Unicity Distance of the Zodiac-340 Cipher

Joachim von zur Gathen
December 12, 2021

Emily Sundberg
Clemson University
MATH 8570
April 18, 2023

Background

- In the late 1960s, the infamous serial killer known as the Zodiac Killer murdered at least 5 people in Northern California.
- He sent letters to news outlets and the police to taunt them for not being able to catch him.
- Four of these letters had encrypted messages. “Zodiac – 408” was deciphered within a week and “Zodiac – 340” was deciphered in December 2020 by David Oranchak, Jarl Van Eycke, and Sam Blake (“The Zodiac Breakers”). The solution was confirmed by the FBI and has not been seriously challenged.
- To this day, the identity of the Zodiac Killer and if he is still alive remains unknown.

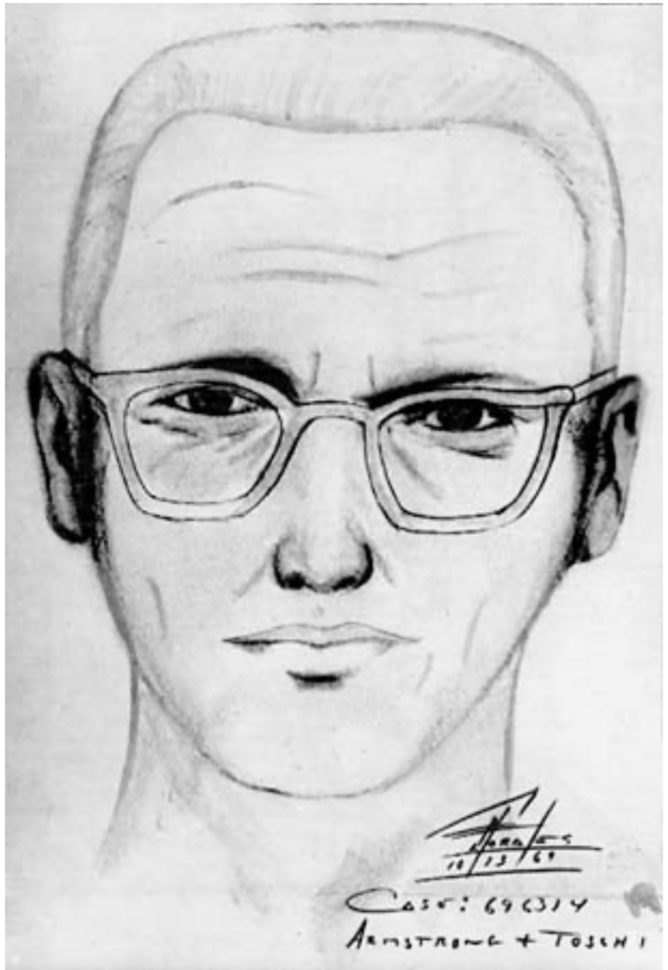


Figure 1 – Zodiac Killer Sketch

Zodiac-340 Cipher

- 340 total symbols
- 63 different characters
- 20 x 17 grid
- Went unsolved for 50 years

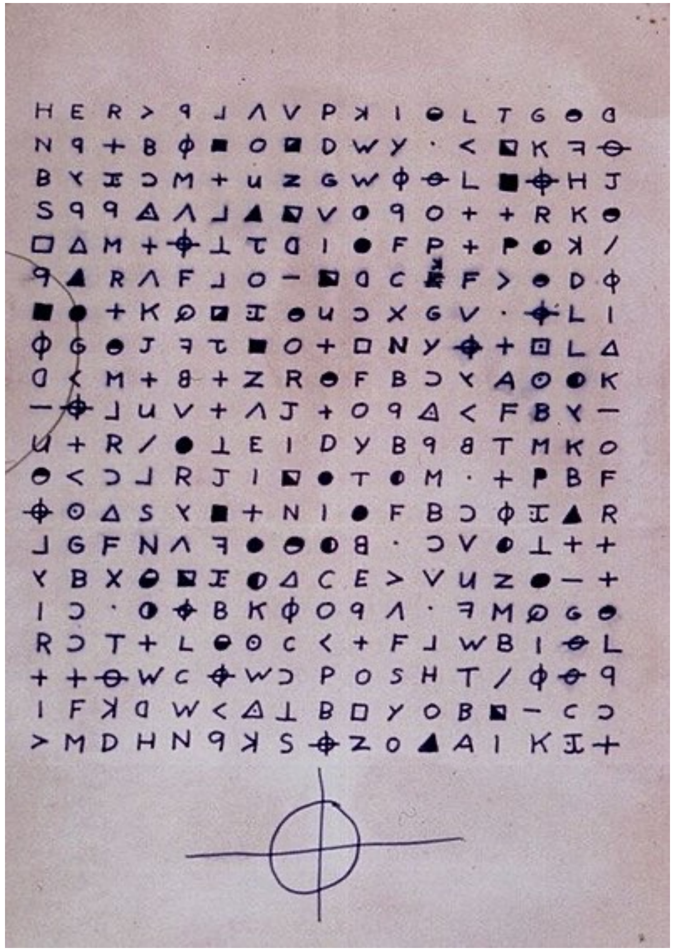
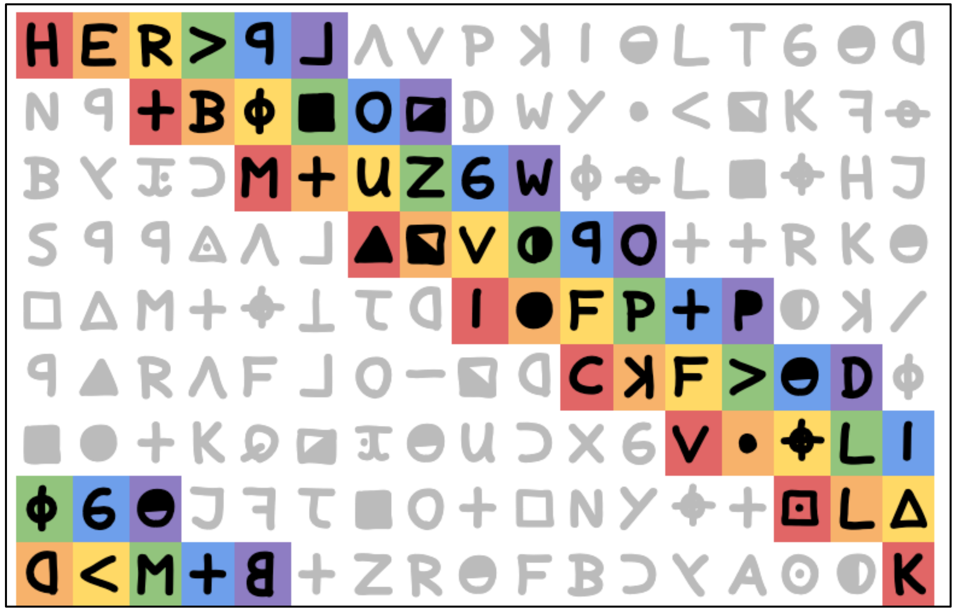


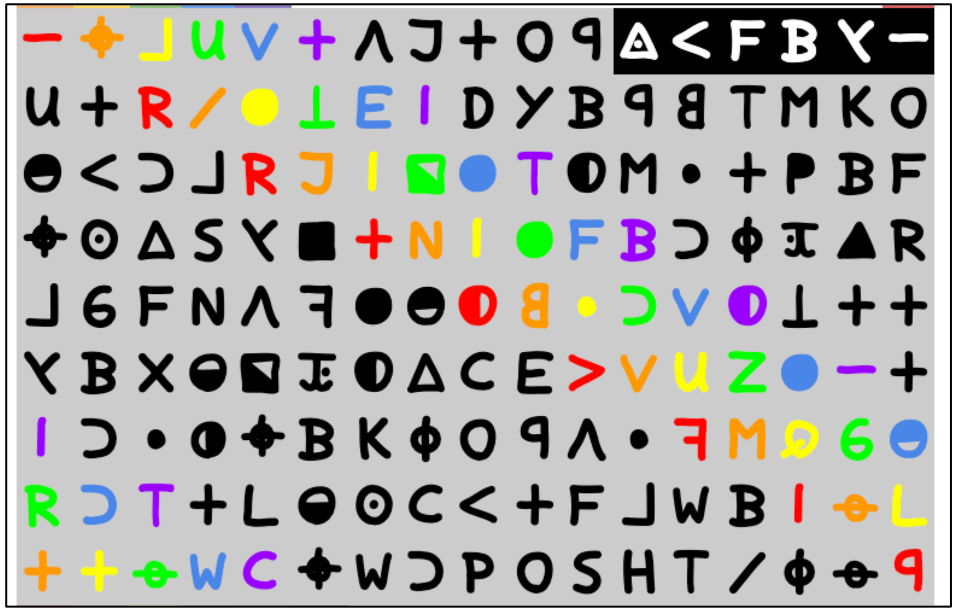
Figure 2 – Zodiac 340 Cipher

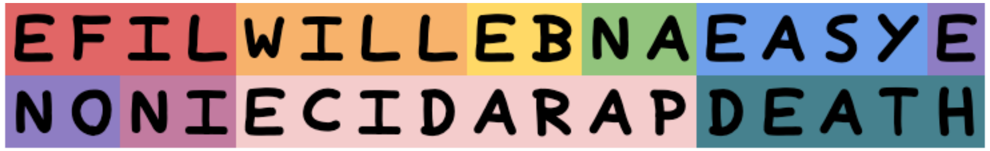
I HOPE YOU ARE HAVING LOTS OF FAN IN TRYING TO CATCH ME THAT WASNT ME ON THE TV SHOW WHICH BRINGO UP A POINT ABOUT ME I AM NOT AFRAID OF THE GAS CHAMBER BECAASE IT WILL SEND ME TO PARADLCE ALL THE SOOHER BECAUSE E NOW HAVE ENOUGH SLAVES TO WORV FOR ME WHERE EVERYONE ELSE HAS NOTHING WHEN THEY REACH PARADICE SO THEY ARE AFRAID OF DEATH I AM NOT AFRAID BECAUSE I VNOW THAT MY NEW LIFE IS LIFE WILL BE AN EASY ONE IN PARADICE DEATH

Zodiac-340 Encryption Methods

- **Homophonic Substitution**: Similar to the concept of a regular substitution cipher, but certain common letters like e, t, and a are mapped to several different ciphertext letters.
- **Sectioning of the text**: The text is sectioned into two blocks of 9 rows and then one block of two rows.
- **Transpositions**: Reading the plaintext elements in a particular order according to some rule. The rule must be bijective.







Figures created using zodiackillercipers.com

Unicity Distance

- Recall the definition of unicity distance:
  - The average amount of ciphertext required for an opponent to uniquely compute the key, given enough computing time. [2]
  - The formula for unicity distance is:

$$d = \frac{I(key)}{log_2(len) - H(lang)}$$

where I(key) is the information content of the keyspace, len is the size of the ciphertext space , and H(lang) is the entropy of the plaintext space.

- Information content is $\log_2(\mathcal{K})$ for each of the contributions to the keyspace
- len $= |\mathcal{C}| = 63$
- $|\mathcal{P}| = 26$

Calculating the Unicity Distance

$$d = \frac{I(key)}{log_2(len) - H(lang)}$$

- len $= |\mathcal{C}| = 63$
- $|\mathcal{P}| = 26$
- $|\mathcal{P}|$ with blanks $= 27$
- $|\mathrm{CT}|$ with blanks $= 430$

For homophonic substitutions: $\mathrm{I(subs)} = \log_2(26^{63}) \approx 296.13$

For sectioning of the text: $\mathrm{I(sect)} = \log_2(26{,}167) \approx 14.68$

$$\sum_{1 \le i \le 3} \binom{20-1}{i-1} \sum_{1 \le i \le 3} \binom{17-1}{i-1} = 26{,}167$$

For transpositions/reversals: $\mathrm{I(trans)} = \log_2(208) \approx 7.70$

52 choices for transposition length
2 choices for reversal or not
2 choices for unused rows or not

Replacements: $\mathrm{I(replace)} = \log_2(\mathrm{R}) \approx 244.12$

$R = \binom{340}{25} \cdot 27^{25}$ (27 is the plaintext space with an added blank)

(25 is the number of replacements – an overestimation)

I(key) is the sum of the components so I(key) ≈ 562.62

$\log_2(\mathrm{len}) = \log_2(63) \approx 5.98$

$\mathrm{H(lang)} = 1.8 \cdot \frac{430}{340} \approx 2.27$

1.8 is the entropy of the Zodiac language
430/340 is the ratio of total characters to non-blank characters

$$d = \frac{562.62}{5.98 - 2.27} \approx 152$$

Conclusions

- The unicity distance of the Zodiac-340 Cipher is at most 152.

- Some of the assumptions were more generous than necessary so it may be possible to find a smaller value.

- Since 340 is much larger than 152, it can be determined that the solution given by The Zodiac Breakers is correct.

Works Cited

[1] Gathen, Joachim. (2022). Unicity Distance of the Zodiac-340 Cipher. 91-100. 10.3384/ecp188395.

[2] Cartor, Ryann. “Feb2-Handout”. Math 8570, Cryptography, Clemson University, 2/2/2023.

Additional Sources

- Figure 1 : https://en.wikipedia.org/wiki/Zodiac_Killer#/media/File:Zodiac-Killer.jpg
- Figure 2: https://commons.wikimedia.org/w/index.php?curid=75983993
- Figure 3 https://commons.wikimedia.org/wiki/File:Zodiac_Killer_Cross.svg
- https://www.youtube.com/watch?v=iuNyQ44JYxM (Sam Blake's Talk)