when conditions were right, selection plus recombination would restore the original genetic message. But this is to assume that selection can act simultaneously at many loci, which requires that each of the multitude of genetic changes should be separately advantageous. This is precisely the assumption he has rejected in order to conclude that intervention from outer space is needed.

It is sad to see such a creative mind devoted to reaching such an absurd conclusion. It might have been better for the reputation of a great scientist if this book had been left to the decent obscurity of a facsimile edition. ■

John Maynard Smith is in the School of Biological Sciences, University of Sussex, Falmer, Brighton BN1 9QG, UK.

Secrets, codes and decoders

The Code Book
by Simon Singh
Fourth Estate/Doubleday: 1999. 416 pp. £16.99/$24.95

Between Silk and Cyanide: A Codemaker's War 1941–1945
by Leo Marks
Free Press/HarperCollins: 1999. 622 pp. $27.50 (hbk)/£6.99 (pbk)

Charles H. Bennett

Cryptography, in its narrow meaning the art of secret communication, has always been the stuff of intrigue, of military campaigns and assassinations that succeed or fail depending on whether encrypted messages survive the scrutiny of eavesdroppers. Simon Singh's *The Code Book*, a popular history in the tradition of David Kahn's classic, *The Codebreakers* (Simon & Schuster, 1997), covers the subject from Julius Caesar through medieval Arab cryptanalysis, European military and diplomatic ciphers of the past few centuries, the Second World War's Enigma and Navajo Code-Talkers, to today's struggles over encryption on the Internet.

Basic techniques of cryptography and cryptanalysis are carefully explained, as are the archaeological cryptanalyses of Egyptian hieroglyphs and Minoan Linear B. The technical and historical material is enlivened by just the right amount of biographical detail, much of it gleaned from Singh's interviews with living cryptographers.

Leo Marks' *Between Silk and Cyanide* is far narrower in scope, being a memoir of the author's work between 1942 and 1945 in Britain's Special Operations Executive (SOE), in charge of communications with secret agents in occupied Europe.

An older and perhaps even more important branch of cryptography than secret communication is authentication: the art of establishing with whom one is communicating and verifying that their messages have not been altered en route. Indeed, some of the earliest forms of writing may have originated as a side effect of an authentication device — the Sumerian bulla, a sealed clay vessel containing loose tokens representing the kinds and quantities of goods in an accompanying shipment.

Users of secret codes have often been lulled into a false sense of security, with regard to both secrecy and authentication. A famous example described by Singh is the encrypted correspondence implicating Mary Queen of Scots in Anthony Babington's plot to assassinate Queen Elizabeth I of England. Trusting the code's security, Mary used words that left no doubt of her guilt. Elizabeth's cryptanalyst Thomas Phelippes not only broke the code of the intercepted correspondence, but even tricked the plotters into naming the planned assassins by forging, in Mary's hand, an encrypted request for this damning information. Babington, believing the coded message to be from Mary, duly replied, and all were caught and executed.

Much of *Between Silk and Cyanide* concerns the unfortunate consequences of the 'poem code' initially used by the SOE, and Marks' effort to substitute more secure codes, including the provably unbreakable 'one-time pad'. The poem code was insecure because it depended on having the agent memorize a poem. If the Germans could guess the poem, or force a captured agent to reveal it, they could read all the agent's previous messages as well as forging new ones to their liking, which would be accepted by the SOE as authentic. To guard against such forgeries, agents were told to apply certain 'security checks' to their legitimate messages, such as a deliberate pattern of misspellings. But these security checks were often forgotten, and in any case could also be obtained by interrogating the captured agent, who would have to give some answer consistent with previously intercepted transmissions. Many agents chose to carry an SOE-provided cyanide tablet to forestall such interrogation.

The improved codes that Marks eventually put into effect resided not in an agent's memory but on a piece of silk fabric concealed in their clothing or personal effects. On the silk was printed a list of random keys, each of which was to be used to encrypt only one message, then cut off and destroyed. The security check consisted essentially of a secret password, agreed on between the agent and SOE, which the agent would include in each message before encryption.

Because each message was encrypted by a different random key, the previously intercepted transmissions revealed no information about the password itself, so a captured agent would be free to lie about it without being caught in any inconsistency. The remaining unused part of the silk was, of course, also likely to be captured along with the agent, but, lacking its cut-off portions, it neither compromised the previously transmitted messages nor enabled the agent's captors to forge legitimate-seeming new messages without knowing the password.

Meanwhile, the weaknesses of poem code had contributed to a major guessing game, with the British suspecting that many agents had fallen into enemy hands, but continuing radio correspondence with them anyway to avoid alerting the Germans of their suspicions. In one instance the Germans apparently decided they wanted the British to know that a certain agent had been captured, and so staged a Morse code radio drama in which the agent, whom Marks believes had actually been captured much earlier, was heard to begin a normal Morse transmission, which then became incoherent, finally breaking off abruptly with a sound like that of a lifeless hand resting on a telegraph key.

The two authors' styles could scarcely be more different. Singh approaches each of his many topics carefully, balancing human

Ancient Egypt's cryptic hieroglyphs

This 'praenomen', or throne name, of Ramses II is probably describing him as strong, the chosen one of the sun god Re. Many more forms of writing — from cuneiform to Japanese phonetic scripts — are featured in *The Story of Writing: Alphabets, Hieroglyphs & Pictograms* by Andrew Robinson (Thames & Hudson, £9.95).

interest with enough technical detail to make the basic cryptographic principles intelligible to a lay reader. My only regret is that he did not give more weight to authentication and other aspects of cryptography besides secrecy, for example the role of digital signatures in electronic commerce.

By contrast, Marks' technical explanations are not always intelligible, and are sometimes buried in a torrent of colourful language: "The ladies of the First Aid Nursing Yeomanry, otherwise known as the coders of Grendon, had force-fed their eight indecipherables with a diet of transposition keys and all but one of the invalids had responded to treatment. The malingerer was waiting on my desk with a curt note from the Grendon supervisor acknowledging defeat."

Nonetheless, Marks' book makes exciting reading, and is full of information and opinions one cannot find elsewhere. Much of the information in Singh's book can be found elsewhere, but not in such an accessible and enjoyable form. ■

Charles H. Bennett is at the IBM T. J. Watson Research Center, PO Box 218, Yorktown Heights, New York 10598, USA.

A compendium of Victorian culture

The Great Exhibition
by John R. Davis
Sutton: 1999. 238 pp. £20, $36

The Great Exhibition of 1851: A Nation on Display
by Jeffrey A. Auerbach
Yale University Press: 1999. 278 pp. $40, £25

Sophie Forgan

The Great Exhibition occupies one of those hallowed places in history as the first and most successful of its type. It certainly had the stuff of myth in its making. The troubled background of recent revolutionary unrest in Europe, the near-disaster of the architectural design rescued by Joseph Paxton's blotting-paper sketch, the fairy-tale 'crystal' quality of the building which gave it its name, its huge size, the overwhelming number and richness of the exhibits gathered from all corners of the globe, the unsurpassed crowds of orderly visitors, the message of peaceful internationalism and free trade preached by its supporters — all confirm the impression of Victorian Britain at the height of its power.

The material continues to provide an inexhaustible source of anecdotes: for example, the highest tender (not accepted) for servicing the refreshment rooms came from a well-known London brothel-keeper, and the exhibition provided the launching pad for Messrs Schweppes' long involvement in the soft-drinks industry.

HISTORICAL PICTURE ARCHIVE/CORBIS

A heroic national achievement, or an object lesson in taste, mostly bad?

A reassessment is timely. In 1950, Charles Gibbs-Smith viewed it as a heroic national achievement; Nikolaus Pevsner saw it as an object lesson in taste, mostly bad; Asa Briggs argued in 1954 that it was a defining moment in the formation of middle-class political and economic values, although his later work in 1988 viewed it as a compendium of 'things', of Victorian material culture. Others see it as the birthplace of modern consumer culture.

Both authors here take much from previous studies, but have their own perspectives. John Davis is particularly concerned with the political and economic context in which the exhibition evolved, and the way that exhibitions could help transform people's ideas about industrialization and modernity. His analysis of the "modernizing agenda" of the organizers has a distinctly familiar feel. Jeffrey Auerbach, on the other hand, is more interested in the exhibition as a "cultural battleground", in which ideas about national identity were forged. Both argue that the exhibition could mean quite different things to different groups, and that that was an important reason for its success.

Fully half of each book is devoted to the background and preparations for the exhibition. Davis is particularly interesting about earlier French and German exhibitions, the former having an aesthetic focus and the latter a more overtly educational agenda. The road from the original idea for a national industrial exhibition to the international exhibition of the works of industry of all nations in Hyde Park was tortuous and uncertain. The shifts of aim are carefully charted as the organizers responded to the need to gain support and encompass a broader section of the nation. It was a minor miracle that the exhibition took place at all.

Each author has valuable points to make about the choice and layout of the exhibits. Large, piled-up 'trophy' exhibits in the central avenue revealed the organizers' priorities; they generally put art or colonial raw materials in the most prestigious place. Technology and moving machinery were popular, especially working exhibits. Visitors could watch the entire process of cotton production from spinning to finished cloth. Scientific instruments were found in class X, and included electric telegraphs, microscopes, air pumps and barometers, as well as musical, horological and surgical instruments.

Both authors tally the number of medals awarded, either for workmanship (Prize medals) or for novelty of invention or application (Council medals). They conclude, as did some scientific contemporaries, that the British had few reasons for complacency. Auerbach is better informed about relevant work in scientific history, but perhaps he accepts Charles Babbage's 'decline of science' view too readily.

The arguments both before and after the exhibition about the role of scientific and technical education in industrial progress are well aired. And the book recognizes the importance of the chemist Lyon Playfair in organizing the exhibition and helping with the classification of objects. Already a protégé of Sir Robert Peel, the former Tory prime minister, he became a protégé of Prince Albert, helped by the fact that he was also a German speaker and did his research training in Germany.

Although both books tell a similar story, their emphases are different and there is surprisingly little overlap. Davis is more sure-footed in terms of the political entanglements; Auerbach has more material on what people actually thought about the exhibition. One has a real sense of how the Great Exhibition happened and what it looked like, a vast bazaar with palm trees, flowers, organ music and the clank of machinery. Both books provide a treasure trove of pictures, many of them unfamiliar. The exhibition could clearly encompass a wide variety of meanings and interests. Minor quibbles apart, it seems that, rather like the Great Exhibition itself, there is something for everyone here. ■

Sophie Forgan is in the Department of Law, Arts and Humanities, University of Teesside, Middlesbrough TS1 3BA, UK.