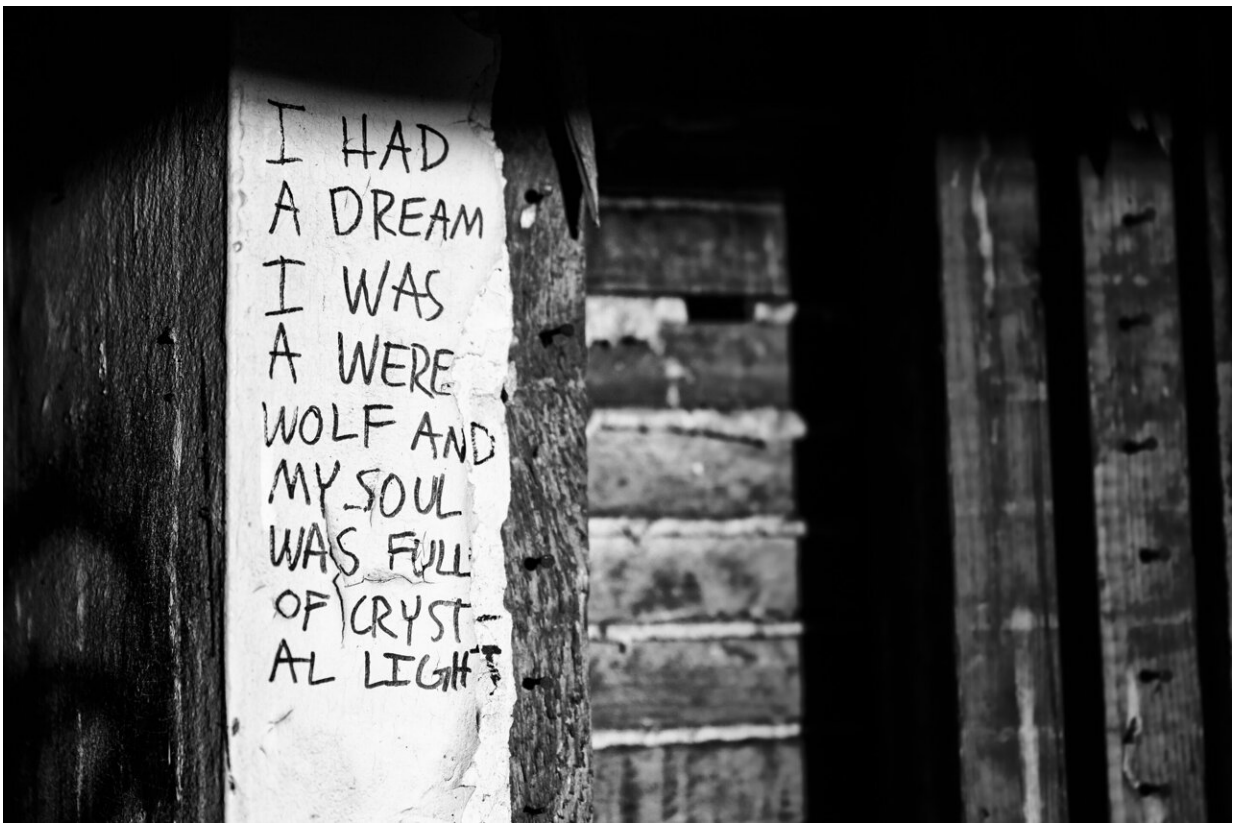
Cryptology from the crypt: How I cracked a 70-year-old coded message from beyond the grave

August 29 2019, by Richard Bean



Credit: Brett Sayles from Pexels

In recent weeks I managed to decrypt a difficult cipher that, despite expert codebreakers' best efforts, had remained unsolved for 70 years.

The code was created by the late Cambridge professor and scientist Robert Henry Thouless, who passed away in 1984. He created it as a "test of survival" to see if he could communicate with the living after his death. Thouless thought if he successfully transmitted cipher keywords to the living through spiritual mediums and the message was received, this would prove he had survived his death.

In 2019, I was more interested in seeing whether computer speed, storage and networking capabilities had advanced enough to break a code that had outlived its maker. After about five days I had my answer.

The cipher text read: INXPH CJKGM JIRPR FBCVY WYWES NOECN SCVHE GYRJQ TEBJM TGXAT TWPNH CNYBC FNXPF LFXRV QWQL

The solution: "A number of successful experiments of this kind would give strong evidence for survival."

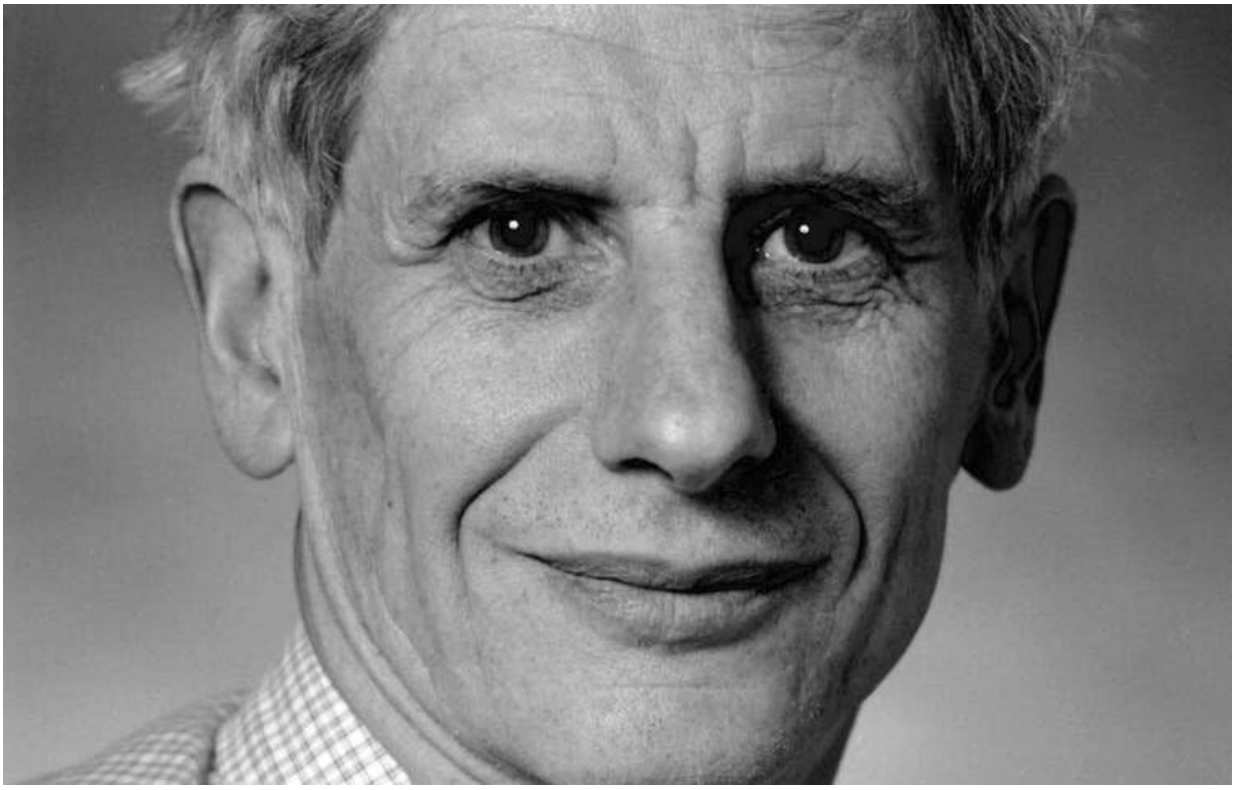
In the name of Psi-ence

In 1882, the Society for Psychical Research was founded in the UK. Its purpose was to study spiritualism, the paranormal, psychic powers and the possibility of life after death. During World War II Thouless became one of its many famous presidents—a list that also included Britain's future prime minister Arthur Balfour and radio pioneer Sir Oliver Lodge.

In the course of his academic work at Cambridge, Thouless devised experiments to test claimants for evidence of "psi"—a term he introduced in his 1942 paper "Experiments on Paranormal Guessing". The word was used to describe all phenomena of "telepathy," "clairvoyance," "precognition" or "extrasensory perception" that could be tested or described.

He considered different ways to create an experiment which could test for survival after death. One test involved an object or message to be sealed in a package so after the author's death mediums could attempt to describe what was inside. A disadvantage here was that the package could only be opened once to check an answer. So in his seminal paper "A Test of Survival", Thouless turned to cryptography as a source of experiments.

He published two ciphers in this paper, which he called Passages. Passage II used a book cipher—a code in which the key comes from some aspect of a book or another text.



Robert Thouless's son David Thouless (pictured) won the Nobel Prize for Physics in 2016. He passed away this year. Wikimedia Commons, CC BY-SA

Cracking Passage II

In August 2019, I produced a table of English letter frequencies in a successful attempt to break an unsolved cipher of the Irish Republican Army, presented in a 2008 book co-authored by California computer scientist James J. Gillogly.

I used the books of Project Gutenberg—a large collection of books scanned or typed by volunteers as the input texts. I wrote a program to check all 37,000 of the English books, using my table of letter frequencies to then score the output text for a solution to Passage II.

After a few days, I found the source book was "The Hound of Heaven" by Francis Thompson, entered into Project Gutenberg in July 1998. This is a most appropriate text to reflect Thouless' religious beliefs, as it is a famous Christian poem.

The lesson from this discovery is that book ciphers can still be a very secure way of encrypting text if the key text can be kept secret, as the only method of solution is to exhaustively test all texts. The most famous example of a book cipher is the Beale ciphers of 1885, which purport to describe the location of hidden treasure in the United States.

In the current age of Project Gutenberg and networked computer systems, Passage II could not have remained unsolved for long.

A poetic approach to code

Thouless's Passage I used the well-known Playfair cipher which was quickly solved after being made. The keyword was "SURPRISE," with the plain text coming from Shakespeare's Macbeth. Solving this was an impressive feat of cryptanalysis in the pre-computer age, and neither the solver nor the method used is known.

In 1949 Thouless produced Passage III using a double Playfair technique with two English keywords instead of one. Gillogly solved it in 1995, publishing an article in "Cryptologia" with Larry Harnisch. The keywords were "Black Beauty" from the 1877 Anna Sewell novel. Naturally, Gillogly tried the text of Black Beauty as the source book for Passage II, without success.

Commenting on Gillogly's 1995 solution, a Society for Psychical Research spokesperson said: "When Thouless devised the test in the late 1940s he could hardly have foreseen the future power of computers."

Due to the growth in computer speed, storage and networking capability, breaking Passage II became feasible. In the present day, quantum computing threatens to make many current encryption algorithms obsolete.

Any future similar tests of "survival" will require the use of some kind of encryption algorithm that is immune to technological advances. As was the case with Thouless, whoever devises such a test will have to take into account that computer power in the future may make the science fiction of today a reality.

Provided by The Conversation