Dear Editor

The paper "A Test of Survival" in the Proceedings of the SPR (vol 48, part 175, pp 253-263, July 1948) by R. H. Thouless proposed the novel idea of testing for survival after death using cryptography.

Thouless considered the many attempts to prove survival after death involving placement of an object or message in a sealed envelope which the depositor, after his or her death, would attempt to describe through a medium. One objection to this test was that the medium might obtain clairvoyance of the contents of the envelope while the depositor was still alive, and another was that the experiment is finished as soon as the envelope is opened.

Thus, his test involved the publication of two "passages" encrypted with different algorithms. He took two plain English text passages, encrypted each passage using different English key words, and published the two resulting ciphertexts in his 1948 paper. His concept was that he would keep the keys secret during his life and attempt to transmit the keys, via medium, to the living after his death. Then the decryption process with a key would result in plain English text if and only if the key had been transmitted correctly or discovered through cryptanalysis. He hoped this would overcome the objections he had described with the envelope test.

He used the well-known "Playfair" cipher for Passage I, which was quickly solved by an unnamed cryptanalyst. The keyword was "SURPRISE" and so Thouless replaced Passage I with Passage III in a later paper, using the "Double Playfair" cipher ("Additional Note on a Test of Survival", *Proceedings of the SPR*, vol 48, part 176, pp 342-343, April 1949).

In 1995, Jim Gillogly and Larry Harnisch, using a computer search, discovered the key phrase for Passage III was "Black Beauty" ("Cryptograms from the Crypt", *Cryptologia*, vol 20, no 4, pp 325-329, 1996).

Passage II was encrypted using a "book cipher". The 74 letter ciphertext was given as "INXPH CJKGM JIRPR FBCVY WYWES NOECN SCVHE GYRJQ TEBJM TGXAT TWPNH CNYBC FNXPF LFXRV QWQL". The encryption algorithm chosen involved taking a sequence of words from an English book, then omitting all second and later repetitions of words already used. This sequence was then turned into a key text of letters. Thouless hoped that the key text derived this way would be close to statistically random. It was then used to encrypt the plaintext by an additive process.

This year I decided to see if the keywords could be found in the English books from the "Project Gutenberg" online library. I looked at all possible sequences of keywords from the library and used English language letter frequency tables to help "score" the output to identify likely keywords.

I discovered that the keywords beginning the poem "The Hound of Heaven" by Francis Thompson resulted in a coherent decryption of Thouless's given ciphertext.

The key words with the duplicates removed were:

> I FLED HIM DOWN THE NIGHTS AND DAYS ARCHES OF YEARS LABYRINTHINE WAYS MY OWN MIND IN MIST TEARS HID FROM UNDER RUNNING LAUGHTER UP VISTAED HOPES SPED SHOT PRECIPITATED ADOWN TITANIC GLOOMS CHASMED FEARS THOSE STRONG FEET THAT FOLLOWED AFTER BUT WITH UNHURRYING

CHASE UNPERTURBED PACE DELIBERATE SPEED MAJESTIC INSTANCY THEY BEAT A VOICE MORE INSTANT THAN ALL THINGS BETRAY THEE WHO BETRAYEST ME PLEADED OUTLAW WISE BY MANY HEARTED CASEMENT CURTAINED RED *TRELLISED INTERTWINING CHARITIES FOR THOUGH.*

The derived key text was then IADDG YSWBU PGPLZ NWIKU ZJSNK BKRJV EXCAW OOJWN XQHYJ NYCWB AFBAB YSQYY SLTKR UNDAA IBQA*Z FNMA*.

The original plaintext was ANUMB EROFS UCCES SFULE XPERI MENTS OFTHI SKIND WOULD GIVES TRONG EVIDE NCEFO RSURV IVAL.

The letter and letter pair frequency of the key text (extended to 78 or 79 words by the italicized letters and words) match those given in the Thouless paper.

The frequency count of the letters in the key text was as follows.

E	H	M	T	V	C	F	G	L	O	P	R	X	D	I	Q	U	Z	J	K	S	W	B	N	Y	A
1	1	1	1	1	2	2	2	2	2	2	2	2	3	3	3	3	3	4	4	4	5	6	6	6	7

Of the 78 letter pairs in the key text, 69 occur once, three twice (BA, KR, WB), and one thrice (YS).

Thouless stated that if the keys were found after his death and were communicated through different mediums to different sitters, this could be regarded as strong evidence for his survival.

The keys were discovered by computer search by two different people, rather than the "traditional" medium approach, and so the evidence for his survival depends on the interpretation of the discovery process, which he could not have anticipated.

In 2012, Klaus Schmeh provided an updated test based on Advanced Encryption Standard (AES) in his book "Nicht zu Knacken". The ciphertext and algorithm are also given on his blog, Klausis Krypto Kolumne.

Research Fellow, RICHARD BEAN
Faculty of Engineering and Information Technology
The University of Queensland
Brisbane, Australia
Email: r.bean1@uq.edu.au