Reviews

The Reviews department features reviews of selected publications. Most reviews are solicited, but colleagues are invited (and indeed encouraged) to participate in this reviewing activity by indicating their wish to review a work, by suggesting titles to the Reviews editor, or by submitting a manuscript. In the latter instance please consult with the editor to avoid duplication. Books, monographs, journal articles, films, videotapes, and other publications relating to the history of computing will be described briefly in the Capsule Reviews section. Comments on books, articles, or reviews are welcome. NB: Reviews without bylines are by the editor. —*Henry S. Tropp*

REVIEWS

☐ Franksen, Ole Immanuel. **Mr. Babbage's Secret. The Tale of a Cypher and APL.** Birkerbød, Denmark, Strandbergs Forlag, 1984, 320 pp., Dkr 320.00.

Two reviewers have given their views of the book—Ed.

A very brief glimpse into the cryptographic work of Charles Babbage is given in just three pages of David Kahn's classic work *The Codebreakers* (1967). Kahn mentions Babbage's interest in solving enciphered personal announcements in the "agony columns" of the (London) *Times*, as well as ciphered messages when requested by relatives, acquaintances, and, in one instance, royalty. Kahn gives two delightful quotations from Babbage: "Deciphering is, in my opinion, one of the most fascinating of arts, and I fear I have wasted upon it more time than it deserves"; and, speaking of his experiences as a schoolboy, "The bigger boys made ciphers, but if I got hold of a few words, I usually found out the key. The consequence of this ingenuity was occasionally painful: the owners of the detected ciphers sometimes thrashed me, though the fault lay in their own stupidity." (Kahn remarks that in later life Babbage's rewards for his cryptographic ability became "less punishing.") *Mr. Babbage's Secret* will be welcomed by many students of the history of computing who wish to know more about one of computing's most colorful and best-known personalities.

Ole Franksen is with the Electric Power Engineering Department at the Technical University of Denmark. He became interested in computers as a graduate student when he first used an IBM 602A punched card calculator in a study of heating problems in electric power generators. His work with computers in power engineering has continued since then, and he has made substantial contributions in this area. In addition, his work has led him to a broad interest in the history of computing and the history of science in general. An earlier paper, "Mr. Babbage, the Difference Engine, and the problem of notation: An account of the origin of recursion and conditionals in computer programming," was reviewed in the *Annals*, in both an Essay Review (Vol. 5, No. 4, October 1983, pp. 411–414) and a Capsule Review (Vol. 4, No. 4, October 1982, pp. 378–379). Another work of Franksen's that may be of interest to some readers of the *Annals* is his monograph, *H. C. Ørsted—A Man of Two Cultures* (Bang & Olufson, 1981). In *Mr. Babbage's Secret* he continues in the style of his earlier paper and considers another aspect of the work of Charles Babbage, many of the technical details being illuminated by simulations in the APL language. The author undertook this work with the financial backing of IBM in the Scandinavian countries. The book was published in connection with the APL84 Conference in Helsinki in June 1984.

Most of the book is taken up by three long chapters, each one having the same format—a treatment of the main topic of the chapter followed by a shorter discussion of relevant computer simulations and analyses. These chapters are preceded by a very short prologue and followed by an even shorter epilogue of two pages. Herman H. Goldstine has contributed a biographical sketch of the author. The book concludes with 19 pages of notes giving references and acknowledgments; there is no index. The book was handsomely produced on good-quality paper. Several black-and-white illustrations and many reproductions of excerpts from contemporary references and manuscripts occur throughout the text.

Chapter 1, "The Philosophy of Deciphering," introduces Babbage's deciphering work, which began in about 1846 and extended over some 18 years. Many of Babbage's ciphering problems came from personal notices published in the *Times*, some through private communications, one as an expert witness for the defendant in a lawsuit, another from Henrietta Maria, queen of Charles I, and others from members of his family. The chapter concludes with a "cryptographic tool-box of user-defined APL-functions" intended to

simulate as closely as possible Babbage's methods of breaking the ciphers. There are 10 pages of APL functions, all carefully designed and documented and with examples of their use, for solving ciphers based on false word divisions, word reversals, and Caesar and reciprocal forms of monoalphabetic substitutions.

Chapter II, "Between Mathematics and Reality," is an essay of some 120 pages introduced by the three topics of notation, permanence of form, and "a new mode of analysis" or geometry of form which may be found in Babbage's writings. That this chapter might appear at first to constitute a digression from the author's cryptographic discussions does not decrease its importance. Some readers may wish to read this chapter last, browsing through those pages that hold some initial interest before reading the entire chapter. However that may be, in Chapter II Franksen considers in some depth what should be one of the central themes in programming: the representation of data and the definition of operations on them, a theme he has evidently pondered deeply and read widely for some years. It is his central thesis that the well-known work of Kenneth Iverson on the development of APL and the more recent and much less known work of Trenchard More on array theory allow a geometric interpretation of data. Franksen supports this thesis with a wide-ranging discussion involving the work of Newton, Leibniz, Euler, Lagrange, Gauss, Whewell, Boole, Cantor, Klein, Viking runes and their decipherment, the life and work of Danish mathematicians, the development of programming languages (especially that leading to APL and its later extensions), and even Alice and the Chesire Cat. This chapter is one that can be savored and thought about at different levels and at different times. Each reading should help further illuminate fundamental ideas and bring out minor but interesting details. Persons who have a knowledge of APL will be interested in the discussion of Babbage's paper on notation that appeared in the *Edinburgh Encyclopedia* in 1830. Statements such as, "All notation should be as simple as the nature of the operations to be indicated will admit," and, "When it is required to express new relations that are analogous to others for which signs are already contrived, we should employ a notation as nearly allied to those signs as we conveniently can," could have been written about APL, although some of them predate Babbage.

Chapter III, "A Conservation Law of the Message," continues the treatment of Chapter I but on more general terms and in light of the discussions in Chapter II. The author discusses Babbage's unpublished work on the construction of dictionaries of all words in one, two, . . . , letters, the frequency of occurrence of letters in text, word recreations of various persons (e.g., a story in which all vowels other than *e* were omitted), and a long treatment of the Vigenere Cipher.

An evaluation of the place of *Mr. Babbage's Secret* in the literature of cryptography must be left to other reviewers. In the literature of computing, however, the book may be regarded as an interesting example of the use of a programming language to complement and illuminate the discussion of a quantitative subject. Franksen's use of APL here is in the spirit of the use of the language presented by Iverson in his 1979 Turing Award Lecture, "Notation as a tool of thought" (*Comm. ACM*, Vol. 23, No. 8, August 1980, pp. 444–465). Furthermore, the author introduces the language inobtrusively, so that a reader who wishes to ignore the APL language may do so without detracting from understanding and enjoying the narrative. Those readers who wish to complement the text with the APL functions, or even who wish to use the text as an introduction to APL, have an excellent opportunity to do so. The book may also be regarded as a contribution to the examination of the mathematical foundations of programming languages. Last and possibly most important for the present reviewer, this book is an example of a treatment of a technical topic, a literary style, and a publishing quality that is becoming increasingly rare in the present decade of "high technology" where little seems permanent or worth preserving.

In the epilogue Franksen says, "Others, perhaps by nature more rebellious, refuse lifelong confinement to the field they were reared in. Yet, by widening the scope, they are subject to adverse criticism from the professionals encamped on their few or many frontiers. This is a calculated risk, a foreseeable charge, which they find honourable to face." He could have added that such persons very often produce work that is much more interesting and stimulating than that of their colleagues with more narrow professional interests. They are certainly much more congenial companions! With his wide range of scientific, historical, literary, and linguistic interests, Ole Franksen is undoubtedly one of these all too rare persons. We should be indebted to him for sharing with us *Mr. Babbage's Secret*.

K. W. Smillie
Department of Computing Science
University of Alberta
Edmonton, Alberta T6G 4H1
Canada

There are people who show a certain predilection or even adoration for Charles Babbage (may Lady Lovelace serve as an early example). Which is a thing

easy to understand. There are also people who show a certain predilection or even adoration for APL (Alan Perlis, whom I value highly, is a good example). This, too, should be tolerated. But if both these traits coincide, you will get an emulsion—not a mixture. And grit is added to this mayonnaise by introducing into it Babbage's amateurish dabbling in cryptography, according to what the title and part of the contents say.

Mathematically speaking, Franksen's book is trivial despite the fact that David Hilbert and Felix Klein are mentioned a number of times; cryptologically, it is shallow and even contains some errors. I don't think that the historian will find anything new in it. Some parts of the book are very hard to read, especially in those places where APL programs printed by a wire printer are reproduced in facsimile. And there is no index.

One more thing: there are a great number of quotations, which prove that the author is well-read, but very often have nothing to do with the subject. Most of them sound good, and those who are in need of quotations are invited to turn to this book.

My regrets go to Herman Goldstine for having agreed to write the introduction.

F. L. Bauer
Institut für Informatik
Technische Universität München
Arcisstrasse 21
D-8000 Munich 2
West Germany

☐ Hinsley, F. H., with E. E. Thomas, C. F. G. Ransom, and R. C. Knight. **British Intelligence in the Second World War: Its Influence on Strategy and Operations.** Volume 3, Part I, London, Her Majesty's Stationery Office, 1984, £17.95. New York, Cambridge University Press, $39.50, xvi + 694 pp.

The penultimate part of Hinsley's impressive official history covers the period from June 1943 to summer 1944; its main subjects are the war at sea and in the air, the Mediterranean and the V weapons (V1 pulse jet and V2 rocket). Its interest for *Annals* readers lies principally in descriptions of the intelligence derived from the huge output of Enigma cipher machines (see Rejewski 1981) and the much more complex cipher traffic known to the United Kingdom's Government Code and Cypher School (GCCS) at Bletchley Park, England, as "Fish." The need to decrypt Fish led to the construction of Colossus I and II, the world's first, albeit very special-purpose, electronic computers (see Flowers 1983; Good 1982). The teleprinter on-line machines on which Fish was encrypted were mainly the Lorenz SZ40 and 42 and the Siemens and Halske T52 (code-named "Tunny" and "Sturgeon," respectively, by GCCS; for detailed descriptions of the latter, which had 10 wheels, see Davies 1982; 1983). (A mysterious third machine, "Thresher," whose real name is not given, is accorded a mere mention.)

Appendix 2 relates how GCCS first encountered Fish in 1940 and broke it from June to October 1942, using machines for deciphering after the settings were found. Improvements in German enciphering methods caused a working party to conclude that high-speed machines were essential for further progress to be feasible. The first such machine was Heath Robinson, which had fewer than 100 vacuum tubes ("valves" in England) and was somewhat rudimentary. Nonetheless, 24 were ordered, but only two were delivered, because work was concentrated on Colossus. By the war's end, 10 Colossi had been delivered.

The network of Tunny links is charted in the book. Decrypted Fish messages, which were up to 60,000 characters long, were of considerable strategic value, since they were often sent at army group level or higher. In particular, Colossus made a significant contribution to the success of the D-day landings on June 6, 1944; although the details are not given here, they should follow in Part II, which will cover that period.

Intelligence derived from Fish was the perfect complement to deciphered Enigma traffic, which revealed information of a more tactical nature. Being portable, Enigma machines were used at lower levels; well over 100,000 machines were issued to the German forces. Numerous specific examples of Enigma-based intelligence are given throughout the book—many more than for Fish.

In Hinsley's view, GCCS's successes against Enigma shortened the war in Europe by as much as three years (*Times* 1981). Thus Volume 2 and this part of Volume 3 show the crucial role played by Enigma in the critically important battle of the Atlantic. While it is true that the breaking of army and naval Enigma by GCCS owed little directly to the Poles, it depended very largely on the "bombes," which, when suitably programmed with probable words, ascertained the key settings used by the numerous Enigma nets. Gordon Welchman, the codesigner with Alan Turing of the sophisticated British bombes, indicates that the bombe program would have suffered significant delays had it not been for the breakthroughs in 1940 made possible by the Polish contribution (Welchman 1982, p. 165).

Unfortunately, in Appendix 1 of Volume 1 of the present work, which deals with the contribution made by the Poles to GCCS on Enigma, Hinsley underesti-

mates the effect of the Enigma machine, five rotors, and other important material the Poles sent to GCCS in August 1939 (Rejewski 1981, p. 227), implying that GCCS would have been in exactly the same position after the capture of Enigma rotors from a U-boat, U-33, in February 1940. He therefore concludes that the Polish help advanced GCCS's work against Enigma by only seven months (Hinsley 1979, p. 494). Hinsley refers, however, only to "Three Enigma wheels ... captured from the crew of U-33" (Hinsley 1979, p. 336); it would therefore appear that an Enigma machine was not taken from U-33. In the absence of a machine, GCCS would have had to reconstruct the reflecting rotor and the entry ring (the connections between the plugboard and the stationary entry rotor).

Which rotors were taken from U-33? Hinsley does not say. Were any the naval rotors? In 1940, the full naval set was eight, of which rotors VI to VIII were issued only with naval machines (Rohwer 1977, p. 233). If even one naval rotor came from U-33, GCCS would have had to reconstruct three rotors in order to make up a full set of five for the air force traffic, which was the only kind then vulnerable to attack; naval Enigmas presented too many difficulties in 1940. If none were naval, GCCS would still have faced the same problem for two rotors. A measure of that problem's magnitude is illustrated by the fact that 40 years later Welchman, one of GCCS's top Enigma cryptanalysts, could not believe that the Poles had managed to re-create rotors IV and V by cryptanalytic means (Welchman 1982, p. 16). Documents and German procedures that had assisted the Poles before 1939 were neither available nor being used so as to have helped GCCS with rotors IV and V in 1940 (see Rejewski 1981, pp. 221, 227).

GCCS would also have had to have found a method for working out the keys used by Enigma nets—another major difficulty to which Hinsley makes no reference. Perforated sheets, invented by the Poles, were used for this purpose in early 1940. Welchman independently reinvented these in late 1939 and might still have done so had there been no Polish assistance. But the massive task of preparing the sheets could not have been started until GCCS had an Enigma machine and the relevant five rotors. It took GCCS about 14 weeks to make the sheets in 1939 (Hinsley 1979, p. 493). Following U-33, that period alone would have brought time forward to the end of May 1940. The sheets would then have been useless against current air force traffic after a major change in German keying methods on May 1, 1940 (Hinsley 1979, p. 109)! In real life GCCS and the Poles had found about 100 daily keys by the end of May, leading to the decrypt-ment of several thousand messages (Kozaczuk 1984, p. 93).

Time to reconstruct an Enigma machine (with reflecting rotor, entry ring, and the two or more missing rotors), to test and make perforated sheets, and to think about the need for and the outline design of a British bombe—for none of which Hinsley makes any allowance—must therefore be added to his seven months. He considers only one of these problems when assessing the Polish contribution—the requirement to develop analog machinery (the bombes)—and that dismissively. Yet as late as July 1939 (immediately before the Poles came to its rescue), GCCS believed that there was little prospect of reconstructing Enigma's intricate wiring on its own (Hinsley 1979, p. 54). If its pessimism was well founded, and that might still have been the position even following U-33, significant work on making the British bombes would have been impossible until after the Enigma captures of March and May 1941 (see Hinsley 1979, p. 337).

Hinsley suggests that the Polish help resulted only in the earlier delivery of the British bombe and GCCS reading a German air force key sooner, both being brought forward seven months. A very different view is given by Welchman, who was head of Hut 6 (army and air force Enigma) at GCCS for several years. For a variety of convincing reasons, connected with the organizational and the cryptanalytical aspects of GCCS's Enigma work (see Welchman 1982, pp. 164–165), he considers that had it not been for the Poles, "*Hut 6* Ultra would never have gotten off the ground" (my emphasis) (p. 289).

As this part of the work reveals, GCCS also decrypted messages enciphered on advanced cipher machines other than Enigma and Fish. It contains many examples of invaluable intelligence derived from the messages of the Japanese ambassador to Germany (General Hiroshi Oshima—as often with the holders of positions he mentions, Hinsley does not give the name, which is a pity) and of the Japanese naval mission in Berlin. Appendix 11 is an excellent illustration of the value of this material. It sets out a lengthy and copiously detailed British Admiralty intelligence report on Type XXI U-boats. That report was completely derived from decrypts of the naval mission's messages and contained information of a quality that it would have been quite impossible for an agent to have obtained in Germany. In addition, agents' reports could raise suspicions that the material had been planted or the agents "turned." In complete contrast, the diplomatic traffic on Purple, like messages sent by Enigma and Fish, never, so far as is known, contained information designed to deceive the allies.

Although Part I does not give the name of the machine on which the Japanese diplomatic messages were enciphered, it was almost certainly Purple (see Kahn 1967, p. 508; 1984, pp. 108–109), which had been reconstructed by William Friedman and his brilliant U.S. Army team with help from the U.S. Navy's OP-20-G section. GCCS had received several copies of the Purple machine from the United States in 1941 (Kahn 1967, p. 23). Even so, not until the spring of 1944 was the cipher—presumably the settings used for the messages—of the Japanese naval attaché broken. One reason for the delay may have been that in October 1942 and May 1943, GCCS had agreed with the U.S. Navy and Army, respectively, to concentrate on German and Italian ciphers, and to leave Japanese ciphers largely for attack by those departments (Hinsley 1981, pp. 57–58).

This part of Volume 3, like Volume 2 (and Volume 1, except for Appendix 1), is impeccably researched and well produced. Hinsley's readers benefit greatly from the fact that he worked at GCCS (as a naval intelligence expert, not a cryptanalyst). As with the other volumes in the series, Part I is a reference work and not intended for bedtime reading; the average reader is likely only to want to dip into it on selected topics. The series is an intelligence history—not a cryptological one. It contains no mention of the cryptanalytical methods used by GCCS except for the general references to machines in two appendixes. It may be history from the files and without personalities, but given the very nature of the subject, that was almost inevitable; we would probably otherwise be waiting for the first volume to be finished. Hinsley's scholarship and unequaled knowledge of his subject make him a perfect guide to these mysteries. He has created a classic with this magnificent series of volumes, which will undoubtedly be the reference work on the subject for countless years to come.

REFERENCES

Davies, D. W. 1982. The Siemens and Halske T52e cipher machine. *Cryptologia 6*, 289–308.

Davies, D. W. 1983. The early models of the Siemens and Halske T52 cipher machine. *Cryptologia 7*, 235–253.

Flowers, T. H. July 1983. The design of Colossus. *Annals of the History of Computing*, Vol. 5, No. 3, 239–253.

Good, I. J. January 1982. A report on T. H. Flowers's lecture on Colossus. *Annals of the History of Computing*, Vol. 4, No. 1, 55–59.

Hinsley, F. H., with E. E. Thomas, C. F. G. Ransom, and R. C. Knight. 1979. *British Intelligence in the Second World War: Its Influence on Strategy and Operations*. Volume 1. London, Her Majesty's Stationery Office.

Hinsley, F. H., with E. E. Thomas, C. F. G. Ransom, and R. C. Knight. 1981. *British Intelligence in the Second World War: Its Influence on Strategy and Operations*. Volume 2. London, Her Majesty's Stationery Office.

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

Kahn, D. 1984. *Kahn on Codes*. New York, Macmillan.

Rejewski, M. July 1981. How Polish mathematicians deciphered the Enigma. *Annals of the History of Computing*, Vol. 3, No. 3, 213–229.

Rohwer, J. 1977. *The Critical Convoy Battles of March 1943*. London, Ian Allan.

Times (London). September 9, 1981. Interview, p. 5.

Welchman, G. 1982. *The Hut Six Story: Breaking the Enigma Codes*. New York, McGraw-Hill.

Ralph Erskine
25 Hawthornden Road
Belfast BT4 3JU
Northern Ireland

☐ Thompson, Thomas M. **From Error-Correcting Codes through Sphere Packings to Simple Groups.** Washington, D.C. Mathematical Association of America, Carus Mathematical Monograph No. 21, 1984, 228 pp. + xiv, $21.00 (MAA members, $16.00).

Thompson provides an excellent example of the constant interaction between applied and theoretical mathematics. This particular tale begins in 1947 with the frustration of Richard Hamming, then a young mathematician at Bell Laboratories. Thanks to George Stibitz's pioneering work a decade earlier, Bell Labs had a newly constructed general-purpose relay calculator, the Model V. Like all the Bell relay devices, the Mod V had an error-detection code. A check failure sounded an alarm, and the attending operators then dealt with the cause. On weekends, however, the calculator was run unattended, and Hamming had access only on weekends.

> Two weekends in a row I came in and found that all my stuff had been dumped and nothing was done. I was really aroused and annoyed because I wanted those answers and two weekends had been lost. And so I said, "Damn it, if the machine can detect an error, why can't it locate the position of the error and correct it?"

In a memorandum dated July 27, 1947, his first solution appeared, and we had the birth of what is now an independent branch of mathematical research, error-correcting codes. Hamming's original work and its subsequent use by Claude Shannon in a now-classic work on information theory led to the work of M. J. E. Golay. Golay codes triggered the sphere-packing results of John Leech, which in turn led to the discovery by J. H. Conway of three new simple groups.

The question of sphere packing—that is, "In Euclidean n-space E^n, how many disjoint, open, congruent n-spheres must be located to maximize the

fraction of the volume of E^n that the n-spheres cover?"—goes back to an 1831 paper by Gauss. Leech's packing of E^{24} is described in Chapter 2: "The packing actually evolved in two steps, the second being the trigger for the discovery of new large simple groups," which is the subject of Chapter 3.

Thompson has done a marvelous job of reconstructing the events that led to the results described in this small volume. As he states in the preface,

> By tracing some of the twists, turns, switchbacks and dead-ends of this path, we hope to provide a small window on the history of mathematics in the twentieth century. . . . But one claim we can make on the basis of this study is certain: The record will not be neat and tidy. . . . Chaos and spontaneity, not austere order, mark the way much of mathematics is done. The elegance of the printed article conceals the circumstances that precipitated the results. The history of mathematics is a story of people and their guesses, misfortunes and struggle, not merely a list of theorems and their proofs.

To deal with the human aspect of these events, Thompson made use of interviews, telephone conversations, and letters with the main participants: Conway, Golay, Hamming, Leech, and Shannon. In spite of this assistance, Thompson is still not entirely happy.

> But even with all this encouragement and help, I was not able to paint a complete picture. There is still disagreement on some of the historical facts. On others, memories could not fill all the gaps. In even one case, antipathy for the entire project, indeed on the history of mathematics, closed the door on the corroboration of certain details.

All of this is familiar to anyone working in contemporary history. In particular, the editors of this journal know that what we do will be incomplete and subject to still-unanswered questions and unresolved controversy. Thompson's work, despite his admitted frustrations, is first-rate historical research and good clear writing. As a mathematics teacher, he has gone to great pains to make the material understandable to anyone "with even a casual acquaintance with vector spaces and groups. . . . I wrote each page so that an upper-division student could understand it."

This volume was originally written as Thompson's Ph.D. thesis at the University of California, Davis (see a review in the *Annals*, Vol. 2, No. 1, January 1980, p. 90), under the supervision of Sherman Stein. Stein, who has long had an interest in packing and tiling problems, told me that he had been thinking about the interrelationship of these topics and had hoped to find the right student to work on it. There is no question that he found the right person.

Henry S. Tropp

CAPSULE REVIEWS

☐ Kahn, David. **Cryptology and the Origins of Spread Spectrum.** *IEEE Spectrum*, September 1984, pp. 70–80.

Although not of direct interest to the history of computing community, this article is worthy of note because it comments on the activities of Alan M. Turing during his visit to Bell Laboratories for two months during the height of World War II. Kahn describes an unbreakable scrambler used to guarantee secure telephone communications between Allied leaders. Turing had been working on a similar idea and was sent by the British government to investigate the reliability of the SIGSALY device that was under development by the U.S. Army Signal Corps. The article is well illustrated with contemporary photographs and circuit diagrams. Besides the comments on Turing, other early notables such as Claude Shannon, many of the electronic engineers at Bell Labs, and even the actress Hedy Lamarr are mentioned in connection with the subject of codes and cryptology.

M. R. Williams
Department of Computer Science
University of Calgary
Calgary, Alberta T2N 1N4
Canada

☐ Schneck, Paul B. (ed.). **Special Section on Computing in Space.** *Communications of the ACM*, Vol. 27, No. 9, September 1984, pp. 901–936.

This section contains three papers ("Development and Application of NASA's First Standard Spacecraft Computer (NSSC-1)," "Design, Development, Integration: Space Shuttle Primary Flight Software System," and "Architecture of the Space Shuttle Primary Avionics Software System (PASS)") that are of some interest to the historical community. While primarily written to introduce the reader to the subject of the computer requirements of the space shuttle, they also contain information on the historical development of this equipment.

M. R. Williams

☐ Pugh, Emerson W. **Memories that Shaped an Industry.** Cambridge, MIT Press, 1984, 336 pp., $25.00.

This seems like a very interesting book on an important part of the history of computers. On the whole, it is rather objective considering that it comes from an IBM source. I believe the author began the book by assuming that the major developments in magnetic core memory had been done inside of IBM and then

had to shift his ground completely after he got into the subject matter. The layout of the book has somewhat that flavor, starting in the first two or three chapters about IBM and then shifting over to the recognition that the magnetic core memory came to IBM from MIT. [*Editor's Note:* Magnetic core memory was developed by Jay W. Forrester at MIT.] It is a good story with some interesting insights into the personalities and the politics of the situation. On the whole, I believe it is an accurate reflection of what happened, at least as much as one can expect from a single author.

Jay W. Forrester
Alfred P. Sloan School of Management
Massachusetts Institute of Technology
Cambridge, MA 02139

☐ Davies, Donald W. **Sidney Hole's Cryptographic Device.** *Cryptologia,* Vol. 8, No. 2, April 1984, pp. 115–125.

Donald Davies, of the United Kingdom's National Physics Laboratory, continues a series on cipher equipment in London museums with a detailed description of Hole's unusual rotor machine, two examples of which are in the Science Museum. His article reproduces many of the detailed engineering drawings that accompanied the Australian patent. Built for the British War Office in 1926, Hole's machine consists of two modified typewriters connected by a pneumatic rotor mechanism. The rotor interconnection has five moving cylinders, each with 28 holes: each hole changes the vacuum connection between the 28 keys on the two typewriters. The machine was somewhat insecure cryptanalytically. Its bulk and pneumatic operation alone would have made it completely unsuitable for field use, unlike the German Enigma machine. Not surprisingly, no machines are known to have gone into service with any army, although it was patented in many countries.

Ralph Erskine

☐ Tilt, Borge. **On Kullback's χ-Tests for Matching and Non-Matching Multinomial Distributions.** *Cryptologia,* Vol. 8, No. 2, April 1984, pp. 132–141.

Solomon Kullback was one of the first three mathematicians recruited as cryptanalysts in 1930 for the Signal Intelligence Service by William Friedman (David Kahn, *The Codebreakers,* pp. 386, 576). This paper considers some aspects of the χ (chi) cross-product sum test that Kullback devised in 1935 for the purpose of matching alphabets by comparing certain aspects of frequency counts; it is related to the famous "index of coincidence" (see Kullback, *Statistical Methods in Cryptanalysis,* para. 21; Kahn, pp. 380–382). Kullback's book was first printed in 1938 for army use, becoming widely available only in 1976, when it was published by the Aegean Park Press as part of its invaluable Cryptographic Series.

Tilt shows that there is an error in Kullback's Equation 21.7 (nonmatching distributions) and sets out a correct version. He also derives the mean of χ in a case not discussed by Kullback—partially matched distributions.

Ralph Erskine

☐ Kruh, Louis. **The Slidex RT Code.** *Cryptologia,* Vol. 8, No. 2, April 1984, pp. 163–171.

Kruh's article consists of a short historical introduction, to which the instructions (including an imaginary vocabulary) for using the Slidex code are appended. The code was one of about 20 codes and ciphers authorized for use in *Overlord,* the allied invasion of Normandy on June 6, 1944. Intended for radiotelephone (RT) use, the Slidex code consisted of a frame holding a card with 12 columns and 17 rows. Each card had words, letters, and numbers in its boxes. Messages were to be sent in a mixture of code and clear speech. As could have been forecast, this turned out to be a dangerous combination.

The code was first used in manuevers in southern England in March 1944: the efficient German listening service cracked it quickly. Each country's intercepting units monitored, and attempted to break, the enemy's low-level signal traffic—a quite separate exercise from the cryptanalysis of high-level codes and ciphers. Aileen Clayton's excellent *The Enemy Is Listening* shows how similar codes were penetrated by the Royal Air Force's "Y" service.

It must be extremely difficult to invent secure, but easy to use, codes for widespread use in RT or telephonic speech. In the Pacific war, the Marine Corps attached Navajo Indians to command posts for voice communications; only 28 non-Navajos spoke the language, and none were German or Japanese (David Kahn, *The Codebreakers,* p. 550). Since the Slidex code was so inherently vulnerable, it is disturbing to read that it was still in service in December 1944, despite adverse reports by the Signal Corps on its security.

Ralph Erskine