CRYPTOLOGIA October 1993 Volume XVII Number 4

REVIEWS AND THINGS CRYPTOLOGIC

Louis Kruh

ADDRESS: 17 Alfred Road West, Merrick NY 11566 USA.

SOTHEBY CATALOG FEATURES RARE CRYPTO BOOK

Fine Books and Manuscripts, New York, June 14 and 15, 1993. Auction catalogue 6438. Sotheby's, 1334 York Ave., New York, NY 10021 USA. 1993. 270 pp. $34.00; $41.00 overseas.

A gorgeous catalogue on fine glossy paper with more than 100 photographs, many in full color, of exceptional books, historical bindings, rare early printing, autographed letters and well known authors.

For aficionados of cryptology, the auction is notable for its sale of the first printed book on the subject, *Polygraphiae libri sex* by Johannes Tritheimius, which was published in 1518. The catalogue features a photograph of the book's woodcut title page and a lengthy description and background of the copy in the auction. A brief excerpt follows.

> FIRST EDITION, complete with both parts: the first printed book on CIPHERS AND CRYPTOGRAPHY. Tritheim's treatise, dedicated as a manuscript to Emperor Maximilian I in 1508, was published posthumously: he died 13 December 1516. The preliminaries include a BIBLIOGRAPHY OF TRITHEIM'S WRITINGS, compiled by his disciple Joannes Duraclusius. The two parts, *Polygraphia* and *Clavis polygraphiae*, though having separate titlepages, colophons, and signatures, form a single work, with a quire register for both parts printed on the last leaf of the latter. Many special characters were cut for this edition to show different writing systems, including Tironian notes, the ancient mode of shorthand which was forgotten for centuries until Tritheim revived its study.

Presale estimate for the book was $2,000-3,000; it was sold for $3,500. The book was offered for sale by David Shulman, a noted bibliophile, longtime col-

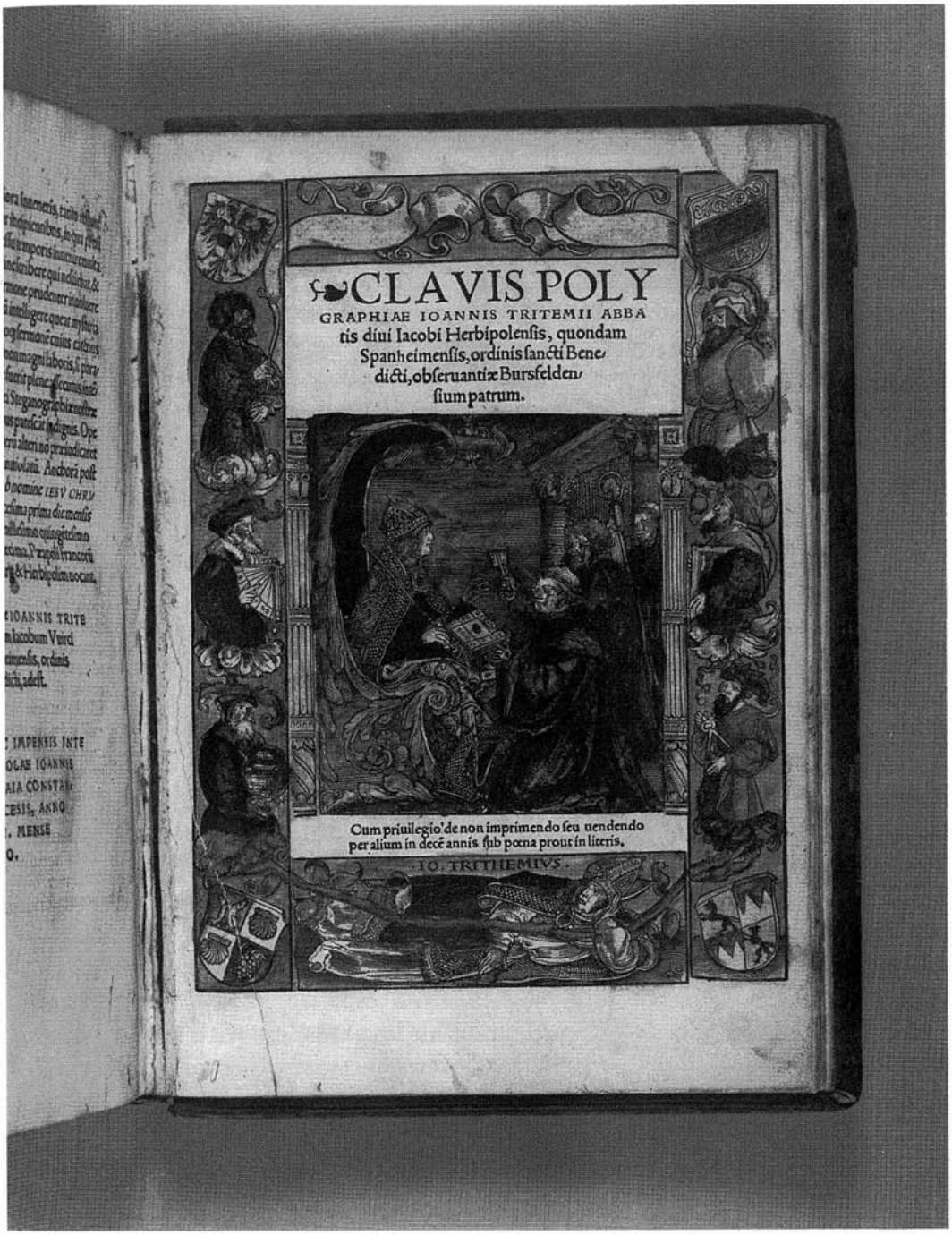

Photo credit Sotheby's.

lector of books on cryptology and author of *An Annotated Bibliography of Cryptography* (New York: Garland Publishing, Inc., 1976).

Several years ago, Shulman donated another copy of *Polygraphia libri sex* with his collection of more than 500 cryptologic books, considered one of the finest private collections in the world, to the New York Public Library (NYPL). He is donating part of the proceeds from this sale to the NYPL to assist with the cataloguing of the collection.

Sotheby's illustrated catalogues are published for all regularly scheduled auctions and may be purchased singly or by subscription. A subscription Newsletter, published nine times a year, provides an advance calendar of all Sotheby's sales worldwide and full color photographs of auction highlights. A brochure describing both publications is available from Sotheby's Subscription Department, P. O. Box 5111, Norwalk CT 06856 USA.

See opposite page for plate from text.

CRYPTIC POEM IN MYSTERY

Dexter, Colin. *The Way Through The Woods*. Crown Publishers, Inc., 201 E. 50th Street, New York NY 10022 USA. 1992. 296 pp. $20.00.

British author Colin Dexter has won numerous awards for his crime novels that feature Chief Inspector Morse, a heavy drinking, introverted and intuitive detective. This latest book has already been named best mystery novel of the year in England.

A young Swedish girl disappears near Oxford and Morse insists she was murdered. But there is no corpse. A year later, an anonymous letter is sent to Thames Valley Police Headquarters. It contains a cryptic poem that the writer says is the key to the mystery. Unable to unravel its message, the police ask the help of the literary correspondent of *The London Times*. After publication in the newspaper, the public responds with analyses and deciphering methods.

The plot has puzzles within puzzles, from esoteric poetry to anagrams to crosswords, and Morse does not disappoint his loyal readers with his investigatory methods and detection techniques. But even the most observant reader will be surprised by the twists and turns in the plot as its solution is revealed.

POSTAL STAMP COMMEMORATES CRYPTO HISTORY

In 1991, the U.S. Postal Service issued the first in a series of five annual World War II 50th anniversary commemorative stamp sheets with ten different 29-cent stamps.

FIRST DAY OF ISSUE

Photo credit Fleetwood, Cheyenne WY.

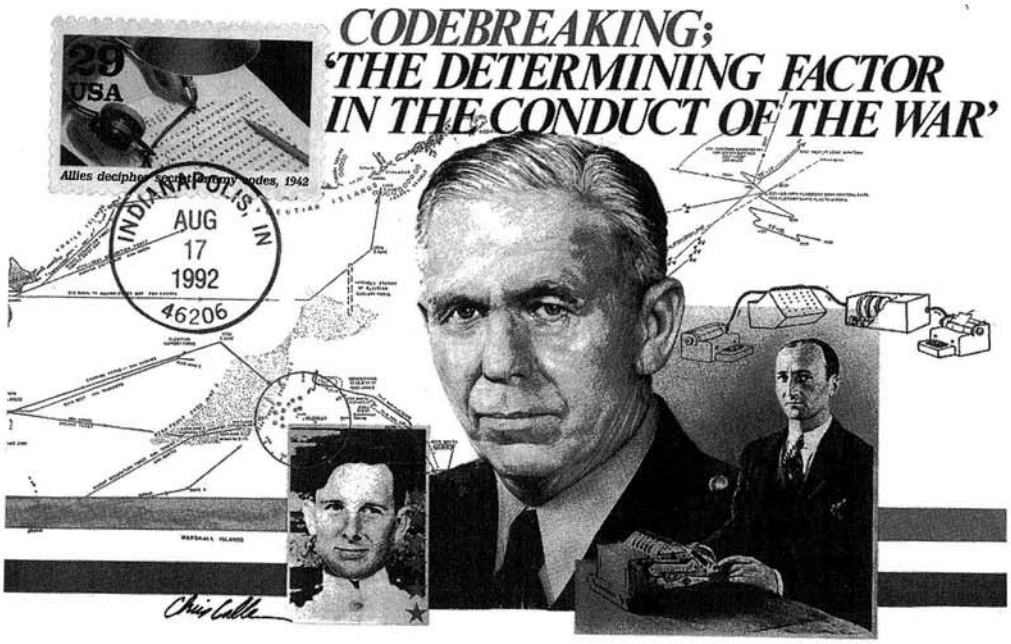

Photo credit Fleetwood, Cheyenne WY.

The second set issued August 17, 1992, is titled "1942: Into the Battle." Among its ten stamps is one that carries the caption, "Allies decipher secret enemy codes, 1942." It shows headphones, a pencil and an enciphered message.

A special First Day Cover (envelope) and cachet, and First Day Postcard and cachet have been created by Fleetwood, a division of Unicover Corporation. (See opposite page.) The Cover, with its cancelled "enemy codes" stamp, is postmarked first day of issue. Its cachet, headlined "Codebreaking: Turning The Tide in the Pacific," features color illustrations of Admiral Chester W. Nimitz, Commander in Chief of the Pacific Fleet and Captain Joseph J. Rochefort, head of the Combat Intelligence Unit in Hawaii.

The First Day Postcard also has a cancelled "enemy codes" stamp and its cachet, headlined "Codebreaking: 'The Determining Factor in the Conduct of the War.' " features General George C. Marshall, Army Chief of Staff, Captain Rochefort, and William F. Friedman with a Hebern cipher machine.

The "enemy codes" Cover is available from Fleetwood, One Unicover Center, Cheyenne WY 82008-0001 USA, as part of its 1992 WW II commemorative First Day Cover set. This includes individual covers and cachets for each of the ten 1992 WW II commemorative stamps issued to commemorate the anniversary. The Cover set (stock number 570273) is $32.00 plus $4.50 for postage, handling and insurance.

The "enemy codes" First Day Postcard (stock number M92-106) is $1.85 plus $2.60 for postage, handling and insurance. First Day Postcards with individual cachets for each of the other WW II commemorative stamps are also available.

CRYPTO REBELS WRITE-UP

Levy, Stephen. "Crypto Rebels." *Wired*. 544 Second Street, San Francisco CA 94107 USA. Volume 1, Number 2 (May/June 1993). 54-61. Subscription, six issues, $19.95; single issue, $4.95.

Wired is a new magazine aimed at the "Digital Generation." The cover story in its second issue examines the growing "Cypherpunk" movement to insure individual privacy.

According to the author, Cypherpunks believe that all information about an individual belongs to that person and opinions, medical records, personal data collected by local, state or national governmental agencies, communications sent by the individual or any other information should be available only if the person involved chooses to reveal it. And the means through which this privacy would be maintained is by the widespread use of the virtually unbreakable public-key cryptography.

Opposing forces are U. S. government agencies who seek to insure their ability to read public-key encrypted messages by the continuance of electronic surveillance and by having access to public-key cryptography's secret keys when authorized by a judge.

The author suggests that the government cryptologic monopoly was destroyed in 1975 when Whitfield Diffie created public-key cryptography. His later work with Martin Hellman is recounted along with the implementation of the Diffie-Hellman system by three MIT computer scientists who founded RSA Data Security to market their patented algorithms.

Phil Zimmerman, a political activist, wrote, "if privacy is outlawed, only outlaws will have privacy" and he developed a cryptosystem, PGP (Pretty Good Privacy) for use on PCs. Zimmerman, concerned that the use of cryptography may someday be prohibited by the government, wanted his software distributed quickly. His method was to put it on computer bulletin board systems and on Internet where anyone could download it free of charge. RSA has claimed that PGP includes its patented algorithms.

A well known figure in academic crypto circles, Georgetown Professor Dorothy Denning, counters Cypherpunk beliefs by pointing out that "Organized Crime leaders, drug dealers, terrorists, and other criminals could conspire and act with impunity" if electronic surveillance was illegal and authorized agencies did not have access to private keys used in public-key cryptography.

The article explores many views and contains a great deal of fascinating information.

HISTORY OF WRITING

Gaur, Albertine.*A History of Writing*. Cross River Press, 488 Madison Ave., New York NY 10022 USA. Revised edition. 1992. 236 pp. $35.00.

The story of writing is a tale of adventure that spans some twenty thousand years and touches all aspects of human life. But with major advances in computer technology during the past 25 years, the preservation and dissemination of knowledge no longer depends on the actual process of writing. Therefore, in a departure from other histories of writing, the author approaches the subject from the late 20th-century concept of information storage and retrieval, to examine the interaction between society and writing and to introduce the subject to a wider and more general audience. In essence, it is a history of the entire apparatus by which human speech or ideas have been rendered into visible form; pictographic, syllabic, or alphabetic. Gaur traces chronologically and geograph-

ically all the major scripts that have contributed to writing's development in a highly readable and informative way.

The book is divided into five main sections. I. "Origin and development of writing." II. "The Main Groups: their characteristics, history and development." The last chapter in this section, "Invented Scripts" is a fascinating review of many instances where the names of kings, rulers, statesmen, writers, reformers, Buddhist monks and Christian saints are associated with the invention of certain scripts. It leads into III. "Decipherments," which has two chapters. "The Scholars and Their Work," covers the decipherment of Egyptian hieroglyphics and the cuneiform script. The second part, "Undeciphered Scripts" describes work still to be done on scripts of ancient Crete, Maya glyphs and the Indus script. The final two sections are, IV. "Social attitudes to writing and literacy," which includes a brief discussion of cryptography, and V. "Moves towards the future," which describes the use of computers and their deleterious effect on writing.

This large (8" × 10") impressive book printed on glossy stock has more than 100 remarkable photographs of manuscripts, inscriptions on ancient pottery, seals and sealings, tablets, unique languages, uncommon examples of writing and other unusual items. A dictionary of more than 200 scripts at the end of the book, which ranges from Abyssinian to Yunnan, provides a comprehensive reference list of the most important scripts, with examples and pertinent information for each one.

SHAKESPEARE AUTHORSHIP UPDATE

Uncovering Shakespeare: An Update. A Provocative Look at the Shakespeare Authorship Question. Three-hour videotape on two VHS cassettes edited from a live videoconference, plus 20-page book of readings from both sides of the issue. GTE Service Corporation, GTE VisNet, One Stamford Forum, Stamford CT 06904 USA. 1992. $180.00 plus $6.00 postage and handling.

For more than 200 years questions have been raised about the authorship of the plays and sonnets attributed to William Shakespeare. During this period some 50 names have been suggested as the person who really wrote the plays including Queen Elizabeth. For most of those years leading contenders have been Sir Francis Bacon and Christopher Marlowe, with Bacon the dominant figure. He is probably the favorite choice of cryptologists because Bacon supposedly concealed his name in a cipher in many of the Shakespearean works. His supporters probably reached their peak around the beginning of the 20th century.

In 1920, a new entry was proposed by an English school teacher, J. Thomas Looney. His choice was Edward de Vere, Earl of Oxford. Presently, De Vere seems to have replaced other candidates, including Bacon, as the favorite. (Before leaving Bacon, however, it should be noted that Bacon still has his advocates. A strong and eloquent one is a retired attorney from Omaha, Nebraska, Penn Leary, whose 1990 book, *The Second. Cryptographic. Shake-speare* (see review, *Cryptologia*, 14(4): 371) is a lively and well written presentation of his research and reasons for supporting Bacon. He recently distributed a computer disk containing a summary of his arguments and evidence, and programs he has written for decrypting Shakespearean text to uncover Bacon's name.)

On September 17, 1992, the first national telecast of an interactive seminar explored the question of whether Shakespeare or the Earl of Oxford was the true author of the Shakespearean works. The live videoconference, moderated by William Buckley, featured an international panel of leading Shakespearean authors, lecturers and scholars plus experts in the theater and Elizabethan politics.

The panel provided a provocative and interesting discussion by Oxfordian proponents and Stratfordian advocates with a lively give and take on the evidence cited to support each view. The format included call-in questions from various universities that were participating in the seminar from off-site locations. These occasionally opened other avenues of discussion.

Key arguments for de Vere are based on his education, background and position in the royal court of Queen Elizabeth. Virtually all of the Shakespearean plays are placed in royal courts, the world of the nobility or the highest circles of society. There are characters in the plays seemingly based on figures in Queen Elizabeth's court. De Vere had the insider's knowledge needed to write these plays and his supporters point to Shakespeare's lack of education, background or experience to write about royal or aristocratic matters. They also say the politics of the period prevented de Vere from publicly taking credit for the plays which is why he used Shakespeare's name. An important issue raised against his authorship is that he died in 1604 and major Shakespearean plays were written after that date. His advocates claim he wrote them before his death.

New evidence to support de Vere comes from the bible he owned. An examination of his bible took place when it was exhibited at the Folger Shakespeare Library in Washington. It had been annotated by de Vere with over 1,000 marked passages and writing in its margins. Among the hundreds of books that influenced William Shakespeare, the bible was the most important and analyses have isolated Shakespeare's use of the bible from those of other Elizabethan writers. The analysis shows a relationship between the sections highlighted in de Vere's bible and Shakespeare's use of the bible in his plays.

Cryptology plays a very minor and perhaps flawed role. There is a reference to sonnet 76 which includes the phrase "Every word doth almost tell my name" and the suggestion that "every word" is an anagram for Edward de Vere. Also, the word *vere* means truth and it occurs often.

The program is intellectually stimulating and somewhat frustrating because neither side could produce the "smoking gun" or muster sufficient evidence to decisively crush the other side's arguments. But it is three hours of fascinating entertainment that may lead viewers to seek further reading on the authorship question and perhaps read or reread the plays and sonnets while searching for clues to the author.

BRITISH ARMY SIGNALS IN WORLD WAR I

Ferris, John, ed. *The British Army and Signals Intelligence During the First World War*. Alan Sutton Publishing Inc. Wolfeboro Falls, NH 03896-0848 USA. 1992. 359 pp. $60.00.

According to the author, "a careful search of the papers of several British departments of state, of associated military forces and of British and allied officers ... leads to a startling conclusion. Signals intelligence affected the British Army during the First World War no less than in the Second."

In this unique book, Ferris, after an introductory overview, provides documents, Army reports, memoranda, and other uncommon items related to eight signals intelligence subjects. These are: "Field Telephones and Telegraphs: Intelligence and Security"; "Traffic Analysis"; "Aircraft Intelligence"; "Signals Security and Cryptography"; "Signals and Operational Deception"; "Codebreaking: Organisation"; "Codebreaking: Techniques"; and "Codebreaking in the Middle East." A chapter is devoted to each topic and Ferris begins each one with a review of the documents it contains.

In Signals Security and Cryptography, the material shows how difficult it is to maintain proper cryptographic security; the discovery that Britain's standard field cipher, the Playfair, was vulnerable; and that the failure of British cryptography during 1917 and 1918 was due to insufficient communications between cryptographers and cryptanalysts. Also included is a translation of a German document on cryptographic security which demonstrates a superior approach to the subject. Subsequent events, however, indicated they were not much more effective.

Two lengthy and highly informative papers constitute the section on Codebreaking Techniques. The first, "Memorandum on Code Breaking Techniques in the Middle East, 1917," details British methods for attacking enemy ciphers.

While other systems are briefly discussed, the paper concentrates on solving double transposition ciphers, which were considered highly sophisticated ciphers at that time. The other paper, "Enemy Codes and Their Solution," is described as one of the best sources known to exist about the techniques of codebreaking. Its fifty-five pages with nine appendices shows the methods used to solve codes used by German Field Wireless Stations.

The author has assembled a marvelous collection of official documents not often seen or discussed and, as a result, almost every chapter offers fascinating reading and revelations. Extensive notes, a bibliographical essay and an index also help to make the book a valuable reference for further research and reading.

CRYPTO BIBLIOGRAPHY

Cryptography and Cryptosystems. (Jan. 1989 - Present). National Technical Information Service, U.S. Dept. of Commerce, 5285 Port Royal Road, Springfield VA 22161 USA. 1993. $65.00.

The National Technical Information Service (NTIS) Published Search program provides an exclusively prepared bibliography with the most current data available on a specific topic from an individual database source. Coverage includes articles in scientific and technical journals, papers presented at conferences, books, reports, and other worldwide sources.

This bibliography contains 250 citations on the theory, design, standards, protocols, and applications of cryptography and cryptosystems. Citations examine cryptographic algorithms, techniques, cipher systems, and keys of various types. A numbered title list and a subject index give users quick access to citations of special interest. In addition to bibliographic data, each citation contains an informative abstract which provides a quick, inexpensive way to determine which items require follow up.

This Published Search done in June, 1993 includes references published as recently as April, 1993. In addition to citations from the U.S., sources include publications from China, Netherlands, Japan, Germany, Korea, United Kingdom, and other countries.

The NTIS Published Search program covers hundreds of different subjects in almost every discipline. A complete listing of titles is in the NTIS Published Search catalog available from NTIS.

THE UNCENSORED TRUTH

Poundstone, William. *Biggest Secrets: More Uncensored Truth About All Sorts of Stuff You Are Never Supposed to Know*. William Morrow & Co., Inc., 1350 Ave. of the Americas, New York NY 10019 USA. 1993. 272 pp. $20.00.

An unusual book that reveals the diverse and sometimes tabloid-type secrets of celebrities, business, government, and the media. Based on original research, the author exposes the true ages of famous people, secret formulas of various products, how Jerry Lewis stays awake for his annual telethon, what "Code Red 123" means in a hospital, how award shows keep the winners secret, the true identity of Trevanian, the best selling author of spy thrillers, explanations of famous magical tricks, subliminal messages in Saturday morning cartoons, backwards messages on records, and much, much more.

In a chapter, "Codes and Texts," Poundstone reveals codes used in hospitals, airlines, and retail stores; the use of verification codes on lottery tickets; the meaning of graffiti; and hidden pictures in various media, including U.S. currency. A sizeable section is devoted to the Beale cipher but the secret hiding place of the treasure it supposedly conceals is not disclosed. Poundstone cites this writer's use of stylometry to demonstrate the story is a hoax. He also provides further stylometric research that leads to a similar conclusion.

The book is not only enjoyable and informative, it provides a variety of interesting tidbits to enliven your next conversation.

HIEROGLYPHS - HERE'S LOOKING AT YOU

Watterson, Barbara. *Introducing Egyptian Hieroglyphs*. Scottish Academic Press, 56 Hanover Street, Edinburgh EH2 2DX, ENGLAND. 1993. 152 pp. $15.00.

This informative book is divided into two sections. Part I explains the principles of picture and alphabetic systems of writing; how writing began in Mesopotamia and how hieroglyphic writing developed in ancient Egypt from earliest times until the 5th century A. D., when all understanding of it had been lost. The rediscovery of ancient Egypt, which began with Napoleon's expedition to Egypt in 1798, is recounted along with the first successful decipherment of hieroglyphs by Jean François Champollian in 1822.

The objective of the second section is to provide readers with enough basic grammar and vocabulary to translate simple Middle Egyptian texts and inscrip-

tions. There are eleven lessons, each ending with the lesson's vocabulary and a set of exercises for students to practice what they have learned. Answers to the exercises are at the back of the book with a glossary of all words used in the exercises. This is arranged under two headings – an Egyptian-English vocabulary and an English-Egyptian vocabulary. Also included is a list of the hieroglyphic signs used in the lessons.

Dr. Watterson has written an easily understandable text, which may make learning how to decipher hieroglyphic inscriptions an enjoyable educational project for the family.

DIFFERENTIAL CRYPTANALYSIS

Biham, Eli and Adi Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, 175 Fifth Avenue, New York NY 10010 USA. 1993. 188 pp. $39.00.

The Data Encryption Standard (DES) was developed by IBM and adopted by the U.S. National Bureau of Standards, now the National Institute for Standards and Technology, in the mid-1970's. Since then it has withstood continuous and intensive cryptanalytic attacks by the world's leading cryptologic researchers.

In this book, the authors "develop a new type of cryptanalytic attack which can be successfully applied to many iterated cryptosystems and hash functions." Basically it is a chosen plaintext attack but in certain circumstances "it can also be applied as a known plaintext attack." Their method is called *differential cryptanalysis* "since it analyzes the evolution of differences when two related plaintexts are encrypted under the same key."

After a review of major efforts and techniques to cryptanalyze DES, Biham and Shamir describe the main results accomplished by their own efforts. Successive chapters cover: "Introduction to Differential Cryptanalysis," "Differential Cryptanalysis of DES Variants," "Differential Cryptanalysis of the Full 16-Round DES," "Differential Cryptanalysis of FEAL" (Fast Data Encryption Algorithm), "Differential Cryptanalysis of Other Cryptosystems," "Differential Cryptanalysis of Hash Functions," and "NonDifferential Cryptanalysis of DES with a Small Number of Rounds." Appendices include a technical description of DES and the difference distribution tables of its S boxes.

The state-of-the-art methodology demonstrated by the authors should provide valuable insight to cryptologic researchers enabling them to explore additional ways to test the security of DES and other cryptosystems.

TEACH YOUR COMPUTER TO SPEAK DOLPHIN LANGUAGE

Dolphin Encrypt/Dolphin Encrypt Advanced Version. Dolphin Software, 48 Shattuck Square, Suite 147, Berkeley CA 94704 USA. Basic Dolphin system, $64.00 plus shipping, Dolphin advanced version. $128.00 plus shipping.

Reviewed by Dr. Cipher A. Deavours, Department of Mathematics, Kean College of New Jersey, Union NJ 07083 USA.

As a rule, publishers of PC encryption software make extravagant claims as to the security of their products while maintaining absolute secrecy about how their algorithms work. There is very good reason for all this caution on the part of the product designers — most of the highly lauded encryption schemes that are offered to PC users are distinctly second rate as has been aptly demonstrated in the pages of this journal on several occasions.

It is, then, a breath of fresh air to find a software author who believes in an "open system interface" to users. Peter Meyer, the author of the Dolphin encryption systems, has done a fine job in presenting his product to the marketplace. The two encryption systems, *Dolphin Encrypt* and *Dolphin Encrypt Advanced Version* are both accompanied by clear and easy to follow instruction manuals. Mr. Meyer makes some no nonsense comments about cryptographic security in his manuals and even discloses the C language source code for his system.

Both versions of the Dolphin ciphers are autokeyed block ciphers.The width of the blocks are variable and the plaintext mixing is done under the control of both congruential and linear random bit stream generators. The *diffusion* process employed in the ciphering of data is fairly complex for an inexpensive system such as this one. The DOS command line interface is easy to remember and to use and the advanced version has its own script language (including conditional branching) for automating commonly used sequences of commands. Files are normally compressed during encryption.

The author states that his software will encrypt files at about 4 Kb/sec on a 25Mhz 386SX PC. While this rate is comparable to some other software on the market, I feel that it is excessively slow in a general office environment. The central problem here (which I have seen repeated in many other products) is the use of compiler code written in C. There is simply no way to gain reasonable speed without resorting to assembly language programming — especially if one uses so many random key stream generators. However, since source code is included in the package, a knowledgeable C programmer could easily remedy the speed problem with assembly language subroutines.

Mr. Meyer has stated that one of the criticisms directed at his product resulted from his decision to "introduce a new encryption method which has not already been subjected to exhaustive analysis by professional cryptanalysts and pronounced secure." Considering the rather pathetic state of "professional" cryptanalytic expertise in the public arena, this comment just doesn't hold water. Perhaps Mr. Meyer's algorithm should be examined by the same "professional" crew who were, a short time ago, urging standards organizations to adopt various algorithms that have recently been shown to be dangerously weak. Such professional opinion would be, clearly, not worth the expense of obtaining it.

The Dolphin packages offer good value for the price and are worth acquiring.

SOURCE FOR OUT-OF-PRINT ESPIONAGE BOOKS

Cloak and Dagger Books, 9 Eastman Ave., Bedford NH 03110-6701 USA, calls itself the "World's Largest Dealer in Out-of-Print Espionage Books," which includes related topics such as codes and ciphers. A 53 page catalog listing more than 600 books, a small sample of its inventory, is available.

SPY DEVICES OF THE COLD WAR

Melton, H. Keith. *CIA Special Weapons and Equipment: Spy Devices of the Cold War*. Sterling Publishing Co., Inc., 387 Park Ave. South, New York NY 10016-8810 USA. 1993. 128 pp. $14.95.

This is a fascinating guide to the intriguing espionage devices used by the Central Intelligence Agency during the Cold War. Melton provides a full description and illustration of each piece of intelligence equipment plus purpose of its use and specifications.

The extraordinary collection includes the following categories: personal weapons, photographic equipment, agent communications equipment, audio surveillance, surreptitious entry, incendiaries, firing devices, explosives, automotive attack, harassing agents, and accessories. The latter group includes an amazing "rubber airplane" nearly 20 feet long, with a one-piece wing, tail assembly and cockpit that can be assembled by one person in less than six minutes. It has a speed of 70 mph and a range of 350 miles.

In the secret writing area, there are pictures and descriptions of invisible writing techniques, microdot equipment, one-time pads, burst transmission device, and a combustible notebook for cryptographic material, which can be destroyed instantly by a special incendiary pencil that is inside.

There are miniature cameras, radio receivers, transmitters, surveillance devices and recorders in creative shapes and forms. For example, to reduce the possibility of a signalling device being disturbed after surreptitiously placed near a target, it is designed to resemble what it is named after; a "dog-doo transmitter."

This handsome, large size (8 1/2" × 11") hardbound book brings to life the rarely seen spy devices – cigarette pistol, wristwatch camera, attache case radio station, briefcase recorder, lockpick gun, poison needle, oneman submarine, and dozens of other ingenious items – usually employed by spy-fiction characters.

OPERATION PRIMROSE

Haney, Al. *Operation Primrose ... A Matter of Piracy!* Vantage Press, Inc., 516 W. 34th Street, New York NY 10001 USA. 1992. 263 pp. $16.95.

A factually based historical novel about the World War II intelligence war during the Battle of the Atlantic when German U-boats were sinking more Allied ships than the United States or England could replace. Bletchley Park, at that time, could only read a small percentage of Enigma messages while British codes were being solved by the Germans.

The focus is on attempts to capture German submarines to obtain keys to Enigma ciphers. Three successful attempts are detailed.

The U-110 was forced to the surface by depth charges. Then specially trained boarding parties seized important code and cipher material before gale winds and high waves caused the damaged submarine to plunge to the bottom.

The U-570, supposedly captured by a Royal Air Force bomber, was actually surrendered to the British by its captain without the knowledge of its crew. Aside from benefiting from its valuable cipher material, the British refurbished the Uboat and successfully used it against German submarines.

The U-505 was captured by the U. S. Navy and after the war it was given to the Chicago Museum of Science and Industry where it is still on display.

The capture of a U-boat is not a common occurrence and a defection is very unusual. But, the sequence of events leading to the defection is extraordinary.

In Stockholm. Dr. Mariana Frederickson, the beautiful "daughter of one of Sweden's most noted submarine authorities" is a marine architect, a qualified metallurgist and a "submarine scientist." She is encouraged by Swedish Naval Intelligence to keep informed of technological improvements in submarine warfare for the benefit of Sweden and her U. S. Navy friends. Submarine specialists from various countries including Germany, who are interested in developing more

deadly U-boats, consult with Dr. Frederickson. At a cocktail party she is introduced to a German naval officer and they fall in love. He later becomes Captain of U-570 and agrees to allow his submarine to be captured in return for asylum in the United States where he will be reunited with Mariana.

Haney, a retired army colonel, who was a strategic intelligence officer, keeps the action moving with locales shifting back and forth among Stockholm, Washington, Poland, Bletchley Park (BP), London, Paris, Norway, Lorient and the Atlantic. The invention of the Enigma cipher machine and its subsequent decryption is described by events taking place in The Netherlands, Poland, BP, Washington, and London. Work at BP is frequently noted as events unfold.

It is an exciting WW II adventure concentrating on intelligence, codes and ciphers, and submarine warfare. According to the author, its characters "are based on actual role models" and the main character, apparently Dr. Frederickson, is "a composite of a beautiful SwedishAmerican agent, who is also a submarine expert."

Haney claims the events actually occurred but "the historical novel format permitted the extrapolation of events wherein the full facts have not yet been revealed."

DECODING ANCIENT LANGUAGES

Norman, James. *Ancestral Voices: Decoding Ancient Languages*. Barnes & Noble Books, 120 Fifth Ave., New York NY 10011 USA.1992 reprint of a 1975 book. 242 pp. $9.98.

The art of solving ancient scripts only began during the Renaissance when Europeans became interested in classical Greece, Rome and the Holy Lands. Interest in decipherments heightened in the nineteenth century when Napoleon Bonaparte's brief conquest of Egypt, 1798-1801, focussed attention on its enigmatic monuments and the curious hieroglyphic writing of the Pharaohs.

In addition to explaining how many forgotten languages were deciphered, the author tells about the men who climbed impossible cliffs, traveled across burning deserts or hacked paths through thick forests to uncover mysterious inscriptions or fragments of tablets bearing a word or sentence which, after being pieced together, revealed ancient civilizations.

Norman relates the decipherment of Egyptian hieroglyphic writing, Mesopotamian cuneiform, Minoan Linear B, Mayan pictographs and other ancient languages, including lesser known scripts such as Old Persian and Hittite. The emphasis, however, is on the men who deciphered them: Jean François Champollian, who at age 11 promised himself to read hieroglyphics, Henry Creswicke

Rawlinson climbing the towering rock of Behistun to read its cuneiform inscriptions, John Lloyd Stephens and Frederick Catherwood risking their lives in the jungles of Honduras to uncover ancient Mayan cities. The excitement and frustrations inherent in efforts to decipher the secrets of the past are vividly depicted such as the discovery of cuneiform tablets containing a BabylonianSumerian story of the flood – written 1,000 years before the Old testament version.

The book's coverage is broad but still detailed. It includes maps, many fine photographs of inscriptions, comparative tables, chronology, bibliography and index. It lacks a table of contents and its last chapter dealing with future decipherments has not been updated since written in 1975. But each of the previous seventeen chapters includes historical and etymological background enlivened with biographical data, anecdotes, quotes from diaries and journals and examples of ancient writing, which offset any minor shortcomings – and at a very reasonable price.

DECODING ANCIENT LANGUAGES

Wilson, William J. and C. Larry Craig. *WARLOCK – a New MatrixΘbased Paradigm for Public Key Cryptography.* Floppy disk with: technical paper (WARLOCK4.TXT), C++ source program (WARLOCK4.CPP), BORLAND C++ Project File (WARLOCK4.PRJ), and a PC-based executable program (WARLOCK4.EXE), which implements the paradigm. Datasec Systems, P. O. Box 4152, Huntsville, AL 35815-4152 USA. Free to American and Canadian persons only.

The paper briefly reviews the functionality of contemporary private key and public key (PK) cryptosystems in meeting current and future private sector security needs. To assist in meeting these needs, the WARLOCK paradigm is presented and explained. According to Wilson and Craig, systems such as WARLOCK 4.0 based on this paradigm are designed as alternates to RSA and RSA-hybrid systems by making available single, high-speed, full bandwidth systems capable of the basic cryptographic functions of encryption, decryption, and source authentication (digital signature).

Although WARLOCK is copyrighted and has a patent pending, the authors are making the system available free for private, non-commercial use – much like PGP (Pretty Good Privacy) – to secure user feedback and peer evaluation. To avoid export problems this offer is limited to Americans and Canadians.