# COMPUTER CRYPTOLOGY

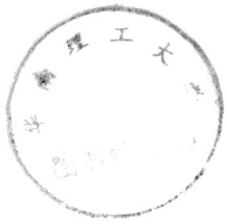
## BEYOND DECODER RINGS

KARL ANDREASSEN

# COMPUTER CRYPTOLOGY

## Beyond Decoder Rings

KARL ANDREASSEN




PRENTICE-HALL, INC.
Englewood Cliffs, New Jersey 07632

*Library of Congress Cataloging-in-Publication Data*
Boyd, Waldo T.
Computer cryptology.

Bibliography: p.
Includes index.
1. Cryptography—Data processing. 2. Ciphers—Data processing. I. Title.
Z103.B65 1988 652'.8'0285 87-1238
ISBN 0-13-166133-7

Editorial/production supervision and
interior design: Kathryn Gollin Marshak
Cover design: Photo Plus Art
Manufacturing buyer: S. Gordon Osbourne



Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

ISBN 0-13-166133-7 025

PRENTICE-HALL INTERNATIONAL (UK) LIMITED, *London*
PRENTICE-HALL OF AUSTRALIA PTY. LIMITED, *Sydney*
PRENTICE-HALL CANADA INC., *Toronto*
PRENTICE-HALL HISPANOAMERICANA, S. A., *Mexico*
PRENTICE-HALL OF INDIA PRIVATE LIMITED, *New Delhi*
PRENTICE-HALL OF JAPAN, INC., *Tokyo*
PRENTICE-HALL OF SOUTHEAST ASIA PTE. LTD., *Singapore*
EDITORA PRENTICE-HALL DO BRASIL, LTDA., *Rio de Janeiro*

A universal language shall be adopted and be taught by all the schools and institutions of the world. A committee appointed by national bodies of learning shall select a suitable language to be used as a medium of international communication. All must acquire it. This is one of the great factors in the unification of man.

*–Abdu'l Baha'*

*I dedicate this work of years to Petra Steinhauser, a* grande dame *of aristocratic bearing, 103 years young and with the wisdom to encourage in practical ways, and of whose mien I am reminded as I tussle with each ciphertext in that tradition.*

# PREFACE

This book is an introduction to cryptology for the microcomputer user. We put the microcomputer to doing the routine scratch-paper work while the mind-initiated, finger-following creative activity is transferred from the pen and pencil to the keyboard, a welcome transition for the many who are thoroughly familiar with the man–machine meld that can occur in keyboarding. Such meld may not come easily for persons who still "hunt-and-peck" the keyboard, since much attention must be allocated to striking the correct keys. However, even those not yet converted to touch-keyboarding will gain considerable advantage over pencil and paper for cryptology work.

Only a cursory introduction to cryptology itself can be offered within the scope of this volume. A number of books detailing the art and science of cryptography and cryptology are referred to in the bibliography, and certainly these are recommended reading for anyone who has more than a dollop of interest in this most fascinating field of professional and hobby occupation. This book should prove a pleasant and intriguing step into a brand-new computer activity, a chance to put not only the larger 64- to 256-kilobyte Central Processing Unit (CPU) to good use, but the 8- to 16-kilobyte "little" micro as well. Likewise, it is assumed that the reader has some knowledge of computer BASIC, and how to use it. Hundreds of books exist on this subject, so only crypto-relevant programming suggestions are given.

The world of the computer has opened up all too suddenly, and not all of this world is wrapped in blessings. While extensive use of computers is not entirely new in the business and industrial worlds, as banks and other financial institutions increase their computer workload, unlawful attempts to transfer funds with the illicit touch of a key will multiply. Why use a gun to rob a bank, with all the attendant hoopla, inevitable telltale photographs, and chance of instant death, when one can sit quietly at home and surreptitiously transfer a block of the bank's funds to a dummy account? Combatting this kind of theft calls for a working knowledge of cryptology by bankers, insurance employees, stockbrokers, grocery managers, and university computer-science professors, to name but a few. Thus, cryptology not only offers the promise of an absorbing hobby, but also unfolds a practical possibility of a career.

This book paves the way to understanding how to manipulate data in a way not even guessed at by the general public, as these pages present but the opening of a box with many, many compartments. Just as there are an infinite number of moves toward Mate! in a game of chess, in the "game" of cryptology there is the pitting of your strategy and tactics against those of other agile minds, and no finite end to the possibilities presented.

After the introductory chapters, which ease the reader into the art of cryptology itself as well as its enhancement by computer, later chapters are built around a menu-selected, interlocked series of programs in the high-level computer language known as BASIC. BASIC has become the Interlingua of computers. It is adaptable from one computer to another, however closely written to a particular brand. BASIC runs more slowly than assembler-installed machine language but the object here is to get started, and to learn to write your own crypto programs. The luxuries of Star Trek speed can be acquired later. While pseudocode is catching on as an excellent Interlingua for printed programs, so far relatively few persons are adept at interpreting it, while the majority is most conversant in BASIC, so again we have held the line at BASIC.

There are, as intimated above, as many variations of BASIC as there are computer brand names. In the main these dialects are superficial and can be understood and adapted with a modicum of effort. The programs herein were written on a TANDY Model 12 microcomputer, which uses the TRSDOS version of BASIC. The program lines have been generously annotated to afford understanding of the functions involved, the better to translate to your own micro's version of BASIC.

Once you understand the function of a line or lines, it is easy to make the few changes necessary to get the program to run on your computer, regardless of manufacturer. For instance, the programs herein use a slash-mark between the filename and its extension: FILENAME/EXT. Your computer's version of BASIC may use a period: FILENAME.EXT. What could be easier

than exchanging the slash for a period, using your BASIC EDIT function? Enter the program as written into your computer, try a RUN, and, at each error advice, make appropriate changes.

Once the individual programs have been entered and debugged, the reader may feel free to adapt, change, replace, or otherwise tailor improvements to his personal needs, within the scope and range of his understanding. Only if someone were to copy and distribute these programs for commercial purposes would the author and publisher become somewhat actively unhappy.

Many readers will invest the time and energy necessary to enter the programs from the printed page into their keyboards; it is the best way to acquire both practice in programming and a thorough understanding of how each program works. For others not so inclined, alternatives are provided.

Alternative programs are available from the author, on eight-inch disks that "play" on Tandy (Radio Shack) Models II, 12/16, and from Wesley Horton, for a number of the popular computers using 5¼-inch disks (see Appendix A).

If you have at least 32 kilobytes of RAM at your disposal, you can use the programs as written; if you have not yet upgraded your little 16-kilobyte micro, it may be necessary to leave off the annotations as you enter the longer programs. This entails dropping the logo headings, explanations of the program, and the portions of lines beginning with '==, the latter being my personalized visual key to REMarks identifying the action, function, and purpose of the lines. Line REM's are quite handy for those who wish to understand the action and make changes in some of the programs, adapting them to a specific computer BASIC, but they are not necessary for anyone who intends to use the program lines exactly as written.

The Tandy Model 12 on which these programs were written has an 8Ø-character screen line. Computers with shorter lines will require modifications of the program PRINT lines. Likewise, each LPRINT (line printer instruction) line should be tailored to your printer peculiarities.

The programs exercise the disk file as the memory for all programs not being used at any given moment, to maximize working RAM (Random Access Memory). Selection of a MENU item automatically RUNs the selected program from file, and, when you have completed work with that particular program, it automatically recalls the MENU. Of course, if you are using cassette tape, the appropriate RUN lines will have to be changed to accommodate the tape drive instead of disk storage. Those using tape storage may find it more convenient to CSAVE each program on a separate cassette, delete the automatic call feature, and call each program by keyboard.

The programs are not elaborate, and only a few of the moderately advanced types of crypto encipherments are covered. Transposition types are

only given one chapter, not because they are considered too advanced for the reader, but because they comprise a separate genre for computer work that deserves extensive coverage on their own merit, along with the many possibilities for closed communication featuring concealment ciphers, for which the computer is well adapted. The aim is to provide the reader with an enjoyable and instructive beginning in hitching the computer to a fascinating and challenging activity.

*Karl Andreassen*

# COMPUTER CRYPTOLOGY

# CONTENTS

# LIST OF PROGRAMS

# INTRODUCTION

Amateur cryptology is enjoying a resurgence of interest due in no small part to the recent and growing phenomenon of personal and small-business computer purchases. Following publication, over a century and a half ago, of "The Gold-Bug," an adventure story about pirates and about buried treasure and a cryptic message concealing its location, cryptology slipped out of its traditional "black room" among nations. "The Gold-Bug" was republished a few decades later and once again fired the imagination of thousands in youthful America, awakening the gaming instincts of enthusiastic afficionados. Magazines devoted to the subject appeared on newsstands. Books were published detailing the then-known methods of secreting the true meaning of a message within an apparently hopeless garble of nonsense words, and offering various approaches to solutions.

Those were the days of Western Union telegrams, and the living-room radio. Television and arcade games on computer screens were decades in the future. It was a time of increasing popularity for hobbies, among them the crossword puzzle and the anagram, and for tracing lines by the numbers to form pictures. *Cryptology,* the technique of concealing the true meaning of a message, and of restoring the mix of letters to a comprehensible whole, carried a popular fascination and challenge within its art and science.

In later years, television came upon the scene, and became a window on the world. Travel gained in popularity and sports gained in attendance. Automobiles were so inexpensive that everyone could own not only one, but two

or three. The former attraction of word and letter games lost out to the sights and sounds of near and far, of new-found freedom for adventure. Magazines with a devoted following of amateur "cipherers" disappeared from the news racks, although crossword-puzzle magazines continued to carry a few cryptograms. Newspaper columns that once carried cryptograms were reduced to carrying anagrams and word-find puzzles.

Despite a decline in popularity in those early years, cryptology has never entirely disappeared from the popular scene. Its activities continue in the "little magazines," and in not-for-profit publications by loyal remnants of that multitude to whom it had appealed.

Popular appetites wax and wane in unpredictable cycles. The Henry Fords of the microcomputer, Apple and Radio Shack, changed the daily lives of young and old alike with the introduction to the marketplace of two ready-to-use, inexpensive computers, the "Apple" and the Radio Shack TRS-8Ø Model I. As popularity goes, they were a sellout. These new toys put the almost magic but hopelessly expensive "mainframe" computer within the reach of everyone. Not unlike the early Model "T" Ford cars, which could be had in any color desired as long as the customer would settle for black, the TRS-8Ø Model I could be had in any color the buyer desired, as long as it was Tandy grey. And akin to the heightened sense of power conferred on the individual behind the wheel of a car, the "power" of the computer to expand consciousness was put into the hands of anyone and everyone by these fascinating gadgets. Computers became known for their ease of handling game programs as well as for quasi-practical but popular checkbook balancing. It wasn't long before a hundred different companies were making a bid for some of the avalanche of sales in this brand-new consumer craze.

During the pre-microcomputer period, business and industry became aware of the time and labor savings that could be gained from use of the computer, but because of the battleship size of "mainframe" computers then available only the largest corporations could afford them. A system of "time sharing" the huge, expensive installations was devised, and smaller companies began to take advantage of computer labor-saving potentialities. Personal computers were a solution awaiting recognition by business and industry for two to three years following their release to the mass market, but, finally, small businesses became big business among computer manufacturers, and models were designed especially for that market.

Personal computers gained popularity so explosively because they are really infinite household appliances. If you buy a typewriter, there is only one thing you can do with it: type on a piece of paper. If you buy a computer, typing (word processing) is but one of thousands of things you do with it. A toaster will toast bread, pop-ups or muffins, but that's about the end of the list. A vacuum cleaner may dust furniture, drapes, and the family auto besides its primary carpet-cleaning application, but, like a newborn

baby, a computer purchase opens up a horn of plenty, an infinite cornucopia of show and tell beyond the expectations of manufacturer and consumer alike. Hobby computers were at first widely used for games as the new owners tried out their wings—primarily games of the blast-em-out-of-the-sky star-wars type. This heyday soon passed, although there remains a hard-core coterie of players both at home and in the arcades. There is an increasing interest in cerebral applications of computer software that tax the skill and imagination of the player, and, of this type, none can surpass the challenge of cryptology.

The larger of the microcomputers aimed at the business office, and their owners were soon exposed to a surprising list of liabilities. The data stored in their memories, hard disks, and tapes were vulnerable to "white-collar" crime, ranging from surreptitious publicizing of personnel files to extremely-difficult-to-detect transfer of funds from corporate to personal accounts. Malicious mischief, such as scrambling files, could cause even greater dollar losses in downtime for the company. An answer to these problems was at hand: cryptology. Consulting companies specializing in computer security sprang into being, and the computer files of most forward-looking companies are now encrypted. Consultants are generally college-trained experts who "graduate" from the ranks of the crypto hobbyist.

Among the reasons for the mid-century drop in interest in hobby cryptology was the inescapable need for pages and pages of routine drudge work as promising approaches to solutions of cryptograms were tried. One had to count letter repetitions letter by letter, and to match adjoining letters in order to construct tables of most-used letter combinations, such as digrams and trigrams. The message under analysis had to be written and rewritten numerous times. These are precisely the kind of tasks that the computer is designed to do quickly and without error. At the touch of a key, what would take an hour to perform with pencil and paper consumes only seconds, or even only fractions of a second, on the personal computer. The advantages of this increase in speed go far beyond simple replacement of finger work, as both positive and negative feedback play a delicate, important part in the cryptanalytic process.

"Ah, if only I had one of those crypto machines," came to be a fantasy wish of amateur cryptanalysts who read about the history-making cipher machines used during wartime. Breakfast-cereal boxes sometimes carried simple ones, hardly worthy of the name "machine," stamped from tin and painted with one whoosh of an air brush. Ovaltine, a milk-additive food supplement, sponsored a long-running series of radio programs that featured "secret" decoding pins and badges. The *Captain Midnight, Red Ryder, Dick Tracy, Tom Corbett,* and *Tom Mix* shows all featured crypto gadgets. Not to be outdone, the *Lone Ranger, Don Winslow,* and *Space Patrol* programs likewise featured their share of crypto marvels for youth and young adults. Comic books got into the act and offered various and sundry deciphering