Secret Manhattan Project ciphers finally solved

While working on the creation of the world's first atomic bomb, mathematician Paul Olum challenged his colleague, the distinguished theoretical physicist Richard Feynman, to solve his two ciphers – Olum 1 and Olum 2. Feynman failed, and the ciphers went unsolved for more than 75 years. Paul Relkin, an American software developer and cryptanalysis enthusiast, has recently published the first successful decryptions of both ciphers. His innovative algorithm for the cryptanalysis of transposition ciphers can be used to decode similar classes of encrypted messages.

During World War II the US initiated a top-secret project with the aim of creating the world's first atomic bomb. This initiative, known as the Manhattan Project, located in Los Alamos, New Mexico, involved several experts, including the distinguished theoretical physicist, Professor Richard Feynman. Feynman was particularly proud of his ability to solve word and mathematical puzzles at speed. He proclaimed he could 'solve any problem that could be stated in 10 seconds to within 10% accuracy in one minute'. His Manhattan Project colleague, the mathematician Paul Olum, frequently challenged Feynman with complex mathematical problems, which Feynman usually managed to solve. However, Olum created two ciphers, or coded messages, that not only stumped Feynman but remained unsolved for another 79 years.

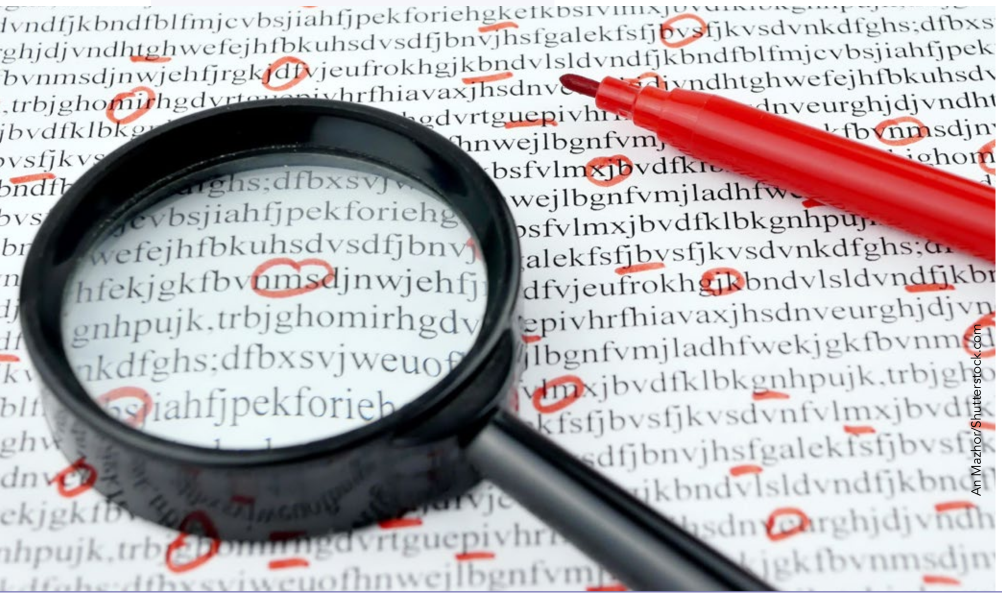
OLUM 1 AND OLUM 2

The ciphers, known as Olum 1 and Olum 2, remained stored in the archives of the California Institute of Technology (Caltech), together with Feynman's attempted solutions. Then just last year Paul Relkin, software developer and a founder of Mapscallion LLC, finally decrypted both ciphers using an innovative decryption algorithm. In two recently published papers, Relkin describes the history behind Olum's ciphers and explains his successful decryptions, using a new algorithm that can be employed to decode similar classes of encrypted messages.

Why did the Olum 1 and Olum 2 ciphers remain unsolved for more than 75 years? Relkin explains that some ciphers are relatively straightforward to solve as they obey some well-known encryption methodologies. Others, however, evade decryption for many years, either because they use novel techniques or, more commonly, because they deploy new variations on standard encryption methods. Relkin believes that Olum employed some ingenious variations designed – successfully until now – to defy conventional decryption tactics.

THE FEYNMAN CIPHERS

Relkin came across the Olum ciphers while researching another set of ciphers, known as the Feynman ciphers. These also dated back to Feynman's time at Los Alamos, but their author is unknown. The first of the three Feynman ciphers was decoded in 1987, revealing a passage from Chaucer's Canterbury Tales. In 2017, while performing a computer-assisted bibliographic analysis of the many editions of the Canterbury Tales published over several centuries, Relkin discovered something critical to his project; the spellings in the Feynman 1 cipher message were unique to a 1930s edition of the Tales transcribed by one FN Robinson. Could ownership of an edition of the Robinson transcription identify the author of the Feynman 1 cipher?


An Mazhor/Shutterstock.com

Olum 1 Cipher

VEWLJNBBELQFWSXHBUSWAIBYQAEQSIGHOVNBSNBVLNWX
ABIQIUBGBICYQFXCEVBWXWBSNGWVEVLHWDHBILMHBLNSGBHSNX
SXBHLQCBOCSOBVWMXFNCWPAGGNEUWGAIBVWIFYWFGGQFE
WMPQIXXWSEWVIHABEBWJXOHAFQLBBNIBHAIVJNSHCWX
PCYUGGOBDWAXBHBWINXWSNJGWVAFOXBLMWAEBPB
BWXCRBWBVLHIJAJINOWXDBIBQCGYWFXHCQAIBCWN
GCSCSHBNAVIEWDHIBLHEBVVYYSLRQPQVCQIWXQEDQBI
WXWEAPBHVWSBSBWXVAVHBWFPUHBYWVNBYIOQWAIFYQ
DXDBICLBWYCNEAIBWINBBWAACIQICVWIXQVCBLHXI
BVLAHMFOBXSIXOQBUEPCOVAWMOFVNCWAPGGNEE
UWAIWXAWAEEWOLEWESHWFXHEGHCIVBHSWJOILA
WFNDDFQWDHILVHBBWAIQBIOUXWSBNIGWVXVQDBVA
WIFGWXNVWEPUHYWDBHIMLHBLPNMWVHYPBYWBHAMF
XXOSCVNBHCWVNYBIOQWAVIYBQXDLBNDVWCCGNAABXQV
WDBHEILHJBLNVWVBHAFXOBCBMYWINSBVOQWLOHC
GGWFBBNSYMDQUBXWSNGBWVWAIVGXHBOJWDBHIB
VLHMWBIHINJGNBFBHDQBIWIBOBJOHUHVYLQMYWSNS
IDFWDDVWEWVHYDLWVWGPWSSHABILBWYWJLHDXXSH

Olum 1 Solution

Arrangements have been made effective Monday, August 2 to facilitate and safeguard the delivery of miscellaneous items purchased in Santa Fe or shipped in from the outside. Paid purchases made in Santa Fe may be directed for delivery to the Santa Fe office, 109 East Palace Avenue, where they will be picked up by our truck and transported to the site. Shipments from the outside may be addressed as heretofore to P.O. Box 1663, Santa Fe. This applies to parcel post, freight and express.

The Olum 1 cipher (above) and its solution, identifying protocols for mail delivery to the Manhattan Project's Los Alamos facility (right).

At this time Relkin happened upon a description of Feynman's papers in the Caltech archives that also referenced Olum's ciphers, and he turned to the Olum ciphers themselves, together with Feynman's notes on his attempts at decryption.

SUBSTITUTION CIPHERS

Feynman had thought that Olum 1 was a substitution cipher, where letters are replaced by other letters, numbers, or symbols that correspond with an encryption key. But Relkin found the usual techniques for solving substitution ciphers unsuccessful and began to ponder if a clue lay in the first Feynman cipher, which was encoded in reverse order. He implemented an identical letter reversal on Olum 1 and created a solver program for a monoalphabetic substitution cipher in the coding language Python, that employed a hill-climbing algorithm – a typical substitution cipher decryption method using the frequency distribution of letters in the target language. Running this program on the reversed text revealed some letter sequences that were potentially English words, but they appeared to have random letters implanted among them.

Olum employed some ingenious variations designed – successfully until now – to defy conventional decryption tactics.

In fact, Relkin discovered that Olum 1 involved a mixture of techniques, including methods used in substitution ciphers, and in null ciphers that mix random letters into cipher message. What initially appeared to be random letters arbitrarily scattered throughout Olum 1 had actually been deliberately placed at intervals that corresponded to the digits in the square root of 2 – a nice mathematician's twist. Removing the random letters and applying the correct key revealed a message that identified the protocols for mail delivery to the Manhattan Project's Los Alamos facility as well as two addresses that were classified as top secret for the project in Santa Fe. The Los Alamos National Laboratory Research Library couldn't find the original message among the Manhattan Project records, but it's likely it dates from a change in mail-delivery systems in 1943.

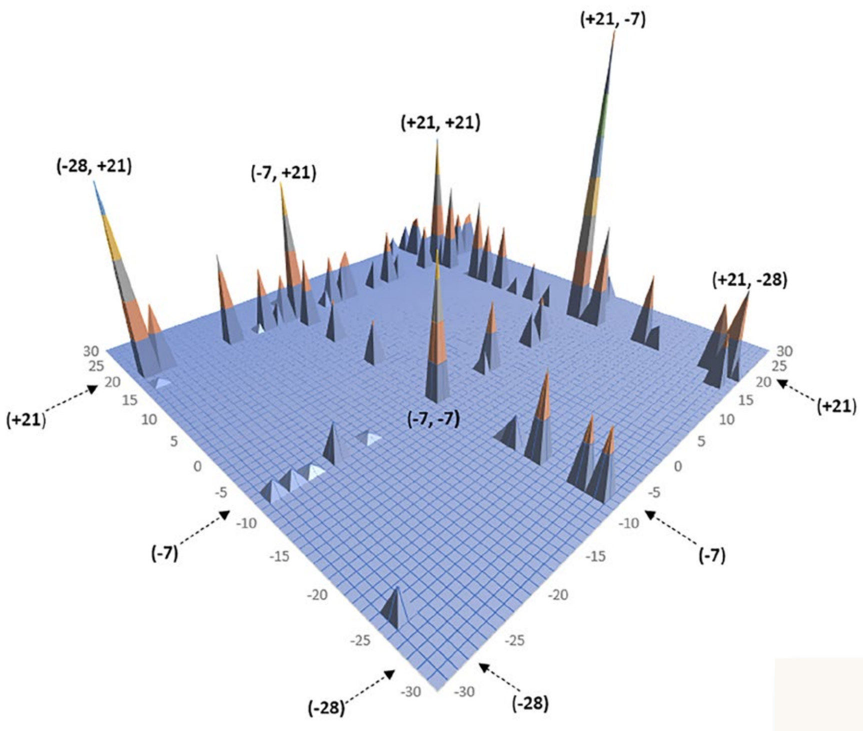
The author of the Feynman ciphers, however, remains a mystery. Relkin learned from Paul Olum's son that the mathematician's copy of the Canterbury Tales was not the Robinson edition. This did not entirely rule out Olum as the author of the Feynman ciphers, but it did not support that conclusion either.

TRANSPOSITION CIPHERS AND ROTATING KEYS

Relkin then turned his attention to Olum 2, which required a different approach. In contrast with Olum 1, the letter frequencies suggested to Relkin that Olum 2 could be a transposition cipher, in which letters are transposed, or moved, to various positions within the code according to a key. Again, he tried several standard decryption methods, but neither a clear message, nor a key, became apparent. These trials led Relkin to embark on a new approach to frequency analysis that would identify the possible transposition intervals. He developed a novel cryptanalysis method that considers the frequencies of two- and three-letter sequences – bigrams and trigrams – of the English language as well as those that randomly occur in shuffled cipher text. He then developed a program that examined all possible intervals of transposition and helped select the intervals most likely to be non-random.

Relkin created a three-dimensional plot, the peaks of which depicted the most probable transposition intervals. When

OLUM 2 TRIGRAM INTERVALS



Relkin's Trigram Interval Plot. The positions of the peaks assisted in identifying several candidate transposition intervals for the Olum 2 cipher. When these intervals were used to transpose the Olum 2 cipher text, they produced three-letter sequences (trigrams) that are statistically more likely to occur in English text than at random. All of the highest scoring intervals were divisible by seven, which provided a clue that the letters of the cipher were arranged in seven-letter rows for encryption. The arrows indicate lines containing multiple high-scoring peaks. These lines occur when the trigrams generated by those transposition intervals contain at least two out of three letters in the correct order.

these intervals were applied to Olum 2, English words were revealed in certain segments of the cipher. He then realised that the cipher message had been split into sections of 35 words and was able to use a rotating key, where the transition intervals altered from one section to the next, to decode the entire message. Finally cracking the code, Relkin revealed Olum 2 to be a passage describing a religious believer's frustration in trying to convince an atheist of the merits of religion. It's known that Olum was an atheist, but the source of the passage itself is another remaining mystery of his two ciphers.

> ***Relkin's innovative methodology for the cryptanalysis of transposition ciphers overcomes several limitations of the algorithms previously available.***

Transposition ciphers were widely used during World War II and the ensuing decade and most used a uniform transposition key. In one variation, however, the cipher message is broken into sections each employing a different key, and these are known as permutation ciphers. The encryption key for each section is often selected at random, but Olum generated the sequence of keys by rotation. The use of multiple encryption keys is now recognised as a way of making transposition ciphers more robust.

A GENERAL UTILITY FOR SOLVING CIPHERS

After his success with the Olum ciphers, Relkin applied his method to other, previously solved transposition ciphers and successfully identified the transposition intervals in each case. These findings indicate that his approach offers a general cipher decryption strategy for transposition ciphers with both single and multiple keys. Moreover, his innovative methodology for the cryptanalysis of transposition ciphers overcomes several limitations of the algorithms previously available.

In the end it was Relkin's deductive reasoning and use of computer analyses that broke the codes. Olum's ciphers were particularly tricky: 'Their author incorporated some clever twists on standard encryption methods that he designed to defeat the commonly used approaches to decryption,' says Relkin.

Solving these ciphers sounds like a fun pursuit but, as Relkin emphasises, 'it can also provide a unique window into historical events and an opportunity to discover new decryption methods that are potentially relevant to both historical and present-day data encryption strategies.'

Olum 2 Cipher

EEIOLCNTPATIILMNIHGUTIG
LFOOOHRBYSCDEYGSEEIEELMERS
BITCBAANEITGDSDDOURDMSIO
MHESELEDNSRRNHNINATONWA
EDSYROWHEDRTRASVAWHEODES
ETVIFNIEHETOIGIELNIITONA
RTHTHLEULIITAISLSUNFCEAI
NIELSLTLBPSNTMTIHSDSIHTR
EIENDUETHHIOMEIIASTVHPFYG
SORNEEIIET

The Olum 2 cipher (top) and its solution (below), describing a religious believer's frustration at their efforts to convince an atheist of the benefits of religion.

Olum 2 Solution

The impregnability of his logic could not be denied. Yet, logic must be regarded as mistress only in her own domain. When she dares disagree with the revelations of divine intuition, then fallacies result. All this I told him, but he persisted in his atheism in spite of everything.

Behind the Research

Paul Relkin

E: pwrelkin@mail.roanoke.edu **W:** mapscallion.com

Research Objectives

Paul Relkin has broken the code of the decades-old Olum ciphers, and in the process developed a novel cryptanalysis method for decrypting transposition ciphers.

Detail

Bio

Paul Relkin is a software developer and a founder of Mapscallion LLC. He has served as Mapscallion's chief technical officer since 2015. His interest in decrypting unsolved historical ciphers follows from his work on computer encryption techniques and a fondness for history.

Collaborators

I am grateful for the many helpful discussions and editorial assistance provided by Dr Norman Relkin. I thank Dr Ken Olum for his thoughtful comments and recollections pertaining to his father, Dr Paul Olum. I appreciate the assistance of Dr Peter Collopy, University Archivist at Caltech.

References

Relkin, PW, (2021) Solving the Olum 1 cipher. *Cryptologia* [online]. doi.org/10.1080/01611194.2021.1974124

Relkin, PW, (2021) Solving the Olum 2 cipher: a new approach to cryptanalysis of transposition ciphers. *Cryptologia* [online]. doi.org/10.1080/01611194.2021.1992686

Relkin, P, (2017) The Feynman challenge ciphers and Geoffrey Chaucer. ciphermysteries.com/2017/04/30/feynman-challenge-ciphers-geoffrey-chaucer

Morrison, J, (1987) Feynman ciphers. groups.google.com/g/sci.crypt/c/RAxvau5mxJ4

Personal Response

What initially sparked your interest in cryptography?

" As a software developer, my work often involves encrypted and compressed code. Finding faster and more efficient means of encryption and decryption has been a gratifying challenge for me. This, combined with a longstanding interest in unsolved mysteries from the past, led me to learn about cryptography and try my hand at solving some famous historical ciphers. "

Victor Moussa/Shutterstock.com
SkillUp/Shutterstock.com