-138.
7. Delman, B., 2004. *Genetic Algorithms in Cryptography.* Rochester Institute of Technology, Rochester: Unpublished Masters Thesis.
8. Diaz-Gomez, P. A. & Hougen, D. F., 2007. Initial Population for Genetic Algorithms: A Metric Approach. In: *GEM.* s.l.:s.n., pp. 43-49.
9. Matthews, R. A. J., 1993. The Use of Genetic Algorithms in Cryptanalysis. *Cryptologia,* 17(2), pp. 187-201.
10. Miller, B. L. & Goldberg, D. E., 1995. Genetic Algoritms, Tournament Selection and the Effects of Noise. *Complex Systems,* 9(3), pp. 193-212.
11. Odetayo, M. O., 1993. Optimal Population Size for Genetic Algorithms: An Investigation. *Genetic Algorithms for Control Systems Engineering, IEE Colloquium on,* 2(1).
12. Spillman, R., Janssen, M., Nelson, B. & Kepner, M., 1993. Use of A Genetic Algorithm in the Cryptanalysis of Simple Substitution Ciphers. *Cryptologia,* 17(1), pp. 31-44.
13. Symons, C., 2009. *Solving the Zodiac.* 1st ed. s.l.:C. Symons.
14. Thá̆ng, D., 2008. *Analysis of the Zodiac 340-Cipher,* San Jose State University, California: Unpublished Master's Thesis.
15. Toemeh, R. & Arumugam, S., 2008. Applying Genetic Algorithms for Searching Key-Space of Polyalphabetic Subsititution Ciphers. *International Arab Journal of Information Technology,* 5(1), pp. 87-91.
16. Whitley, D., 1993. A Genetic Algorithm Tutorial. *Statistics and Computing,* 4(2), pp. 65-85.
17. Whitley, D., 1994. Genetic Algorithms and Neural Networks. In: *Genetic Algorithms in Engineering and Computier Science 3.* s.l.:s.n., pp. 203-216.
18. Whitley, D., 2002. Genetic Algorithms and Evolutionary Computing. In: *Van Nostrand's Scientific Encyclopedia.* s.l.:s.n.

# Appendices