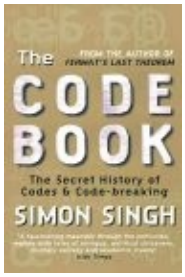
January 2001
News

Cipher challenge cracked



Any readers who enjoyed Simon Singh's "The Code Book", published in September 1999, will know that the author set a challenge at the back of the book, to crack a sequence of ten increasingly difficult encrypted messages. The £10,000 prize Singh offered for the winner of this "cipher challenge" has now been won by a team of five Swedish researchers.

Singh expected that most readers would be able to solve the first few puzzles, that more dedicated readers could hope to solve the next few, and that some fanatics would attempt to solve all ten. The last two stages in particular would require all the artillery at the disposal of the world's most sophisticated code−crackers.

The process of creating the puzzles was extremely time−consuming and exacting, taking two years from start to finish. Singh confided in nobody except Paul Leyland, an encryption expert working for Microsoft in Cambridge who helped him to construct stages 9 and 10 of the Challenge. Singh took secrecy so far that any papers resulting from creating the encoded messages were ritually burnt afterwards in his garden.

The Swedish team worked on the challenge for over a year before announcing their success. They managed to crack the first two ciphers easily using pen and paper. From that point on, they found it necessary to work on computer. Since some of them had studied courses on codes and all were highly computer−literate, some of the stages yielded easily.

Warning − read no further if you want to try the cipher challenge yourself without any information other than that provided in "The Code Book".

However, stage 5 long proved their stumbling block.The team were convinced that the code was some sort of book cipher, maybe with some modifications, but it took them over six months to find the right text to use. In a book cipher, the numbers in the encrypted text are indices to words in a "key text", and the initial letters in these words should give the plaintext. Rather than spoiling things for any readers who may still wish to work on the cipher challenge themselves, let's just say that a knowledge of Singh's own interests and past work was

the starting point for some creative thinking by the winning team.

During their search the team finally resorted to brute force, using a computer program they had written to search for hidden messages inside enormous numbers of texts, some sacred and some profane. They were surprised at just how much seemingly secret information appeared. "What we learned from this was that given enough amount of keytext, seeming improbable amounts of candidate plaintext may emerge." You may have come across the "Bible Code" or any of the other claims of secret encoded information in sacred texts, and have wondered about claims that the probability that such messages could have appeared by chance is tiny. The point is that even if the events you look for have very small probabilities of happening, if you look in enough places for enough improbable events, at least one is highly likely to occur.

Here is a link to a site debunking the Bible codes. If you would like to look at some pro−code sites, here is one from the Jewish viewpoint and another from the Christian viewpoint.

The cipher challenge used both historical and modern codes, in chronological order. The last five stages were intrinsically heavy on computer power. For example, one stage uses an Enigma cipher, with some parameters known and some unknown. As the challenge was intended to be international, the encoded messages were in various languages, some living and some dead.

The final stage was probably the toughest public challenge cipher yet devised. Singh hoped that the attempt to crack it would be a good test of the level of current codebreaking abilities, and this turned out to be so. The winning team broke new ground when they succeeded in decoding it without a supercomputer.

In case this makes you worried about online security − the type of cipher used in this stage is also sometimes used for Internet security − relax. It took several weeks and very powerful computing facilities to crack the cipher − an investment that simply wouldn't be cost−effective for would−be fraudsters.

As soon as the team had solved stage 10 they mailed Simon Singh to let him know, and also faxed his publishers. When, later that day, they received a phonecall from a man claiming to be Simon Singh, who told them that they were not the first people to submit a solution, all seemed lost − until they realised that it was a prank call from one of their friends. Perhaps this wasn't the best prelude to the phonecall they received from the real Simon Singh the next day, who found them very suspicious, and had considerable difficulty persuading them of his real identity!

You can read a complete account of the winning team's code−breaking adventure and find more links to code−related material at Simon Singh's homepage.

Helen Joyce
