CRYPTOLOGIA

A Quarterly Journal Devoted to All Aspects of Cryptology

Volume 8 Number 2 April 1984

Table of Contents

Cryptanalysis of a Maclaren-Marsaglia System — Charles T. Retter — 97

Project on Secrecy and Openness in Scientific and Technical Communication — 109

Hand-Held Crypto Device SEC-36 — Louis Kruh — 112

Sidney Hole's Cryptographic Machine — Donald W. Davies — 115

Literature Reviews — Louis Kruh — 127

On Kullback's χ-Tests for Matching and Non-Matching Multinomial Distributions — Borge Tilt — 132

Software Protection for Microcomputers — John M. Carroll and Pierre G. Laurin — 142

Corrections for Published Copy of UNITED STATES CRYPTOGRAPHIC PATENTS: 1861 - 1981 — Jack Levine — 161

The Slidex RT Code — Louis Kruh — 163

British Intelligence - Volume II - Book Review — Ralph Erskine — 173

From the Archives: Codes and Ciphers for Combined Air-Amphibian Operations — 181

An Unknown Cipher Disk — David Shulman — 187

Biographies of Contributors — 191

Published Quarterly at

Rose-Hulman Institute of Technology

Terre Haute, Indiana 47803 USA

One article was written expressly for this book, "The Spy Who Most Affected World War II." For that distinction, Kahn designates Hans-Thilo Schmidt, an obscure Nazi party member, who was a civilian clerk in the German Signal Corps. Schmidt was the spy who delivered documents that Polish cryptanalysts used to solve the German Enigma cipher machines. This article reveals for the first time the background and details of this virtually unknown man and his unparalleled betrayal which had such an enormous impact on the outcome of World War II.

Besides being a comprehensive and exciting account of notable cryptologic events, the book is a genuine bargain with its price only a fifth of what it would cost to buy copies of the publications in which the original articles appeared.

"INSIDE" NSA?

Bamford, J. The Puzzle Palace: A Report on America's Most Secret Agency, Houghton Mifflin Co., 2 Park St., Boston MA 02108, 1982, 465 pp., $16.95

This is the most comprehensive book ever written about the National Security Agency and it contains an amazing amount of detail starting from its inception as MI-8 in WW I to the present day. Its origin is traced through H. O. Yardley, W. F. Friedman, Pearl Harbor, WW II, and the various studies/committee investigations on unification of cryptologic activities, which ultimately led to President Truman's still secret 1952 memorandum establishing NSA. Bamford describes NSA's Fort Meade headquarters -- he refers to it as SIGINT City -- the physical layout and organization, how it operates, its worldwide influence, and many of its senior officials. President John F. Kennedy once told the intelligence community, "Your successes are unheralded; your failures are trumpeted." As if to underscore the truth of that remark, Bamford is only able to relate few of NSA's triumphs but, almost with excessive zeal, reveals all of its warts, and virtually all are twice-told tales. Where the author has found new information, particularly dealing with personalities, as in most of the chapter on cooperation between the British GCHQ and NSA, it makes for interesting reading. On the other hand, the section on NSA's complex network of listening posts with details on antennas, circuits, microwave signals and locations of secret sites, which is the book's largest chapter and contains new data, will undoubtedly be dull to many readers except for those inimical to NSA's mission.

A great deal of information was derived from an assiduous study of NSA's almost 30-year old, unclassified 20-page monthly newsletter, which the author wrangled from the Agency, from extensive research among the Friedman Papers at

the George C. Marshall Research Library, and many interviews with former NSA officials. The overall result is a fascinating glimpse at previously unpublished items about Friedman, Callimahos, a host of other lesser known key officials, and the intriguing life and times in SIGINT City.

INTELLIGENCE BIBLIOGRAPHY

Constantinides, G.C. Intelligence and Espionage: An Analytical Bibliography. Westview Press, 5500 Central Ave., Boulder, CO 80301, 1983, 559 pp., $60.

The author, who has spent almost 25 years in U.S. government intelligence and national security work, has justifiably described his book as "the most comprehensive and thorough bibliography of English-language nonfiction books on intelligence and espionage to date." It is an enormous work with knowledgeable comments, most of them a page or more, on close to 500 books. In a special category index the author has divided them into 54 categories. The bibliography itself is arranged by author. One of the categories is Communications Intelligence, Cryptology, and Signals Intelligence which contains 40 books. Constantinides demonstrates a familiarity and expertise in the subject matter with incisive comments and cross references in many of his annotations. In his remarks on Yardley's American Black Chamber, he provides views from five other authors and suggests areas in Yardley's career which still need to be explained. With Lewin's Ultra Goes To War, he refers to reviewers of the book as well as other authors to point out inaccuracies and to remind us that because much Ultra material is still secret, the full story has not yet been told. In his overall excellent appraisal of The Codebreakers, he expresses possibly an insider's view that Kahn's assessment of Friedman as being responsible for the U.S.' cryptologic superiority is questionable. Other worthwhile comments abound in this outstanding reference work which will be consulted frequently by persons seeking a guide to intelligence literature.

YARDLEY'S CHINESE BLACK CHAMBER

Yardley, H.O. The Chinese Black Chamber: An Adventure in Espionage. Houghton Mifflin, 52 Vanderbilt Ave., New York, NY 10017, 1983, 225 pp., $13.95

In 1938, Chiang Kai-shek, head of the Nationalist Chinese government which was fighting a desperate losing battle against the Japanese, engaged Yardley to come to the war torn capital of Chungking to set up a Chinese version of the American Black Chamber Yardley had organized and directed in New York. This manuscript, hidden for over 40 years, is the story of his adventures and

intelligence exploits in China from 1938-1940. Most of the account is a fascinating glimpse of life in a strange society of Chinese characters, European traders, politicians, generals, spies, traitors, mistresses and other colorful personalities. Few of Yardley's cryptanalytical episodes are included but he does describe, step-by-step, how he solved a cipher which used a public Chinese code book superenciphered by a book cipher. The book has an introduction by James Bamford, author of The Puzzle Palace, with additional details of Yardley's experiences in China. It concludes with "Memories of the American Black Chamber", a brief memoir by the author's wife, Edna Yardley, who is its last surviving original member.

CODES IN THE ETHER

Monitoring Times, 140 Dog Branch Road, Brasstown NC 28902. Issued monthly, 32 pp., $10.50 for one year, $20.00 for two years.

This 32 page tabloid newspaper is written for shortwave listeners and scanner buffs. It usually has a feature on clandestine stations including spy number broadcasts, i.e., stations transmitting messages in numerical code. A recent issue contained articles on Basic Codebreaking and Japanese messages sent before the Pearl Harbor attack. It covers other offbeat listening areas such as satellite reception, monitoring the AWACS Net, nuclear shipments, etc. and provides the frequency lists. Other features review equipment, books, provide advice on getting started and improving your operation. Free sample copy available on request.

BIOGRAPHY OF ALAN TURING

Hodges, A. Alan Turing: The Enigma. Simon and Schuster, 1230 Ave. of the Americas, New York NY 10020. 1983. 587 pp. $22.50.

Alan M. Turing was an English mathematical genius whose name is perpetuated in the annals of computer history for the Turing machine, a theory and, eventually, a device he invented. His work, starting in the mid-1930s, was the theoretical foundation for the modern digital computer.

Lesser known is his leading role at Bletchley Park, where Government Code and Cypher School cryptanalysts were confronted with improved Enigma ciphers when the Germans upgraded their communications security. Instead of using six or seven plugboard connections, the Enigma operators started to connect ten pairs of letters; and the number of available rotors was increased from three to five. There are 150,738,274,937,250 ways to connect ten pairs of letters, and with just three rotors there are six ways to arrange them -- but with five to