Finally solved Project ciphers

Secret Manhattan Project ciphers finally solved

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 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 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.

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. Relkin could own the 1930s edition of the Robinson transcription identify the author of the Feynman 1 cipher?

At this time Relkin happened upon a description of Feynman’s papers in the Caltech archives that also referenced Olum 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 1 Cipher

VEWLNBBGDCFXYHSBVTAGQIEGQOHNVBSBNLWVNX
ABHUDBGICFOXCVYHBWGBVWLVHWDHBLMHHNSGBHSHNX
SBXLHCQCOSBQBMXWNCWPGAGNEWBAIWFVWFGGEEF
WMGPOXZXXW9H1AHBBEBZXRXOHAFQLBHBIBAH1V5H5CHX
PYUGQBDWAXHBH8XW5WNSJWVQAFOXBFMLWBABFPW
BYCVXCBWVMBVCDGXYCGQYFXHQC8IBCYN
GCCSCHBNAVWDDHBLHBEVY5LYRQPCWGCXQIDEBDI
WXWWEAPBHVWWSBBSXVXAHFDQPPBFYVYNYQBOQAFYQ
XDBIC8LBYC8NEB1WYBHBAWAC1QCVXWQCBLBXIX1
BYLAMPMFBOSXQ00BEPC0AYMWG00VWICWAGPGNNE
UWA1XWWAEAVEWLEW5ESWFFFHCGBYVSWJ0WIA
WFNDQDOGDWHLHBB8AQIHOUXVSN1GWYXQVDBA
WIFGWX1WXWEPHUYWHDHBLHLPNMLWYHFYWBYHBAFMF
XXOYPBHCVNHWYDBQDQWYFQOYDXMLBNDYWFCGGANABKV
WDBHEILJUBLNVWWLFQHAF shocked BFCM8MYWINSBQWLV0HCH
GGWFBXSN5MDQUBX5WSGBWVWYGQX8H0JBDHIBB1
VLMHIIBHN1JQNBFDQBDI8RBI0BCOJQHU8FLQQMTWSTNS
IDFWDDWEVWHYULWVWGMWSHABLBWYLUDDLXSH

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

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, and outside may be addressed as herebefore 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.

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

Paul Relkin

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

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.

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

Olum 2 Cipher

EEIOICNTPATILHMNHIGHTGF
LFOOGHBRSYDEGSEIEELMERS
BITCBANAEIPTGDDDOURDMISO
MHSELENSRHHNHNATONVWA
EDSYROWREDTRASAVHEODES
ETYIFHMHEOTGIENLTONA
RTCYHLLEULITALSUFNCEAI
NIELSLLITPSNMTSHDSNHR
EIENDUETHOMIEMAISTAIVYHPYF
SORNEEIET

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

Research Objectives

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 Collop, University Archivist at Caltech.

Victor Moussa/Shutterstock.com

www.researchoutreach.org

Paul Relkin


Morrison, J, (1997) Feynman ciphers. groups.google.com/g/challenge-ciphers-geoffrey-chaucer

References


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.

Personal Response


text