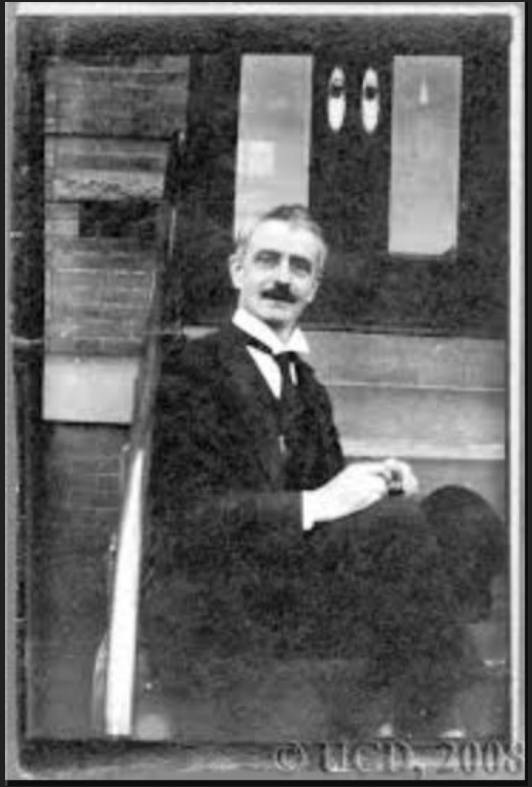
Chaocipher

Daniel Wang, Yonna Yeung

History of John F. Byrne



- Born in Ireland in 1880
- Moved to New York to be a writer in 1910
- Started to work on the cipher in 1918
- Tried to sell it to government from 1918 to 1953
- He failed to sell to the government was his reluctance to disclose how his cipher worked
- Created the autobiography Silent Years
- In this autobiography included examples of plaintext and ciphertext
- Examples included the Declaration of Independence
- No one was able to crack it until 2010, when Patricia Byrne revealed to the world the inner workings of the cipher.

Part 1

Engage the Disks

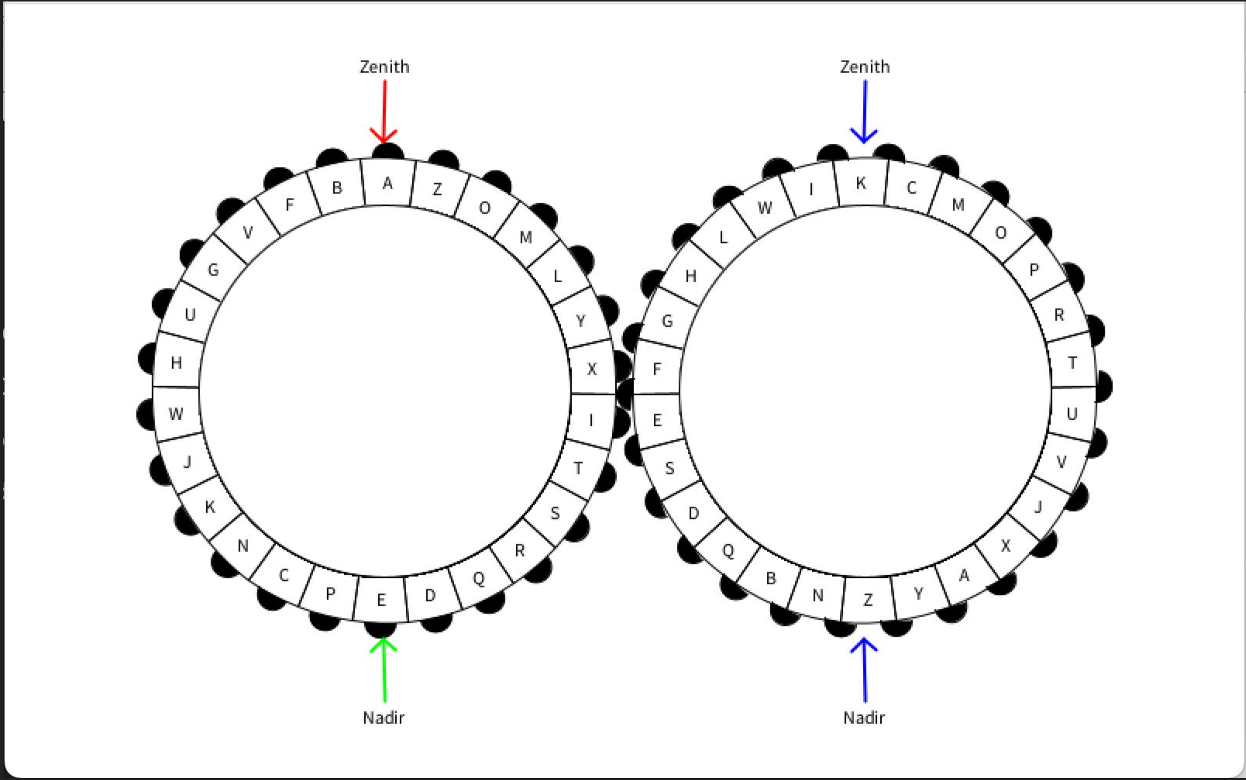
Left Alphabet:
AZOMLYXITSRQDEPCNKJWHUGVFB

Right Alphabet:
KIWLHGFESDQBNZYAXJVUTRPOMC

Plaintext: CAT

Zenith: The first letter of the alphabet

Nadir: The middle letter of the disk (14th letter)

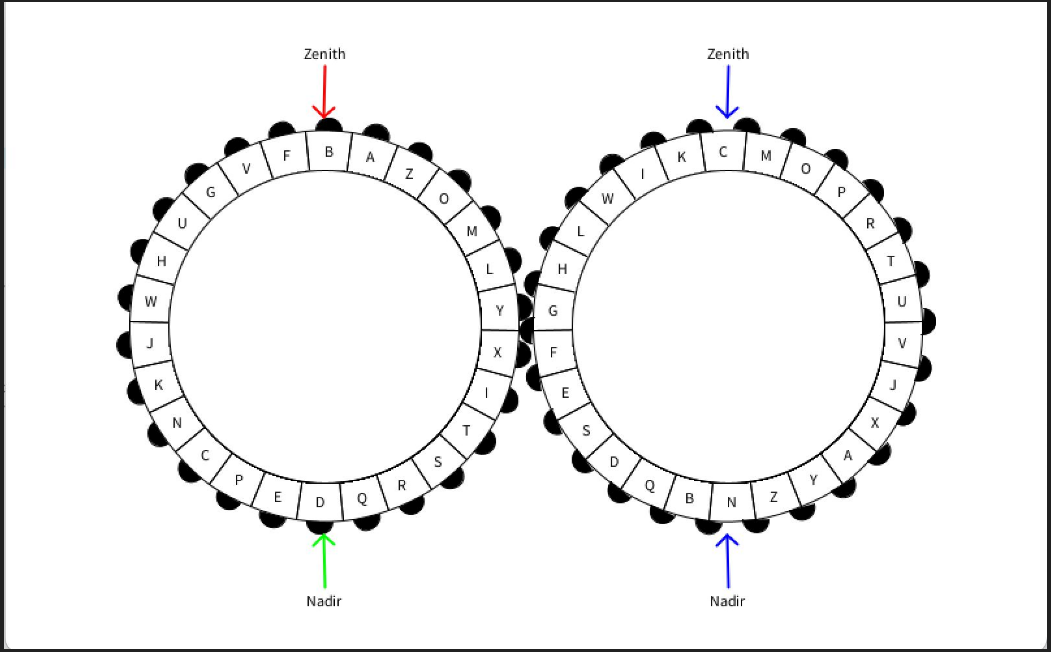

Zenith
Zenith
A Z O M L Y X I T S R Q D E P C N K J W H U G V F B
K C M O P R T U V J X A Y Z N B Q D S E F G H L W I
Nadir
Nadir

Part 2

First Encoded Letter

Left Alphabet: BAZOMLYXITSRQDEPCNKJWHUGVF

Right Alphabet: CKIWLHGFESDQBNZYAXJVUTRPOM


Zenith
Zenith
Nadir
Nadir
B A Z O M L Y X I T S R Q D E P C N K J W H U G V F
C M O P R T U V J X A Y Z N B Q D S E F G H L W I K

Part 3

Permuting Left Disk:

1. Starting Alphabet:

   BAZOMLYXITSRQDEPCNKJWHUGVF
2. B_ZOMLYXITSRQDEPCNKJWHUGVF
3. B_ZOMLYXITSRQDEPCNKJWHUGVF
4. BZOMLYXITSRQD_EPCNKJWHUGVF
5. BZOMLYXITSRQDAEPCNKJWHUGVF

Key:

Zenith

Nadir

Removed Letter

Shifted Letters

Part 4

Permuting Right Disk:

1. Starting Alphabet:

   CKIWLHGFESDQBNZYAXJVUTRPOM
2. KIWLHGFESDQBNZYAXJVUTRPOMC
3. KI_LHGFESDQBNZYAXJVUTRPOMC
4. KILHGFESDQBNZ_YAXJVUTRPOMC
5. KILHGFESDQBNZWYAXJVUTRPOMC

Key:

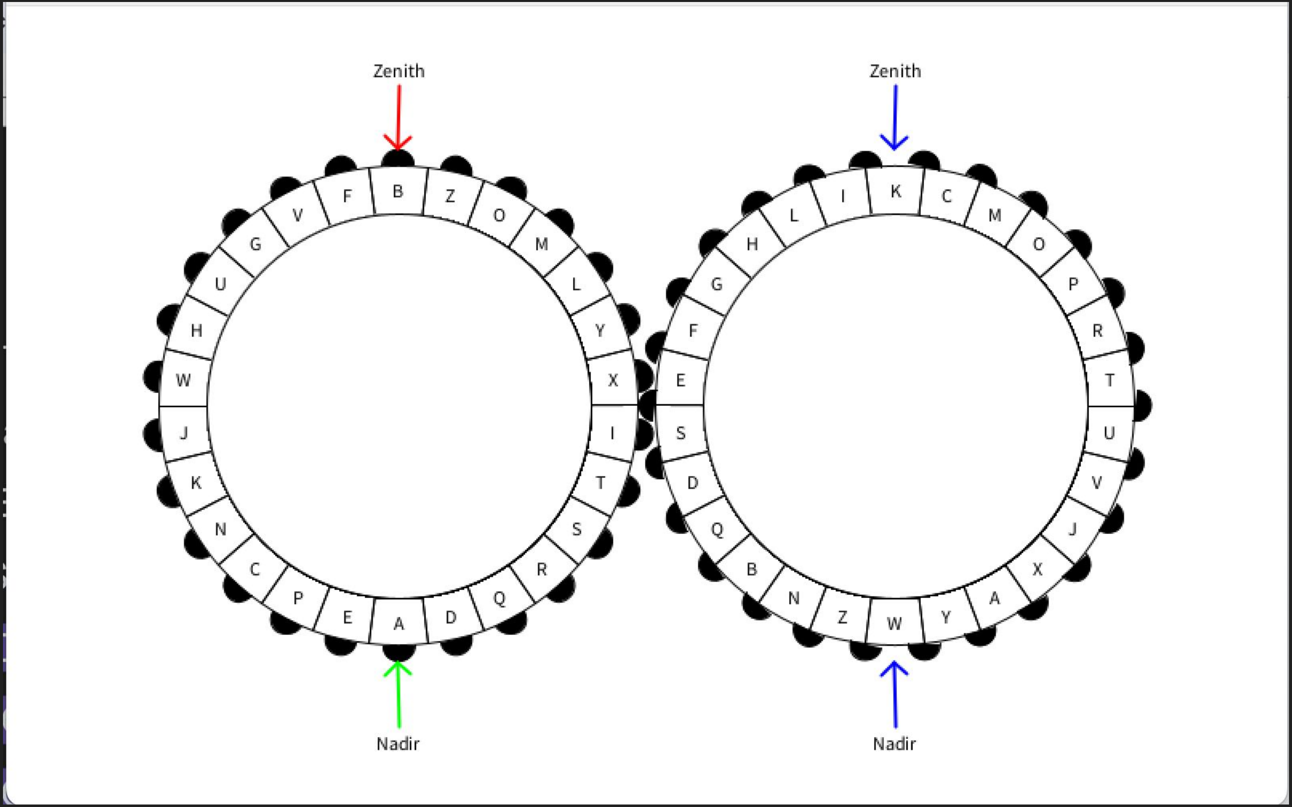
Zenith

Nadir

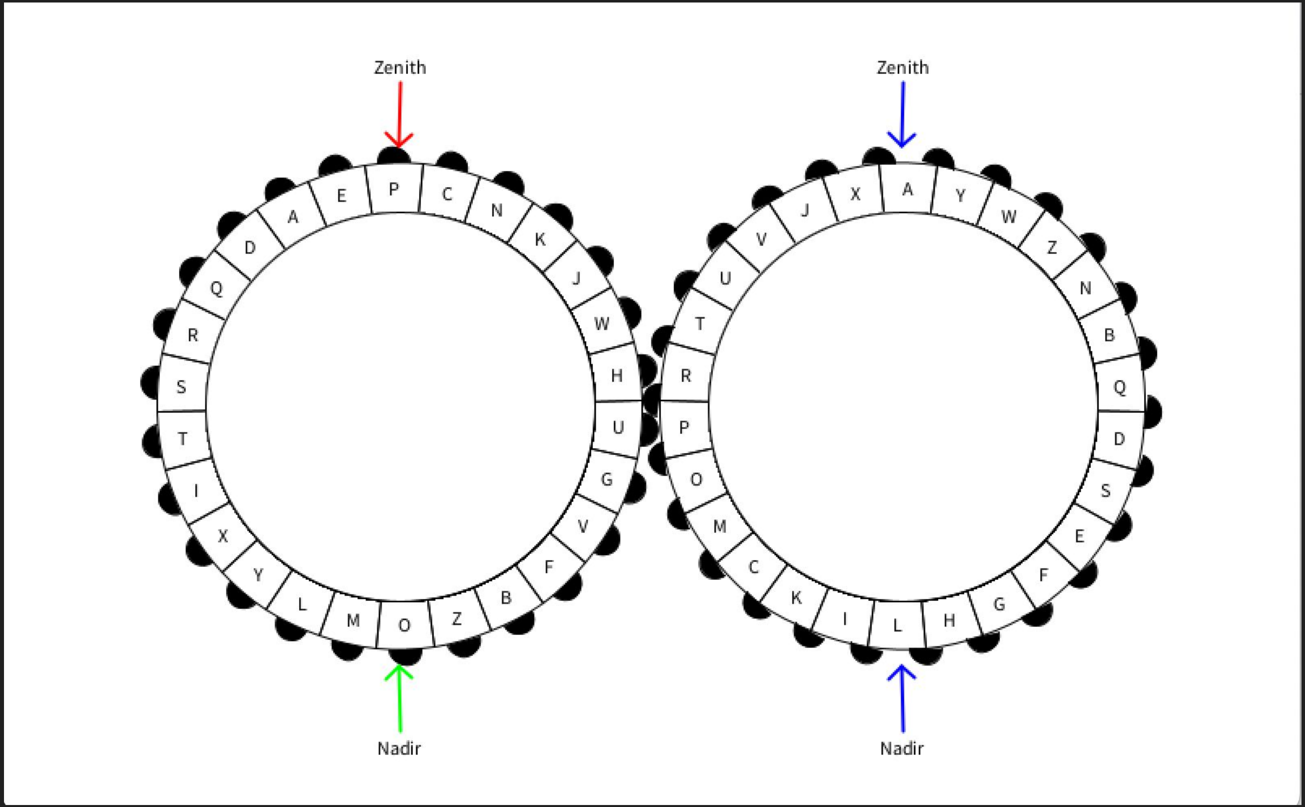
Removed Letter

Shifted Letters

Result of the First Permutations



Get Plaintext A



Final Encryption

BAZOMLYXITSRQDEPCNKJWHUGVF CKIWLHGFESDQBNZYAXJVUTRPOM

PCNKJWHUGVFBZOMLYXITSRQDAE AXJVUTRPOMCKILHGFESDQBNZWY

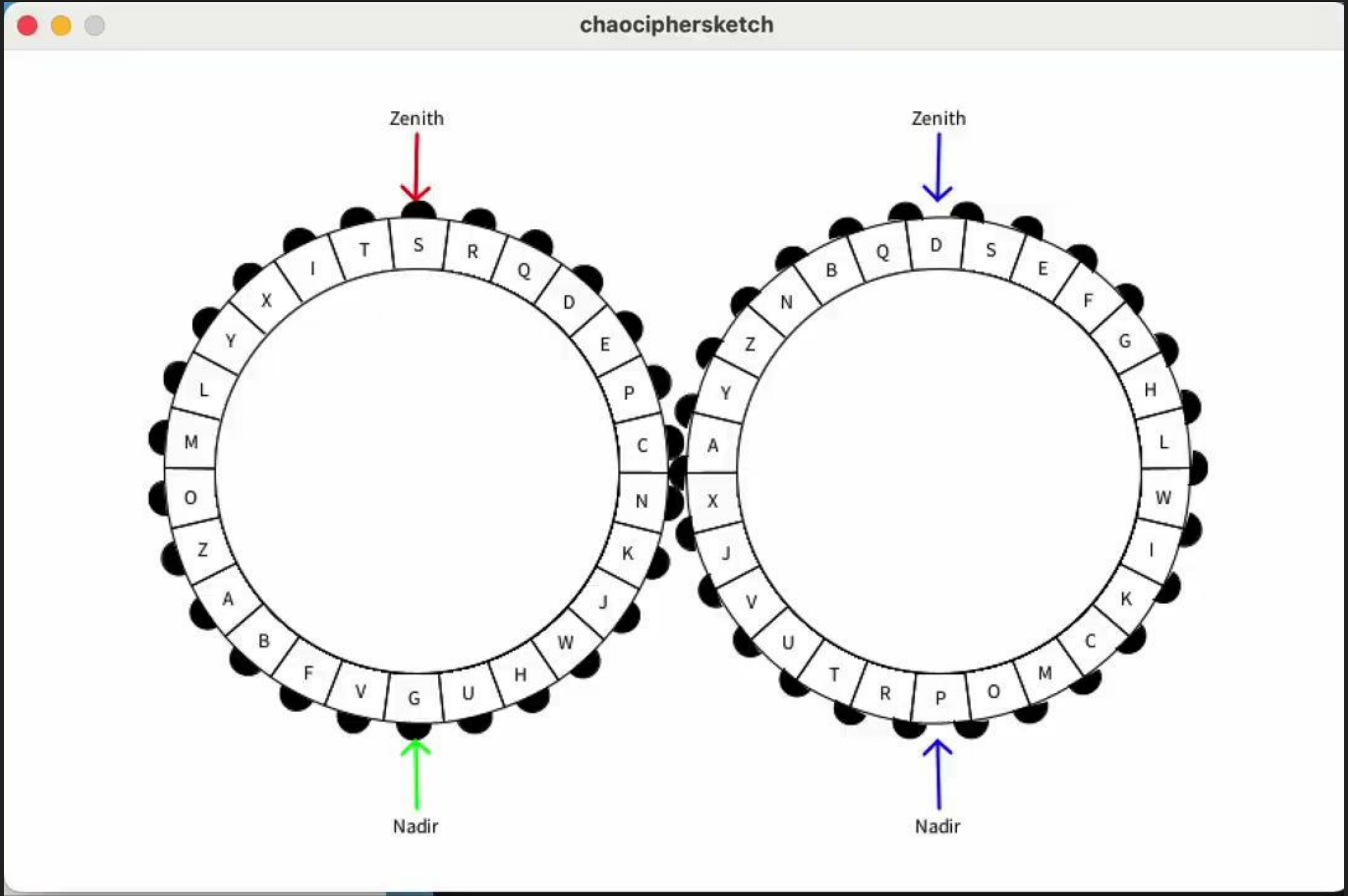
JWHUGVFBZOCMLYXITSRQDAEPNK TRPOMCKILHVGFESDQBNZWYAXJU

C → B

A → P

T → J

Final: BPJ


chaociphersketch
Zenith
S R Q D E P C N K J W H U G V F B A Z O M L Y X I T
Nadir
Zenith
D S E F G H L W I K C M O P R T U V J X A Y Z N B Q
Nadir

Part 5

- Decryption mirrors encryption steps.
- Decrypting involves similar step-by-step process with adjustments.
- Change Step 2: Rotate left disk clockwise until first letter of ciphertext is at zenith instead.
- Zenith letter on right disk is first letter of decrypted text.
- Repeat steps for each permutation of alphabets.

How Secure is the Chaocipher?

- Cipher relies on repetitions in plaintext/ciphertext.
- Breaking involves checking every possible config.
- Find longest repeated sequence for config.
- Cross-check plaintext/ciphertext for consistency.
- Max consistent configs: 444, crackable manually.
- No known solution with just ciphertext.
- Likely accepted by military if info provided.

References

https://www.inference.org.uk/cs482/projects/chaocipher/exhibit1.html

https://www.wondersandmarvels.com/2014/11/the-simply-complex-cipher-chaocipher.html

https://en.wikipedia.org/wiki/Chaocipher#