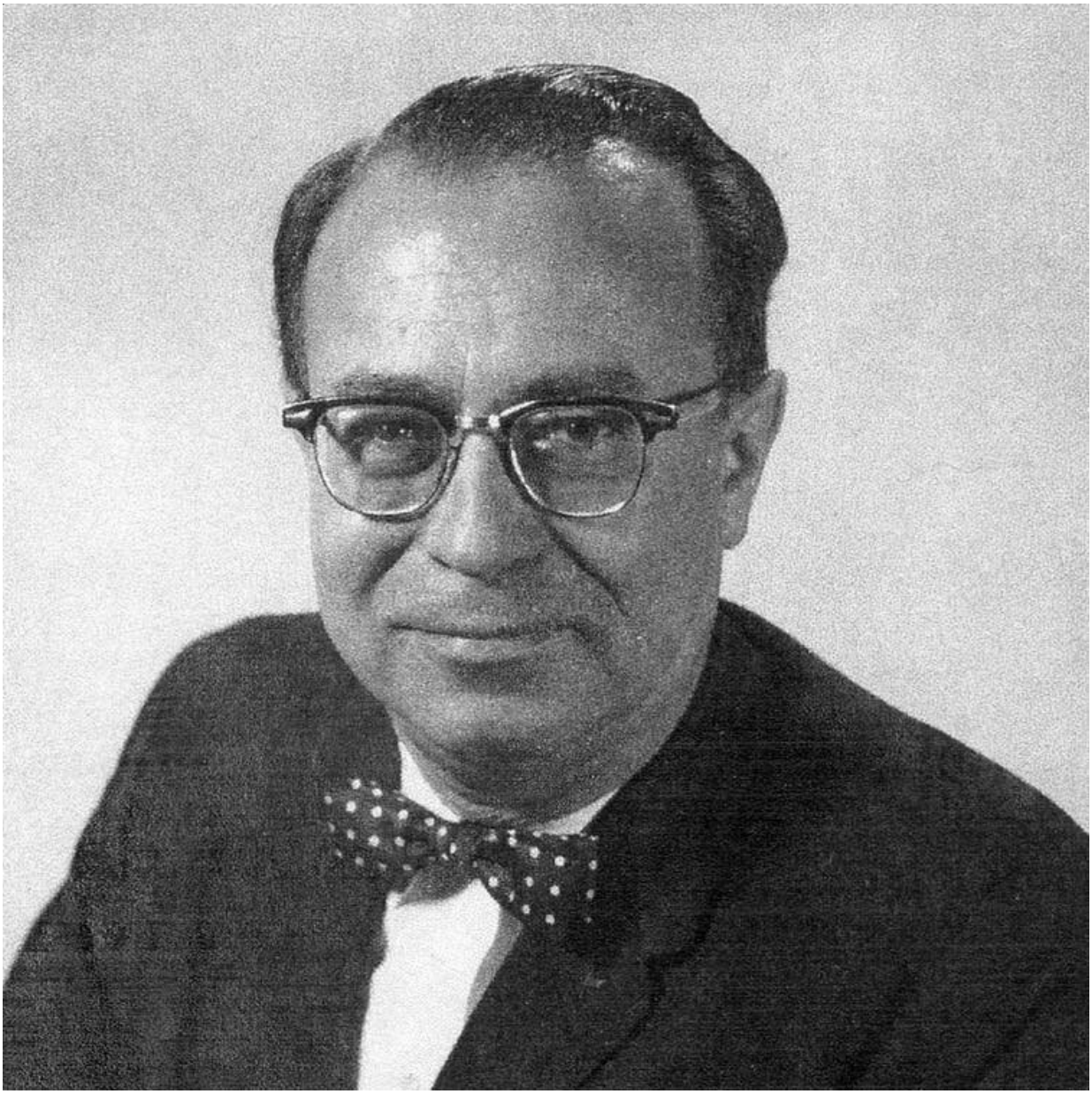
Declassified Cold War code-breaking manual has lessons for solving 'impossible' puzzles

May 31 2021, by Richard Bean



Lambros D. Callimahos, the author of Military Cryptanalytics. Credit: NSA

The United States National Security Agency—the country's premier signals intelligence organization—recently declassified a Cold War-era document about code-breaking.

The 1977 book, written by cryptologist *Lambros Callimahos*, is the last in a trilogy called *Military Cryptanalytics*. It's significant in the history of cryptography, as it explains how to break all types of codes, including military codes, or puzzles—which are created solely for the purpose of a challenge.

The first two parts of the trilogy were published publicly in the 1980s and covered solving well-known types of classical cipher.

But in 1992, the US Justice Department claimed releasing the third book could harm national security by revealing the NSA's "code-breaking prowess". It was finally released in December last year.

Lessons for code-breakers

A key part of Callimahos's book is a chapter titled Principles of Cryptodiagnosis, which describes a systematic three-step approach to solving a message encrypted using an unknown method.

An intelligence agency might intercept thousands of messages made in a target country's ciphers, in which case they already know the method. But if they encounter something new, they must first and foremost figure out the encryption method, or risk wasting time.

As Callimahos details in his chapter, the code-breaker must begin with

all the necessary data. This includes the ciphertext (the enciphered text hiding the real message), any known underlying plaintext (text from before the encryption was applied), as well as important contextual information.

For puzzles, part of the plaintext may be given to help the solver. With confidential military messages, the solver may suspect certain words have been encoded into the ciphertext, based on past knowledge. For example, there may be key terms such as "message begins," "message ends" or "secret," or specific names, places or addresses.

The code-breaker then arranges and rearranges the data to find non-random characteristics. After this, they can recognize and explain these characteristics. In other words, they've found the cipher method.

Applying these steps is an example of "Bayesian inference". The code-breaker considers the weight of evidence and guesses the likely cause of an observed effect.

The Zodiac and Kryptos ciphers

Last year, the famous 1969 Zodiac killer cipher, known as Z340, was solved by an international team of code-breakers after 51 years. The team carefully and systematically developed a list of observations over many years.

Using a process called Monte Carlo sampling, they tested whether the patterns observed in the ciphertext were random or not. Together with a detailed knowledge of the context of the cipher and a solution for a previous cipher by the Zodiac killer, they correctly guessed the encryption method used.

One of the Zodiac cipher solvers, David Oranchak, said in his opinion it

was "at about a seven or eight out of ten in difficulty to decipher."

Similarly, US artist Jim Sanborn's famous Kryptos sculpture, located at the Central Intelligence Agency, has long confounded attempts to unlock its code. It contains four encrypted passages to challenge the agency's employees. The final passage, known as K4, remains unsolved after 30 years.

When Kryptos's code designer Ed Scheidt was asked to rate the cipher's difficulty, he estimated it as being around a nine out of ten on the same scale. He said his intention was for it to be solved in five, seven or maybe ten years.

So what has made K4 so difficult? For one, with only 97 letters the passage is very short, meaning less data and fewer clues. The enciphering method used to create it is unknown, and there's little context as to how it may have been enciphered.

One classic book on mathematical problem solving, How to Solve It by George Pólya, suggests a general principle for solving any problem is to refer to a similar problem that has already been solved. This principle applies in the historical puzzle world, too.

However, Scheidt also noted there was a "change in the methodology" as the Kryptos message progressed—done intentionally to make it increasingly difficult.

It could also be that Sanborn accidentally introduced an error in K4 during the construction of the Kryptos sculpture, which would mean solvers are wasting their time. Making a mistake during enciphering can render a puzzle impossible to solve. In such cases, the creator should admit this to prospective code-breakers.

Lessons for code-makers

Looking at a puzzle from the code-maker's perspective is important. A skilled code-maker should leave at least some non-random patterns in the cipher, so as to not make their puzzle impossible.

Imagine you've created a puzzle, but after many years your intended audience has failed to solve it. If you still want it solved, you have to start releasing clues. Some puzzles, such as the 1979 book Masquerade and the Decipher Puzzles, were only solved after clues were released.

However, if nobody has solved your puzzle even after you release many clues, then the code is simply too tough to crack.

Cryptographer Helen Fouché Gaines wrote about this in her 1939 book. The creator of such a puzzle, she said, "fails to submit material in proportion to the amount of complication he has introduced."

This means you may have to eventually reveal the method you used. One example is a complex algorithm known as Chaocipher. While Chaocipher messages were designed to be highly difficult, they're virtually impossible to decipher without knowing the method.

A 2007 NSA presentation about Kryptos mentions how "dozens" of agency staff have failed to solve K4. But as more historical texts become declassified and our computational, storage and networking capacity grows, perhaps one day an amateur code-breaker will crack the elusive passage—and not an agent of the NSA.

Provided by The Conversation

Citation: Declassified Cold War code-breaking manual has lessons for solving 'impossible' puzzles (2021, May 31) retrieved 24 April 2024 from https://phys.org/news/2021-05-declassified-cold-war-code-breaking-manual.html