



Cryptanalysis Made Easy

The Art and Science of Solving Codes and Ciphers

Copyright © 2008, Chris Evans, Editor

This book was copyright protected and may not be reproduced in part or whole without the express written consent from the author of this book. All Rights Reserved.

www.quikmaneuvers.com

Table of Contents

Introduction

Part One - Introduction to Cryptanalysis

Chapter 1. Terminology and System Types

- Section I: Basic Concepts
- Section II: Cryptographic Systems

Chapter 2. Security of Cryptographic Systems

- Section I: Requirements of Military Systems
- Section II: Cryptanalytic Attack
- Section III: Analytic Aid

Part Two – Monographic Substitution Systems

Chapter 3. Monoalphabetic Unilateral Substitution

Systems Using Standard Cipher Alphabets

- Section I: Basis of Substitution Systems
- Section II: Monoalphabetic Unilateral Substitution
- Section III: Solution of Monoalphabetic Unilateral Ciphers Using Standard Cipher Alphabets

Chapter 4. Monoalphabetic Unilateral Substitution

Systems Using Mixed Cipher Alphabets

Section I: Generation and Use of Mixed Cipher Alphabets

Section II: Recovery of Mixed Cipher Alphabets

**Section III: Solution of Monoalphabetic Unilateral Ciphers
Using Mixed Cipher Alphabets**

Chapter 5. Monoalphabetic Multilateral Substitution Systems

Section I: Characteristics and Types

Section II: Analysis of Simple Multilateral Systems

Section III: Analysis of Variant Multilateral Systems

Part Three – Polygraphic Substitution Systems

Chapter 6. Characteristics of Polygraphic Substitution Systems

Section I: Characteristics of Polygraphic Encipherment

Section II: Identification of Polygraphic Substitution

Chapter 7. Solution of Polygraphic Substitution Systems

Section I: Analysis of Four-Square and Two-Square Ciphers

Section II: Analysis of Playfair Ciphers

Part Four – Polyalphabetic Substitution Systems

Chapter 8. Periodic Polyalphabetic Substitution Systems

Section I: Characteristics of Periodic Systems

Section II: Identifying Periodic Systems

Chapter 9. Solution of Periodic Polyalphabetic Systems

Section I: Systems Using Standard Cipher Alphabets

Section II: Systems Using Mixed Alphabets with Known Sequences

Section III: Solving Periodics with Unknown Sequences

Chapter 10. Aperiodic Polyalphabetic Ciphers

Part Five – Transportation Systems

Chapter 11. Types of Transportation Systems

Chapter 12. Solution of Numerically-Keyed Columnar Transportation Ciphers

Chapter 13. Transportation Special Solutions

Part Six – Analysis of Code Systems

Chapter 14. Types of Code Systems

Chapter 15. Analysis of Syllabary Spelling

Glossary

5 Appendixes (Separate PDF Document)

Frequency, Usage and Word Pattern Tables