

good progress in simplifying living systems to their basics. However, chemists seem to be having a harder time with their bottom-up approach.

The mathematics of Elchanan Mossel and Mike Steel argue that autocatalytic cycles, given relatively simple assumptions, are expected to occur in simple non-living systems. Experiments with *in vitro* RNA evolution are able to test many trillions of sequences simultaneously. Could chemists carry out trillions of reactions simultaneously? Perhaps the new approach of evolving proteins in oil droplets

(*Nature* **440**, 156–157; 2006) could be adapted?

Most of us, most of the time, are solving simpler problems in biology. But we should always be alert to the great problems, such as understanding the processes leading to the origin of life. Given past experience, such great questions will be solved — not by chance but by the prepared mind. This book is a start to preparing that mind. ■

David Penny is at the Allan Wilson Center for Molecular Ecology and Evolution, Massey University, PO Box 11-222, Palmerston North, New Zealand.

research station at Dollis Hill in North London, built it anyway. Flowers triumphantly presented the Colossus to Bletchley Park in January 1944 (not, as had previously been recorded, in December 1943).

“I don’t think they really understood what I was saying — I am sure they didn’t,” Flowers recalled, “because when the first machine was constructed and working, they were taken aback. They just couldn’t believe it! ... I don’t think they understood very clearly what I was proposing until they actually had the machine.”

On 5 February 1944, Copeland writes, the “computer attacked its first message”. Flowers wrote of the epochal event in his diary: “Colossus did its first job. Car broke down on way home”.

But later he grew bitter: “When, after the war ended, I was told that the secret of Colossus was to be kept indefinitely, I was naturally disappointed. I was in no doubt, once it was a proven success, that Colossus was a historic breakthrough, and that publication would have made my name in scientific and engineering circles — a conviction confirmed by the reception accorded to ENIAC ... I had to endure all the acclaim given to that enterprise without being able to disclose that I had anticipated it.”

The team that worked on ENIAC, a high-speed electronic calculator in operation by 1945, conceived of stored programs. Neither ENIAC nor the Colossus was a computer, and it warps history to label them thus. But the key concept of the computer was publicized within months of the war’s end. The British and US scientists who built the first electronic stored-program computers benefited from this openness. The Colossi, in contrast, were broken up, apart from two which ended up at the UK government’s GCHQ listening centre at Cheltenham, and, for all intents and purposes, never appeared in the public world. Only one of these countries has sustained a thriving computer industry. ■

Jon Agar is in the Department of History and Philosophy of Science, University of Cambridge, Cambridge CB2 3RH, UK.

## Secret giants

### Colossus: The Secrets of Bletchley Park's Codebreaking Computers

edited by B. Jack Copeland

Oxford University Press: 2006. 462 pp.

£18.99

#### Jon Agar

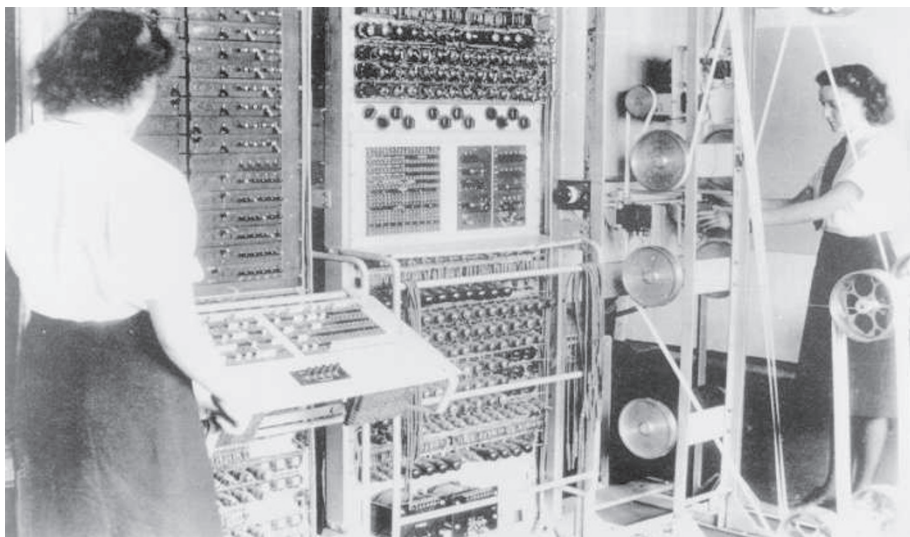
“I find it hard to remember in any detail, after keeping the secret for so long — I tried to blot out of my mind everything that happened at BP, for fear that I might talk in my sleep or under an anaesthetic,” recalled Catherine Caughey, an operator of the Colossus, the wartime electronic cryptanalysis machine. The intense secrecy around Britain’s codebreaking operations of the Second World War was only partially lifted in 1975. Brian Randell, investigating the gap in the life story of Alan Turing between the breathtaking response to Hilbert’s decidability question in the 1930s and the construction of the first electronic stored-program computers in the late 1940s, was allowed to see a clutch of Colossus photographs. For another decade those grainy images, accompanied by terse texts, were the only historical trace of one of the most remarkable machines of the twentieth century.

Only in the 1990s did details emerge. Requests filed under the US Freedom of Information Act prised technical details, compiled by visiting liaison officers, from the American archives. Meanwhile, in Britain, veterans of Bletchley Park finally felt able to speak openly. No longer would they fear, like Caughey, that a trip to the dentist might result in a charge under the Official Secrets Act. Copeland’s valuable collection brings together both technical commentary and personal narratives in an engaging book that will be essential reading for historians of twentieth-century technology and warfare. However, it is also clear that the secrecy of codebreaking did not merely conceal history, but shape it.

The Nazi state used many encryption machines. The Enigma, a cipher machine sold commercially in the 1930s, is now the most famous, a fame shared by Turing, the man most associated with cracking it. But

the higher echelons of Nazi Germany used a more sophisticated machine, the Lorenz SZ40, which was faster, entirely automatic (using Baudot–Murray teleprinter codes), and presumed invulnerable to attack. Eavesdropping stations across Britain recorded radio signals encrypted by the Lorenz SZ40. This stream of data, nicknamed Tunny, was channelled to Bletchley Park. Cracking Tunny was critical to allied success on D-Day: by reading decrypts it was known that Hitler expected only a feint at the Normandy beaches, while the delayed counterattack commands from the Führer to his generals could be read that day in London.

Bletchley Park struggled with Tunny. Two mathematical breakthroughs, by John Tiltman and William Tutte, gave the slenderest of wedges into decryption. But the essence of the problem was speed: only the freshest intelligence would save the most men and matériel. A creaking electromechanical machine, the Heath Robinson, helped in 1943. Fortunately, Tommy Flowers, a skilled Post Office engineer, was shown the problem. His proposal, a fully electronic cryptanalytical machine, met with scepticism even from senior codebreakers. But Flowers, with his team at the Post Office



Cracking invention: the code-breaking Colossus helped Allied commanders intercept Hitler’s messages.