

## Chapter 2

---

### Reading List and Resources

Kahn, David. *The Codebreakers*. New York. Macmillan, 1967.

A monumental - 1164 pages - history of codes and ciphers from ancient Greece to the present day. Good descriptions of the mechanics of cryptanalysis, with emphasis on the people involved. Also available in paperback from Signet (brutally abridged).

Note: A revised edition was published in November 1996.

Gaines, Helen Fouché. *Cryptanalysis*. New York. Dover, 1956.

Originally published before the war, this is the amateur cryptanalyst's bible. Clear, concise descriptions of many ciphers and how to attack them.

Sinkov, Abraham. *Elementary Cryptanalysis A Mathematical Approach*. Washington DC: The Mathematical Association of America, 1966.

This book contains a well-written description of several ciphers. More limited range than Gaines, but the treatment is deeper, with extremely good analysis of the mathematics involved. The third edition contains some BASIC programs for computer analysis.

Friedman, William F., and Lambros D. Callimahos. *Military Cryptanalytics*. Part 1 Vol. 1. Aegean Park Press, 1985.

Advanced solving methods for simple substitution, polygraphic substitution such as Playfair, and irregular substitution such as monome-dinome.

Friedman, William F., and Lambros D. Callimahos. *Military Cryptanalytics*. Part 1 Vol. 2. Aegean Park Press, 1985.

Tables of frequency data for English and other languages, and challenge problems supporting MC Part I Volume I.

Callimahos, Lambros D., and William F. Friedman. *Military Cryptanalytics*. Part 2 Vol. 1. Aegean Park Press, 1985.

Advanced solving methods for repeating-key systems such as Vigenère and Quagmires, symmetry of position, Progressive Key, and advanced polyalphabetic systems.

Callimahos, Lambros D., and William F. Friedman. *Military Cryptanalytics*. Part 2 Vol. 2. Aegean Park Press, 1985.

Introduction to traffic analysis, tables and problems supporting MC Part II Volume I, and the extremely interesting and educational Zandian Problem.

Gleason, Norma. *Cryptograms and Spygrams*. New York. Dover, 1981.

Good introduction to the simpler cons.

**REYNARD's** children's series *Secret Code Breaker*. <http://codebrkr.infopages.net>  
(Reviews of books and software are a regular feature in *The Cryptogram*.)

### **Specialty Publisher**

The Aegean Park Press, P.O. Box 2120, Walnut Creek, CA 94595

Website: <http://www.aegeanparkpress.com> has an extensive list of publications in the field of cryptanalysis. Included are reprints of famous works, and modern contributions.

### **Specialty Journals**

*Cryptologia*, a quarterly journal devoted to Cryptography, is published at *Cryptologia*, Department of Mathematical Sciences, United States Military Academy, West Point NY 10996 USA. <http://www.dean.usma.edu/math/pubs/cryptologia/>

*The ENIGMA* is the monthly magazine of the National Puzzlers' League. <http://www.puzzlers.org>

### **ACA Publications**

In addition to *The Cryptogram*, the ACA publishes various booklets of special interest to members:

**Solving Simple Substitution Ciphers** - by Frances A. Harris (**S. TUCK**).

An introduction to Aristocrats, Patristocrats, and Xenocrypt substitution! Mono-alphabetic substitutions are covered in thorough detail, from the Caesar substitution, through the first principles to the use of pattern words. The text includes statistics for French, German and Italian. 42pp, 9x6. (1959)

**Practical Cryptanalysis** - five volumes by W. M. Bowers (**ZEMBIE**) and William G. Bryan (**B. NATURAL**)

This series was intended as a follow-up for *Elementary Cryptanalysis* published in 1939, to bring the cryptanalytic methods up to date and to include additional ciphers not found in the earlier book. The treatment and examples are particularly matched to the ciphers found in *The Cryptogram*. (1967). Each volume is 9x6.

**Volume 1 - Digraphic Substitution.** Playfair and Four Square ciphers are dealt with at length, starting with identification and peculiarities and leading into sample problems and solutions. The Seriated Playfair is explained, and a test for the period demonstrated. (46 pp.).

**Volume 2 - The Bifid Cipher.** A description of the cipher and how to encipher it is followed by the Three Square Technique, finding the period, and solving the Three Squares. The peculiarities of the Even Period lead into Conjugated Matrix Bifids, and the continuous encipherment cycle. (48 pp.)

**Volume 3 - The Trifid Cipher.** A brief biography of the mysterious F. Delastelle, the inventor of both the Bifid and the Trifid ciphers, is followed by a description of the cipher and its peculiarities, keyword recovery, "naturals", locating tips, use of patterns and repeats, etc. (54 pp.)

**Volume 4 - Substitution and Transposition Ciphers.** This covers 22 of the "Cipher Exchange" ciphers not discussed in the other volumes in this series. A must for anyone attempting these ciphers, the booklet gives a brief description of each cipher and a worked analysis of the solution. (45 pp.)

**Volume 5 - Periodic Ciphers: Miscellaneous.** This volume discusses the general problem of finding the period, and then deals in detail with the Vigenères, Portax and Nihilist Substitution. A digression on alphabet recovery is followed by Quagmires, Auto -, Running -, and Interrupted-Key ciphers, the Tri-Square, Fractionated Morse, Seriated Playfair, and Homophonic ciphers, 17 in all. (45 pp.)

**3 Ways to Solve Cryptograms** - This booklet consists of three sections each by a different author: "Cryptometry Simplified", by Henry C. Wiltbank (**NYPHO**); "The Graphic Position Chart", by Lewis S. Sutcliff (**RED E. ERASER**); "The Care and Feeding of Cryptograms", by Lisle J. Maxson (**FLUKE**). All are aimed at the beginner cryptanalyst tackling substitution ciphers (Aristocrats and Patristocrats).

The first section describes how to make a Contact Chart, and how to interpret it. The second shows what may be learned by noting the relative positions of letters, which start words and which end words, and so forth. The last section suggests vowel and consonant hunting as a fast means to a solution and includes hints on those Special Cases designed to trip up unwary solvers.

Published in 1963, but still very valid. (14 pp., 11x8)

**An Approach to Cryptarithms** - by Frederick D. Lynch (**FIDDLE**), introduces the reader to the subject with some fundamentals of notation, and a description of keyed and unkeyed cryptarithms. The Negation Square is introduced as a means of keeping track of which numbers are known and which are not. Theorems of Triplication in Threes, Casting Out Nines, etc. and 28 "short-cut" theorems follow. The book finishes with discussions on Double Key Cryptarithms, The Duodecimals, and some tables of higher-base numbers. Although this is an older publication, a great deal of fundamental information is packed into its pages. (24 pp., 9x6)

**Solving Cryptarithms**- This 28 page booklet by Jack Winter (**CROTALUS**) was published in 1984 and is an expansion of his series of articles in *The Cryptogram* JF73-JF74. It explains notation, analyses a classical Cryptarithm, discusses Searching for Zeroes and Nines, Multiplication, Divisions, Roots and Other Base problems. The use of Multiplicative Structures is given in detail. The author shows how brute force methods can be used for "toughies". The book concludes with some useful Appendices, including how to compute square and cube roots, and Tables of Decimal, Undecimal and Duodecimal functions. (28 pp., 9x6)

**Novice Notes** - by Gerhard D Linz (**LEDGE**) covers many of the ciphers found in the Cipher Exchange, higher numbered Xenocrypts, and the Analyst Corner. Each chapter discusses how to set up a particular cipher type and then discusses the solving process. There are ciphers at the end of each chapter for further practice. (148 pp., 11x8.5)

**Xenocrypt Handbook** - compiled and edited by William G. Sutton (**PHOENIX**), this book contains data and articles from a variety of sources. Those Language Data Sheets that have appeared in past issues of *The Cryptogram* form the nucleus of the handbook, and are all represented along with pertinent articles. Aids to construction and guidelines are also included, as are aids to solving with specific examples for a few cryptograms in common languages. You will also find help and statistics for the determination of cryptograms in unknown languages. (96 pp., various sizes)

**Manual For Cryptanalysis of the Columnar Double Transposition Cipher (A Study of Cryptanalysis)** - Joseph B. Courville (**GUNG HO**) In World War II double incomplete columnar transposition was used by several governments. Although it was sometimes solved by the "general transposition attack" which required multiple anagramming of ciphers in the same key and of the same length, these were not always available to the analyst. **GUNG HO's** course teaches a pencil-and-paper attack on the more general case, including ciphers whose lengths are close but not identical. (91 pp., 11x8)

For current prices, new additions, and other FOR SALE items, please refer to a current issue of *The Cryptogram*.

#### **ACA Website**

The website for the ACA is <http://www.cryptogram.org>. Information about the ACA: dues, errata from cons in *Cm*, information about ACA events, information about events that may be of interest to members, resources that have been posted, etc., can be found on the website.