witness assignments, as long as my testimony can be based on fact rather than opinion. In one unusually simple patent case, for instance, my main job was to prepare a videotape showing the operation of 12 different data-entry machines! When I testified about the residual value reports, my testimony was always factual; I had only to explain the already-published reports and enter them into evidence.

The income tax lawsuits were based on a stupid provision of the federal income tax law which was repealed in 1981. The provision permitted a taxpayer to take title to a computer already on lease, take tax deductions for several years by depreciating the computer, and then sell the computer at the end of the lease. If the computer had no value then, however, and if the taxpayer knew at the outset that it wouldn't, the deal was "a sham undertaken for tax purposes only," and the deductions would be disallowed. The provision was stupid because it required the taxpayer's initial assumption of residual value to be judged "reasonable at the time," a subjective matter. My testimony could settle the "reasonableness," though, if I had prepared a residual value forecast for the machine in question at about the time the taxpayer acquired it. The courts always accepted my reports as representative of "reasonable forecasts made at the time"; the forecasts did not have to be accurate. I had a better success record winning lawsuits with the residual value reports than I did with the forecasts in them!

I'll end on this note of modesty. I'm still active in some consulting and academic areas, so there may be more paragraphs for these memoirs later. In any case, though, I'm happy to have been a pathfinder and guide for many participants during the formative years of the computer industry.

Reviews

PEGGY KIDWELL, EDITOR

The Reviews department includes reviews of publications, films, audio- and videotapes, and exhibits relating to the history of computing. Full-length studies of technical, economic, business, social, and institutional aspects or other works of interest to Annals readers are briefly noted, with appropriate bibliographic information.

Colleagues are encouraged to recommend works they wish to review and to suggest titles to the Reviews editor.

❑ "Babbage and Cryptography. Or, the Mystery of Admiral Beaufort's Cipher," ***Mathematics and Computers in Simulation***, Vol. 35, 1993, pp. 327-367.

Babbage had planned to write "The Philosophy of Deciphering," but never began it. He left behind copious worksheets which show how much time he spent on cryptography, but what he was doing is very unclear. Ole Franksen has done much to help us evaluate Babbage's cryptographic work and published an interesting and unusual book, *Mr. Babbage's Secret: The Tale of a Cipher — and APL*,[1] in which his discoveries are well documented. In the article reviewed here, he restates some of this work and adds more material with the purpose of illuminating the origin of the Beaufort cipher.

The Vigenere cipher is a stream cipher in which the key stream is a repeated word. Letters are given numerical values

The article raises the question "Did Babbage act as cryptographic expert for the Royal Navy through his friend Beaufort?" No evidence is given — it is just a conjecture.

— for example, from 0 to 25 in a 26-letter alphabet. The plaintext P and keystream K are combined to produce ciphertext C by the rule $C = P + K$, mod 26. This cipher has been "reinvented" countless times.

Beaufort gave us the Beaufort Scale of wind strength; he was an influential and resourceful person and has also given his name to the Beaufort cipher, a variant of the Vigenere with the rule $C = K - P$, mod 26. Decipherment follows the same rule, $P = K - C$, mod 26, and this could make it easier to use.

Franksen shows that the attribution of the cipher to Beaufort is uncertain. Indeed, David Kahn has recorded[2] that it was published in 1710 by Giovanni Sestri. For Beaufort's rediscovery, there are contemporary references to a publication in a scientific journal, but this seems to be lost. A published explanation of the cipher by Beaufort's colleague, Lieutenant Becher, proves to be Vigenere, and the only firm contemporary attribution is on a card, sold for sixpence, written by Beaufort's son William Morris Beaufort. But Beaufort was an honorable man, and it is likely that he really did reinvent the cipher known by his name.

The article raises the question "Did Babbage act as cryptographic expert for the Royal Navy through his friend Beaufort?" but no evidence is given — it is just a conjecture. The factual material concerning Babbage's cryptographic work is good, in particular the account of his solution of a challenge cipher by Thwaites. This material is given more fully in the book, to which there are many references in this article, and its abbreviation in the article loses a lot.

Much of the article, though interesting in its own right, is peripheral to the subject. I found 19 of its 41 pages to be diversions from the real theme. If the space had been used to expand on what Franksen has found from the Babbage manuscripts, it would have been a real contribution to history. It is mostly entertaining but, finally, a disappointment. The book is a better source, though it shares the discursive style. The full evaluation of Babbage's cryptographic work remains a challenge to historians of science.

References

1. O.I. Franksen, *Mr. Babbage's Secret: The Tale of a Cipher — and APL*, Prentice-Hall, 1985.

2. D. Kahn, *The Codebreakers*, Macmillan, 1967.

— *Donald W. Davies*

Biographical note: Donald W. Davies was on the team of scientists at the UK National Physical Laboratory (NPL) that built the ACE Pilot Model computer in the UK. In the 1960s, still at the NPL, he pioneered new concepts for communication networks and data communications, working particularly on packet switching. In 1966 he became head of the Computer Science Division at the NPL. He initiated research in data communications at NPL, including the building of a packet-switched local network and the theoretical/simulation study of flow control and congestion in networks. Since 1978 he has taken as his specialty the security of data in networks, working on this topic first at NPL and then, after his retirement in 1984, as a consultant specializing in banking systems. (See also his obituary for Edward Newman in this issue.)

❑ Bruce Collier, ***The Little Engines that Could've: The Calculating Machines of Charles Babbage***, Harvard Dissertation in the History of Science, Garland Publishing, Hamden, Conn., 1991, ISBN 0-8240-0043-9, 352 pp., $65.00.

This book is an unrevised facsimile reproduction of a Harvard PhD thesis with the same title originally written in 1970. Hence, the key issue for the reviewer is whether or not, after the passage of over 20 years, the book is still a worthwhile addition to the Babbage scholar's bookshelf. The answer is unequivocally affirmative. The thesis has long been regarded as the definitive account of the construction of Babbage's engines, but has hitherto mainly been available via boot-legged photocopies. Now that Collier's work is fully in the public domain, the book is an admirable compliment to Anthony Hyman's standard biography *Charles Babbage: Pioneer of the Computer* (Oxford University Press, 1982), and it gives a much more detailed account of the development of the engines.

Collier makes use of most of the key sources on Babbage, including his correspondence in the British Library, the Babbage papers in the Science Museum, and the Buxton MSS in the Museum of the History of Science at Oxford. Collier was probably the first postwar scholar to use these sources effectively, and they still constitute the main Babbage sources.

The book consists of three major chapters, plus introductory and concluding chapters. The introduction gives a restrained and accurate account of Babbage's life and work, and it lacks only a full discussion of Babbage's economic and theological works (which is of course the product of more recent scholarship). The first major chapter describes the development of the Difference Engine up to 1833. This chapter contains the definitive account of Babbage's dealings with the government and is much less tedious than Babbage's own writings on the subject. While Collier is generally more objective than Babbage, he is occasionally taken in by his rhetoric, stating on page 90, for example, that "Babbage received neither reward nor honor . . . not even an expression of gratitude."

The middle chapter deals with the Analytical Engine, in which Collier has skillfully avoided the "morass of detail" without descending to superficiality. His explanation of the origins of the Analytical Engines is easily the clearest and most readable account so far written. He also corrects the exaggerated view of the contribution of Ada Lovelace to the Analytical Engine. A very lucid picture is drawn of Babbage's mental processes as he alternately elaborated and simplified the engine's design over a period of many years. The last major chapter, which describes the engines after 1846, is perhaps the most important in the book, since it is the period least satisfactorily described in the standard biography. Collier provides a very clear picture of exactly what Babbage was trying to achieve in the last 30 years of his life. Collier also tries to analyze Babbage's assertion that the improvements to mechanical engineering brought about by his engines amply repaid the government's investment in them. As Collier notes, Babbage was himself responsible for the orchestration of much of the evidence, and the validity of the spin-off argument remains an open research question. In this regard, Collier did not do such a good job for the Babbage engines as Michael Lindgren did for the Scheutz engines in his (admittedly much later) *Glory and Failure* (MIT Press, 1990).

Perhaps the most annoying fault of the book is Collier's failure to give the context of many of the personae in the text, who are identified baldly by name without stating the person's occupation or relationship to Babbage. For example, on page 52 correspondence with the Reverend Edward Smedley is cited without further explanation — but Smedley was editor of the *Encyclopedia Metropolitana*, which published Babbage's first essay on the economics of manufacturing, and he was a significant member of Babbage's network in the 1820s. Many other examples could be cited.

Although the thesis has stood the test of time remarkably well, and reprinting without revision was justified, I think it is most unfortunate that no index was prepared for the new edition. This omission will seriously hamper its use by scholars. An index would also have been an opportunity to identify the life-dates and occupations of the personae in the text.

Martin Campbell-Kelly
Dept. of Computer Science
University of Warwick
Coventry, CV4 7AL, England

❑ Magnus R. Hestenes and John Todd, ***Mathematicians Learning to Use Computers: The Institute for Numerical Analysis UCLA 1947-1954***, National Institute of Standards and Technology, 1991, 180 pp., paperbound, $12.50. Available from Washington, D.C.: The Mathematical Association of America.

To anyone who, like myself, had even a small part in the INA (Institute for Numerical Analysis), this thorough, well-organized account of its history should prove fascinating. To others (history being history), the seven chapters devoted to the life of INA from 1947 to 1954 may seem dull; but other