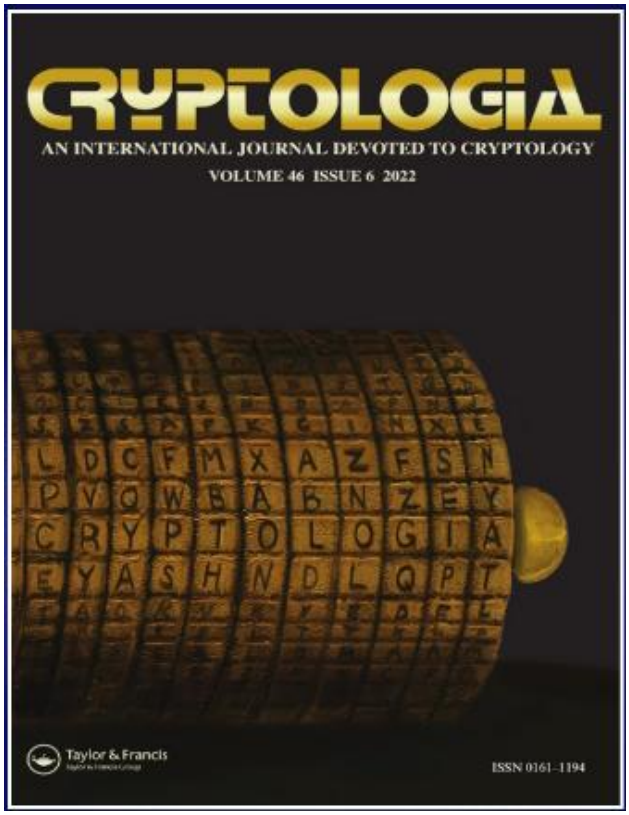
Kaczynski's Ciphers

Jeanne Anderson



27 May 2015

Contents

Abstract

A child prodigy and Harvard University graduate turned serial killer, Theodore Kaczynski—now better known as the Unabomber—constructed elaborate cipher systems to encrypt his thoughts and emotions. His personal journals contain enciphered details of his life, his beliefs and feelings about society, and his crimes. This article introduces the Unabomber's cipher systems and through his use of these systems gives a brief glimpse into a fascinating mind that crossed the line between genius and madness.

1. Background

Now associated almost exclusively with his violent acts as the Unabomber, Theodore Kaczynski had previously been known for being a child prodigy, a Harvard University graduate at age 20, and a PhD-holding mathematics professor at the University of California at Berkeley. His transition from such highly-regarded designations to that of a bomb maker and serial killer has drawn many to question what was transpiring inside his mind. Kaczynski's journals provide a fractional glimpse of the answer to this question, as they contain thoughts so private that he felt the need to devote considerable time to creating and using complex cipher systems to mask them.

The Federal Bureau of Investigation (FBI) first encountered Kaczynski's work in 1978 after a homemade bomb exploded at a Chicago university; however, his identity as the bomber would remain unknown for nearly two decades. This attack commenced a reign of terror that resulted in three deaths, 24 injured victims, and what, at the time, would be "the most expensive manhunt in United States history"[1]. Since Kaczynski's bombs mainly targeted universities and airlines, the FBI labeled the case UNABOM (UNiversity and Airline BOMbing). The media then modified this case title slightly, and the infamous "Unabomber" title was born.

In 1995, despite having successfully evaded arrest for nearly two decades, the Unabomber mailed a manifesto to two newspapers discussing his thoughts on the Industrial Revolution and his motives for the bombings. This turned out to be the key to breaking the case. The manifesto was published in *The Washington Post* and *The New York Times* in hopes that someone could identify the author. Kaczynski's brother, David, recognized Theodore's unique writing style and notified the FBI. David's claims were checked, and Theodore fit the FBI's pre-established profile almost perfectly.

On 3 April 1996, Theodore Kaczynski was arrested. After 17 years and 16 homemade bomb attacks, the Unabomber had finally been caught. FBI cryptanalysis testimony on Kaczynski's enciphered journals became unnecessary, as Kaczynski pleaded guilty to all charges. This guilty plea saved him from a potential death sentence. Kaczynski is currently serving a life sentence without the possibility of parole at the Federal Administrative Maximum Facility in Florence, Colorado.

[1] Douglas, J. and M. Olshaker. 1996. Unabomber: On the Trail of America's Most-Wanted Serial Killer, New York: Pocket. Page 31.

2. Kaczynski's Enciphered Journals

When FBI agents raided Kaczynski's cabin in the backwoods of Montana in 1996, they seized bomb components, a live bomb that was ready to be mailed, and tens of thousands of pages of handwritten journals written between 1969 and 1996[1]. Among these journals were several that were partially or entirely enciphered using systems that Kaczynski had created.

Kaczynski's journals contained systems of encipherment that may not have been solved apart from the corresponding instructions and "keys" found alongside them. Because Kaczynski did not intend to use his encipherment systems to pass messages to anyone else, there was no need to develop mechanisms to share the keys or the rules of the system. The only requirement was for these systems to make sense in Kaczynski's mind, thus they could be as convoluted and operationally impractical as he desired. These freedoms eliminated numerous constraints normally associated with developing and effectively using a system of encipherment.

Within the journals are two distinct encryption systems. Kaczynski labeled these systems Code # I and Code # II. While elements and intricacy of these systems of encryption vary, Kaczynski's intentions in using them were the same: His goal was to keep unintended individuals from accessing his thoughts.

[1] Graysmith, R. 1997. Unabomber: A Desire to Kill, Washington, DC: Regnery Publishing, Inc. Page 444.

3. Code # I

The first and more complex encryption system, Code # I, is written in a notebook that Kaczynski called Notebook X. Notebook X is composed as a dated journal containing plaintext journal entries intermixed with portions of ciphertext. This system utilizes numerous safeguards, including the use of intentional misspellings and encryption errors, meaningless punctuation, nonsense words, and Spanish and German text intermixed with English plaintext and ciphertext. Kaczynski also chose to omit and add word breaks at random and use nulls throughout his enciphered text.

Enciphering or deciphering Code # I requires a 54 x 42 matrix that Kaczynski created specifically for this system (Figure 1), knowledge of the starting point for the matrix, the order of the unscrambling sequences used for determining the route used on the matrix (Figure 2), and a list of meanings where the numbers 0-89 equate to various words, letters, groups of letters, nulls, spacers, and punctuation (Figure 3).

To begin deciphering Code # I, the unscrambling sequence must be compiled. This sequence will essentially serve as the additive to the ciphertext in the journals that will compose step 1 of Code # I. To compile this unscrambling sequence, the Figure 1 decoding matrix will be extracted in different orders to provide varying additive strings. This is a positive aspect of Code # I, as it does not require numerous matrices, but rather, one matrix can be reused in varying orders, and the size of the matrix keeps this reuse from being too much of a security flaw in the system. To find the starting point within the matrix, the third ciphertext character from the beginning of a section of ciphertext is to be extracted; the first two characters of the beginning section are nulls. This position for extraction must be known prior to beginning decryption, as it provides the row on which to begin extracting the unscrambling sequence. Once the beginning point on the matrix is known, Figure 2 provides the varying orders in which the entire unscrambling sequence will be extracted from the matrix. The sequence begins left to right, top to bottom (Figure 2, first step). Once the bottom-right corner of the matrix is reached, the matrix is reused according to the second pattern by beginning in the top-right corner and extracting top to bottom, right to left. The matrix is then used in two additional patterns (see third and fourth patterns of Figure 2) before the initial extraction pattern begins repeating.

Next, the separate portions of ciphertext are strung together and considered one. Once joined, the ciphertext (omitting the third character, which served only to provide

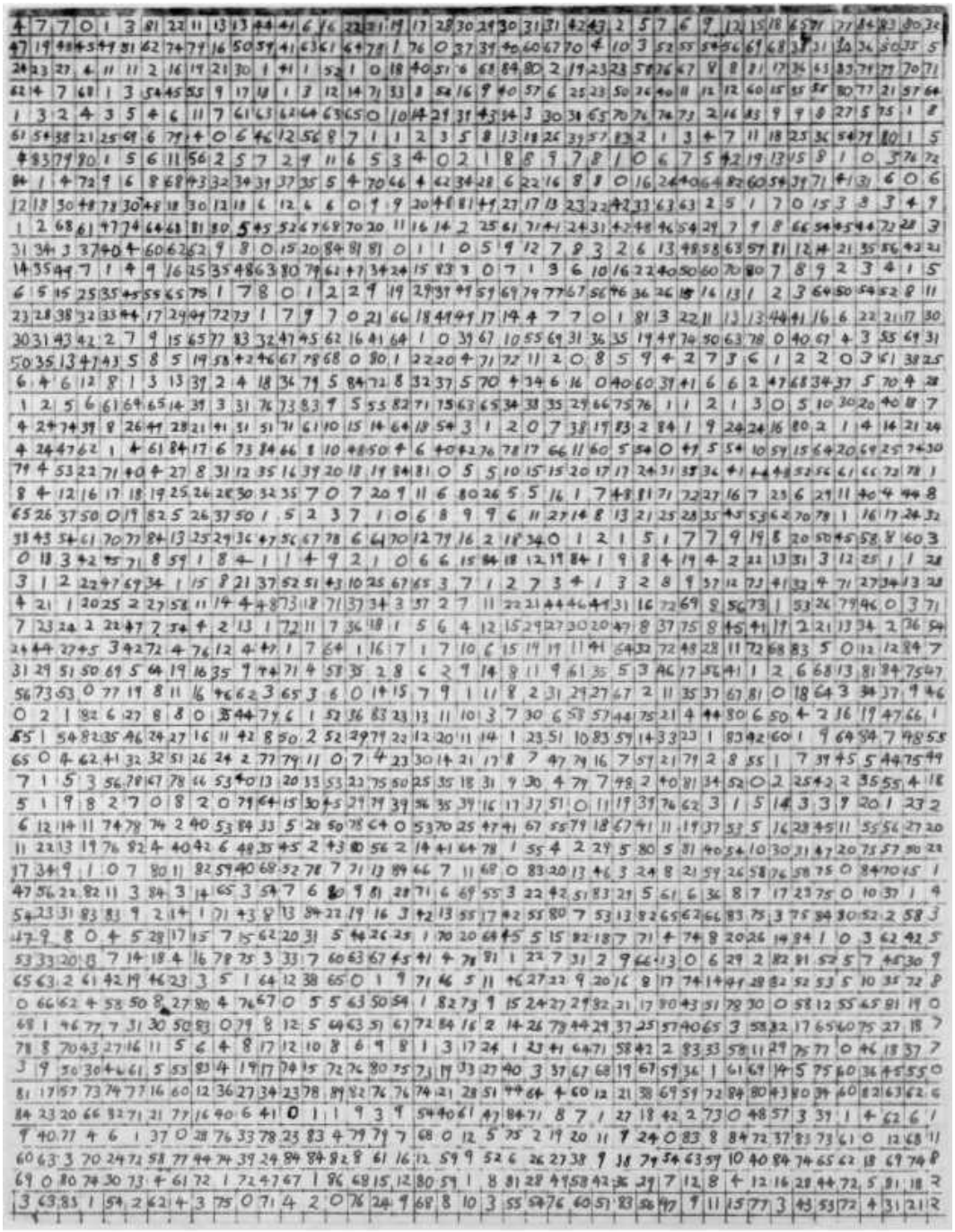


Figure 1. Matrix for Code # I.

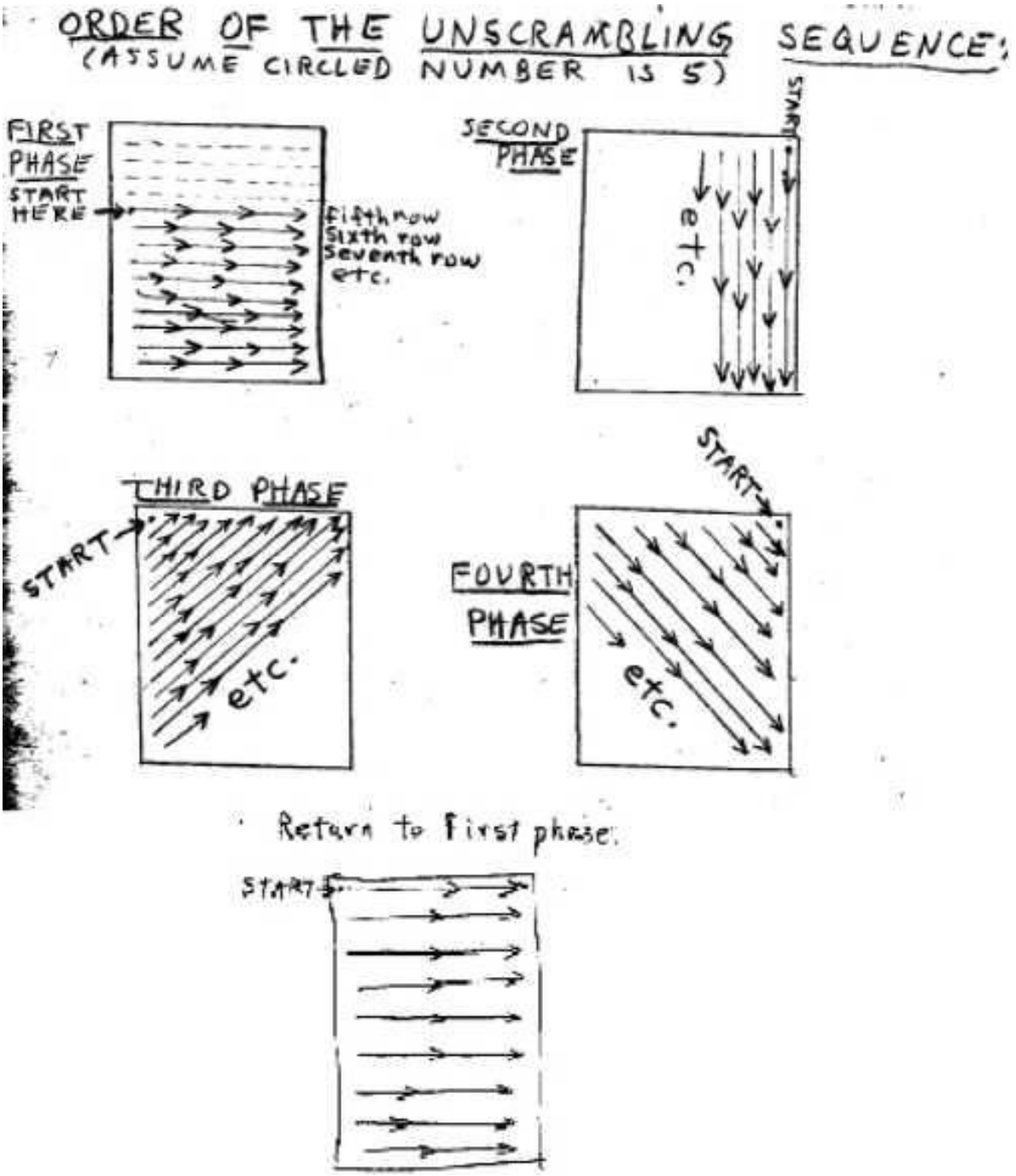


Figure 2. Unscrambling sequence for Code # I.

the starting row for the matrix) can be added to the unscrambling sequence, modulo (mod) 90. While adding, an additional step is incorporated where punctuation marks and any numbers from 90 to 99 are disregarded along with their corresponding character in the unscrambling sequence. These characters are intended as nulls to add a layer of complexity for cryptanalysts. This mod 90 addition will provide a new set of numbers ranging from 0 to 89. This new set can now be replaced by its equivalents on the list of meanings in Figure 3. Once all of the corresponding equivalents are found on the list of meanings, the resulting plaintext can be strung together into a logical message, intentional mistakes can be found and corrected, word breaks can be added or deleted as needed, and foreign and nonsense words can be replaced or eliminated.

To better understand this system, Figure 4 provides an example handwritten by Kaczynski. The entire example (not all pictured in Figure 4) began with ciphertext: "66, 54, 7, ... ," where the third number indicated that the unscrambling sequence would begin on row seven of Figure 1. Figure 4 begins partway through this process on row 10 of the Figure 1 matrix with "47, 74, 64, 68, 81, 80." Beginning there, Kaczynski wrote the ciphertext characters on the top row, below that the unscrambling sequence, then the result of the mod 90 addition. Finally, below the mod 90 result, he wrote the equivalent from the list in Figure 3. This example provides a clear view of how much work remains in the final step to form the plaintext into a logical message. Kaczynski commented on the multitude of errors (many intentional) within his encryption, saying that "it should be possible (with effort) to decode the message even when many errors appear."

Within Notebook X, Kaczynski wrote that while some people may consider him "sick," he finds that he is a happy man. He also wrote the following statements: "Since committing the crimes reported elsewhere in my notes I feel better. I am still plenty angry ...but the difference is that I am now able to strike back, to a degree ...I am definitely glad I have done what I have."

Figure 3. List of meanings for Code # I.

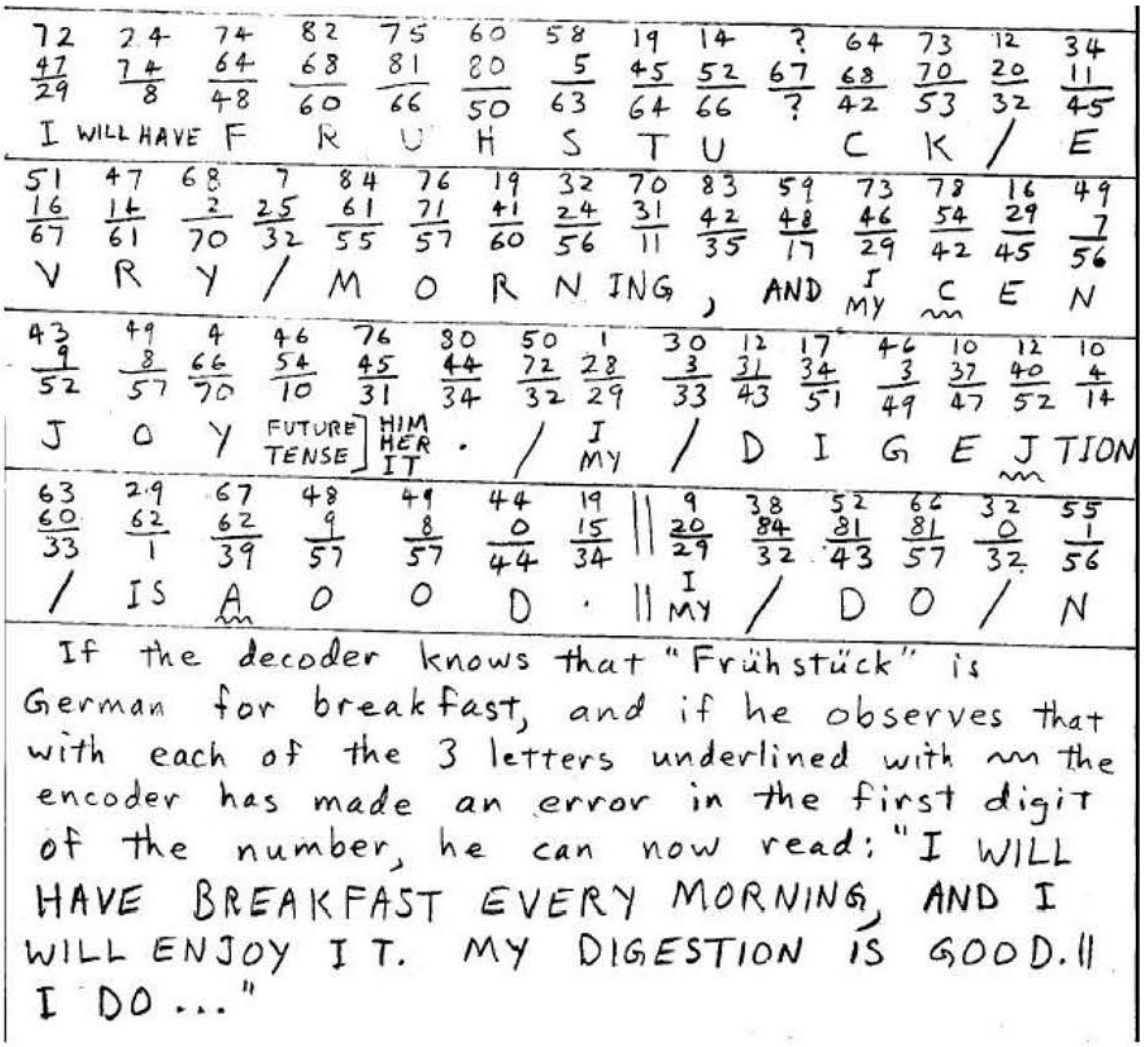


Figure 4. Example of Code # I.

4. Code # II

Kaczynski's second encryption system, Code # II, is significantly less complex than Code # I. Code # II involves two separate notebooks called Notebook A and Notebook B, each filled entirely of strings of comma-delimited ciphertext numbers. Code # II does not employ as many safeguards as Code # I. However, in order to decipher this system, one requires the entirety of both notebooks and a list of meanings similar to, but different from, the one mentioned in Code # I. This list of meanings was divided into three pages as seen in Figure 5.

Within Code # II, Kaczynski included error checks to ensure that within the strings of thousands of ciphertext numbers, he did not miss a character. Circled numbers within Notebook A or Notebook B are used to check the order between the notebooks and are not part of the ciphertext message.

To begin deciphering Code # II, the first number of Notebook B is subtracted from the first number of Notebook A, then the second of Notebook B from the second of Notebook A, and so on. Kaczynski calls the string of numbers resulting from these subtractions "series one." Next, the series one numbers are taken mod 100. This resulting group is called "series two." Each number of series two is then replaced by the corresponding letter, number, syllable, word, punctuation mark, or word spacer on the list of meanings (Figure 5). This final substitution provides the intended plaintext, and as Kaczynski stated, "the decoding is complete."

Using Code # II, while discussing criminal acts he had committed, Kaczynski wrote, "Who says crime doesn't pay? I feel very good about this." Referring to one of his fatal attacks, or "experiments" as he termed his bombs, he also wrote, "Excellent. Humane way to eliminate somebody. He probably never felt a thing. 25000 dollar reward offered. Rather flattering." These snippets give an insightful glimpse into the mind of the Unabomber.

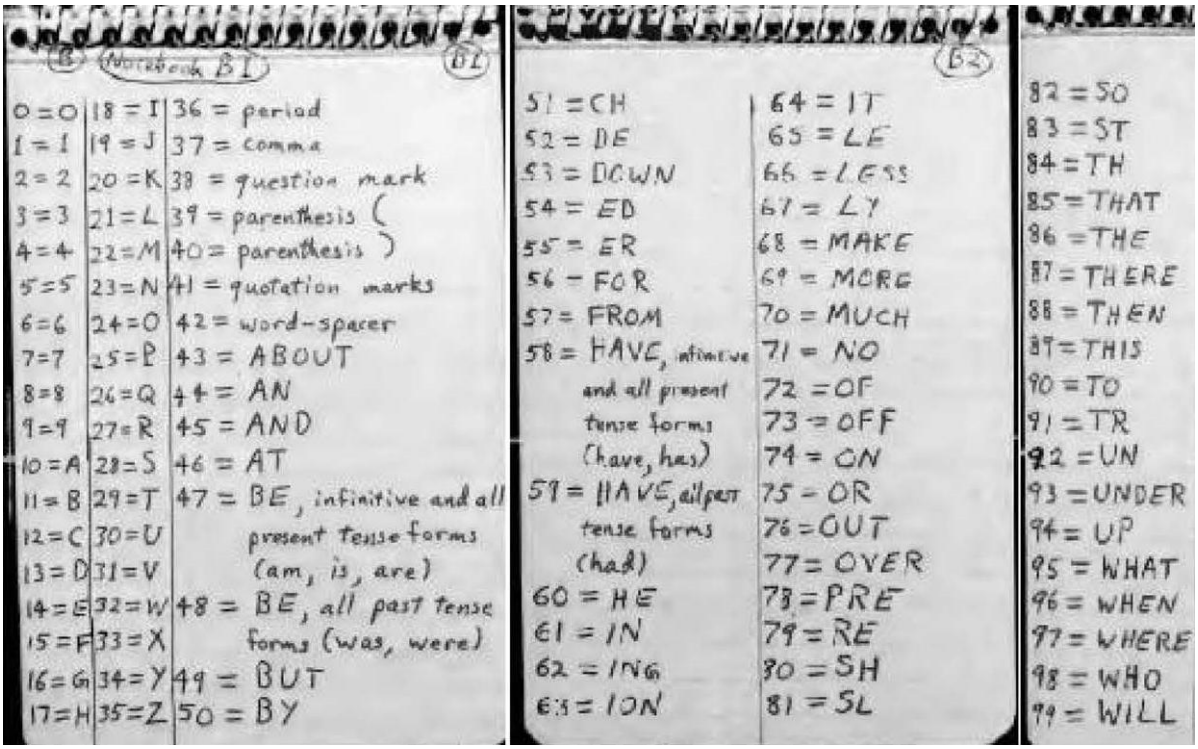


Figure 5. List of meanings for Code # II.

5. Conclusion

Theodore Kaczynski created elaborate systems of encipherment to secrete his private thoughts from unintended readers. His systems, while complex and theoretically successful in concealing messages from someone with no knowledge of the systems, would be impractical for use operationally. They require many key documents to encipher and decipher, and their complexity would rule out broad usage. Kaczynski, however, was able to successfully use these systems as a personal encryption method to secure his outlet for his emotions and personal thoughts. He utilized these systems to both express and conceal his frustrations and anger with society. His writings gave details about his attacks as well as his satisfaction with his crimes.

Back Matter

About the Author

Jeanne Anderson studied mathematics and economics at Georgetown College and Oxford University. She is currently a cryptanalyst in the Cryptanalysis and Racketeering Records Unit of the FBI.

Acknowledgements

This is publication 14-07 of the Laboratory Division of the FBI. The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of the FBI or the U.S. Government. This work was prepared as part of their official duties. Title 17 U.S.C. 105 provides that "copyright protection under this title is not available for any work of the United States Government." Title 17 U.S.C. 101 defines a United States Government work as a work prepared by an employee of the United States Government as a part of that person's official duties.

The author gratefully acknowledges the work and knowledge of Mike Birch, the FBI cryptanalyst who painstakingly worked on cryptanalyzing the journals after their seizure in 1996.

The Ted K Archive

Jeanne Anderson
Kaczynski's Ciphers
27 May 2015

Cryptologia, Volume 39, Issue 3, Pages 203-209. DOI. ISSN: 0161-1194 (Print)
1558-1586 (Online). Tand of Online. Taylor & Francis Group
Correspondence to Jeanne Anderson, CRRU, FBI, 2501 Investigation Parkway,
Quantico, VA 22135, USA. E-mail: jeanne.anderson@ic.fbi.gov

www.thetedkarchive.com